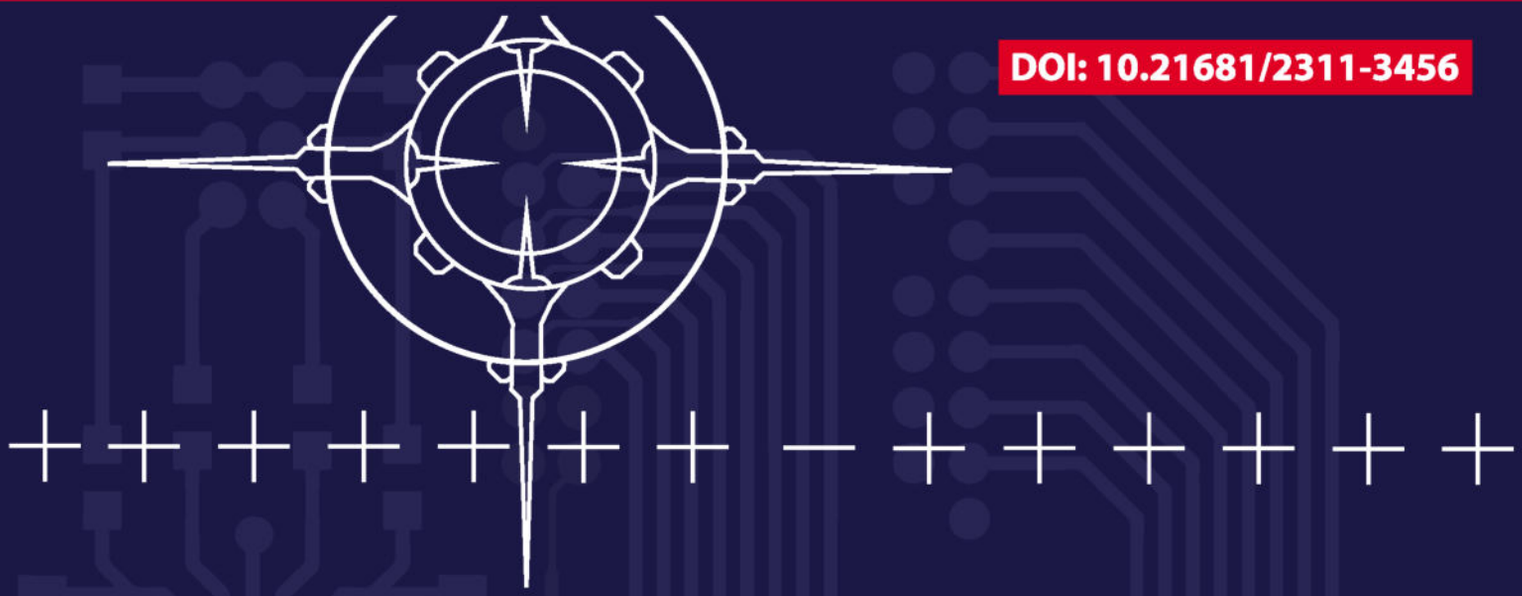
ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

№1 2025 (65)

DOI: 10.21681/2311-3456



Разноуровневые уязвимости

Управление активами

Кибербезопасность систем видеонаблюдения

Эшелон
комплексная безопасность

{KOMRAD}
Enterprise SIEM

ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ И МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

KOMRAD Enterprise SIEM позволяет осуществлять централизованный сбор событий ИБ, выявлять инциденты ИБ и оперативно на них реагировать. Применение комплекса позволяет эффективно выполнять требования, предъявляемые регуляторами к защите персональных данных, к обеспечению безопасности государственных информационных систем и контролю критической информационной инфраструктуры предприятия. KOMRAD позволяет отправлять данные о событиях и инцидентах ИБ во внешние системы (например, ГосСОПКА).

- Визуальный конструктор запросов и директив корреляции
- Высокая производительность
- Гибкая интеграция с нестандартными источкниками событий
- Широкий спектр поддержки источников событий
- Ролевая модель управления доступом
- Оперативное оповещение об инциденте
- Масштабируемость

Чтобы получить демо-версию KOMRAD Enterprise SIEM или заказать пилот у наших партнеров в вашем регионе, свяжитесь с нашим отделом продаж по e-mail: sales@npo-echelon.ru.

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ

№1 (65) 2025 г.

Выходит 6 раз в год

Журнал выходит с 2013 г. (Свидетельство о регистрации ПИ № ФС77-75239). Перерегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 07.03.2019.

Журнал входит в рейтинг научных изданий ВАК в категории К1, индексируется в RSCI, публикует статьи по специальностям 1.2.4 и 2.3.6 – физ-мат. науки; 2.2.15, 2.3.1, 2.3.5, 2.3.6 – техн. науки

Учредитель и издатель

АО «Научно-производственное объединение «Эшелон»

Над номером работали:

Г. И. Макаренко – *шеф-редактор*, И. Ю. Шахалов – *отв. секретарь*, С. С. Игнатов – *верстка*, Ю. С. Логинова – *зам. шеф-редактора*

Подписано к печати 15.02.2025 г.
Общий тираж 120 экз. Цена свободная

Адрес: 107023, Москва, ул. Электрозаводская, д. 24, стр. 1.
E-mail: editor@cyberrus.info, тел.: +7 (985) 939-75-01.
Требования, предъявляемые к рукописям, размещены на сайте: **https://cyberrus.info/**

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс 40707

ОБ ОПРЕДЕЛЕНИИ ПОНЯТИЯ «КИБЕРБЕЗОПАСНОСТЬ» И СВЯЗАННЫХ С НИМ ТЕРМИНОВ

Язов Ю. К.[1]

DOI: 10.21681/2311-3456-2025-1-2-6

Цель статьи: *раскрытие содержания терминов с префиксом «кибер» и оценка обоснованности их применения в отечественной практике.*

Методы исследования: *семантический анализ, сравнение и сопоставление, онтология понятий и их системный анализ.*

Полученный результат: *отмечено широкое применение терминов с префиксом «кибер» и отсутствие их определений в отечественных документах. Проведен краткий анализ предложений специалистов по определению таких терминов, как «киберпространство», «кибербезопасность» и др. и отмечено, что в этих определениях не показано, чем же конкретно отличаются термины с префиксами «кибер» от применяемых сегодня терминов, таких как угроза безопасности информации, сетевая атака и т.д., и почему «новые» термины можно и целесообразно использовать.*

Отмечено, что префикс «кибер» показывает их причастность к компьютерам, в том числе к Internet, информационно-телекоммуникационным системам и т.п. При этом имеет место важный признак такой причастности: в устройствах, системах, процессах, явлениях, к которым имеют отношения указанные слова с префиксом «кибер», обрабатывается (создается, передается, принимается, записывается, уничтожается и т.д.) информация в цифровой форме.

С учетом изложенного даются определения таких терминов, как «киберпространство», «кибербезопасность», «киберугроза», «кибератака» и др.

Ключевые слова: *цифровая информация, информационное пространство, киберпространство, цифровая технология, киберугроза, киберфизическая система.*

Термины с префиксом «кибер» (от англ. «cyber») стали широко применяться в зарубежной литературе еще с 90-х годов прошлого века. При этом префикс «кибер», добавляемый к обиходным словам, показывал их причастность к Internet, компьютерам, информационно-телекоммуникационным системам и т.п. В последние десять лет он очень распространился и в России. Однако в отечественных документах определение терминов, таких как «кибербезопасность», «киберугроза», «киберустойчивость», «киберпространство» и многие другие, которые широко наводнили не только прессу, но и научные издания, до сих пор фактически отсутствуют.

В целом ряде публикаций, некоторые из которых содержат весьма глубокие рассуждения и предложения, например [1–5], поднимался вопрос об определении терминов, связанных с префиксом «кибер», однако при этом не указывался основной признак, по которому термин с этим префиксом отличался от уже применяющихся в России терминов со сходным содержанием. Так, в [1] при анализе научной литературы выделены две отличительные черты применяющегося понятия «кибербезопасность»: наличие угрозы реализации компьютерной атаки и цифровые ресурсы, подлежащие компрометации. В [2] приведено несколько вариантов определения термина «кибербезопасность»:

1) с учетом перевода с английского как «информационная безопасность в сфере (области) информационных технологий, компьютерных технологий и управления»;
2) через «техническую трактовку» понятия как «информационная безопасность в киберпространстве», при этом киберпространство трактуется как «глобальная сфера внутри информационного пространства, представляющая собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая Internet, телекоммуникационные сети, компьютерные системы, а также встроенные в другие технические объекты процессоры и контроллеры, предназначенные для хранения, обработки, модификации и обмена данными»[2];
3) через связку с целями информационной безопасности, определенными доктриной информационной безопасности Российской Федерации, как свойство (состояние) компьютерных информационно-управляющих телекоммуникационных инфраструктур сохранять заданную функциональную устойчивость при гарантированном соответствии требованиям информационной безопасности;
4) через соотношение понятий «информационная безопасность» и «кибербезопасность» как

1 Язов Юрий Константинович, доктор технических наук, профессор, главный научный сотрудник Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. E-mail: yazoff_1946@mail.ru

2 Операции в киберпространстве, МО США, 2010 г.

информационная безопасность в инфосфере компьютерных информационно-управляющих и телекоммуникационных инфраструктур, где под инфосферой (то есть информационной сферой) понимается «совокупность информации, объектов информатизации, информационных систем, сайтов информационно-телекоммуникационной сети Internet, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и оборотом информации, развитием и использованием названных технологий, обеспечением информационной безопасности»[3].

Указанные определения, кроме первого, достаточно близко раскрывают суть понятия «киберпространство», поскольку оно связывается с компьютерными системами информационно-телекоммуникационными сетями, однако из них не видно, чем же конкретно отличается информационное пространство от киберпространства, и это не дает возможность достаточно ясно определить и обосновать целесообразность использования других широко применяемых сегодня терминов с префиксом «кибер», таких как «кибербезопасность» в сопоставлении с термином «информационная безопасность», «киберугроза», «кибератака», «киберустойчивость», «киберпреступление», «кибертерроризм» и многие другие [5–8]. Надо отметить, что количество таких терминов постоянно растет, некоторые из них вполне состоятельные, например, термин «киберфизические системы», а некоторые вызывают даже недоумение, например, термин киберполицейский, что оказывается соответствует не киборгу, а полицейскому, занимающемуся вопросами кибербезопасности. Вместе с тем, имеет место важный признак причастности тех или иных слов с префиксом «кибер» к Internet, компьютерам, информационно-телекоммуникационным системам: в устройствах, системах, процессах, явлениях, в ходе выполнения действий, к которым имеют отношения указанные слова, обрабатывается (создается, передается, принимается, записывается, уничтожается и т.д.) информация в цифровой форме (в [1] – это цифровые ресурсы).

Известно, что информация может представляться в документационной, аналоговой или в цифровой форме. Документационная информация содержится (в буквенно-цифровом виде, в виде иероглифов и т.д.) на бумаге или иных носителях. Аналоговая информация может содержаться в звуке (в частности речи), в виброакустических и гидроакустических колебаниях, в электрическом токе, в электромагнитных колебаниях и др. Она представляется, как правило, в виде непрерывных сигналов.

Цифровая информация – это информация, для обработки которой (генерации, фиксации, приема, передачи, сбора, представления, записи, хранения, копирования, уничтожения, модификации и т.д.) применяются исключительно цифровые технологии. При этом цифровая технология представляет собой совокупность методов, процессов и инструментов, основанных на использовании цифровых данных[4] и цифровых устройств их обработки. Сегодня на основе цифровых технологий функционируют, например: компьютеры и компьютерные сети, в том числе глобальная сеть Internet; системы искусственного интеллекта и машинного обучения; системы распределённого реестра (блокчейн); «интернет вещей» (IoT, Internet of Things – объединение разных устройств в общую сеть, в которой они могут собирать информацию, обрабатывать её и обмениваться данными между собой, с человеком и серверами в дата-центре или облаке), в том числе промышленный «интернет вещей» (IIoT – Industrial Internet of Things); системы сбора и аналитической обработки больших данных (Big Data); киберфизические системы и др. Цифровая информация получается путем соответствующего аналого-цифрового преобразования документационной или аналоговой информации.

С учетом изложенного становится достаточно прозрачным понятие «киберпространство» как часть информационного пространства, в котором циркулирует цифровая информация и функционируют цифровые устройства ее обработки. Ведь в соответствии с п. 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утверждённой Указом Президента РФ от 9 мая 2017 № 203, информационное пространство – совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры.

По сути, информационное пространство, кроме цифровой информации и цифровых устройств, содержит также аналоговую информацию и соответствующие устройства для ее обработки, то есть для генерации, фиксации, приема, передачи, сбора, представления, хранения и т.д. Выделяя его составляющую – «киберпространство», можно сразу ограничить предмет рассмотрения только цифровой информацией и устройствами ее обработки.

Аналогичным образом можно трактовать и иные термины, связанные с префиксом «кибер». В частности, **киберугроза** представляет собой угрозу безопасности цифровой информации и угрозу безопасности

3 Доктрина информационной безопасности Российской Федерации. Указ Президента РФ от 5 декабря 2016 г. №646.

4 Цифровые данные – это информация, представленная в виде цифровых кодов. Для представления таких данных сегодня используется, преимущественно, двоичное, третичное, десятичное и шестнадцатеричное исчисления.

функционирования устройств ее обработки. Киберугрозы – это лишь часть множества угроз безопасности информации и тем более угроз информационной безопасности.

Следует подчеркнуть различие понятий «безопасность информации» и «информационная безопасность». В Доктрине информационной безопасности, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, введено понятие информационной безопасности Российской Федерации как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. Аналогичным образом было введено и понятие информационной безопасности организации как «состояния защищенности интересов (целей) организации в условиях угроз в информационной сфере». Из этого следует, что безопасность информации касается только самой информации, а информационная безопасность – значительно более широкое понятие, охватывающее интересы людей, организаций (предприятий) и государства в информационной сфере. Кроме защиты самой информации, при обеспечении информационной безопасности должна осуществляться также «защита от информации» (навязывания ложной, тенденциозной, социально вредной и иной неприемлемой для личности, общества и государства информации), а также применение мер, направленных на обеспечение прав граждан на информированность и получение ими достоверной и своевременной информации. В этом смысле спектр угроз информационной безопасности значительно шире спектра угроз безопасности информации.

Тесно связан с понятием «киберугроза» широко применяемый сегодня термин «кибератака». В общем случае атака – это процесс реализации угрозы, а значит кибератака это процесс реализации киберугрозы. Однако при этом нужно иметь в виду следующее. Как правило, атака на компьютер реализуется с использованием протоколов межсетевого взаимодействия и именуется как сетевая атака, под которой понимаются «действия с применением программных и (или) программно-технических средств и с использованием сетевого протокола, направленные на несанкционированный доступ к информации, воздействие на нее или на ресурсы автоматизированной информационной системы»[5]. Таким образом, кибератака, реализуемая в информационно-телекоммуникационной сети или в информационной системе, является, по сути, синонимом сетевой атаки.

Особо следует остановиться на определении понятия «кибербезопасность». Оно охватывает понятия, во-первых, «безопасности цифровой информации» и, во-вторых, безопасность функционирования цифровых устройств ее обработки в условиях существования и реализации киберугроз. В связи с изложенным **кибербезопасность** – это состояние защищенности цифровой информации и устройств ее обработки от киберугроз. К таким устройствам могут относиться компьютеры и их программные и программно-аппаратные элементы, компьютерные (информационные) системы, промышленные программно-аппаратные комплексы, автоматизированные системы управления технологическим производством, информационно-телекоммуникационные сети и т.д.

В некоторых публикациях, наряду с термином «кибербезопасность», стал применяться термин «киберустойчивость». Как правило, при этом имеют в виду устойчивость функционирования компьютера, компьютерной системы и иных цифровых устройств в условиях реализации киберугроз. Этот термин не применяется к информации. С учетом изложенного под **киберустойчивостью** следует понимать способность цифровых устройств противостоять киберугрозам.

Аналогичным образом можно определить такие термины, как:

- «киберпреступление» – преступление, связанное с нарушением безопасности цифровой информации, устройств ее обработки, а также с причинением материального, финансового или иного ущерба гражданам, учреждениям, организациям, предприятиям и государству путем противоправных действий в киберпространстве;
- «кибермошенничество» – это один из видов киберпреступлений, целью которого является причинение материального, финансового или иного ущерба путем хищения с использованием компьютерной сети личной информации граждан (например, номеров банковских счетов, паспортных данных, кодов, паролей и т.п.);
- «кибертерроризм» (от лат. terror – страх, ужас) – система взглядов (идеология) и преднамеренная деятельность отдельных лиц, групп, организаций и спецслужб иностранных государств, направленная на использование компьютеров и информационно-телекоммуникационных сетей в террористических целях. Такими целями могут быть, например, преднамеренное нарушение функционирования информационно-телекоммуникационных сетей, значимых объектов критической информационной инфраструктуры страны, в том

5 ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Приказ руководителя Ростехрегулирования от 18 декабря 2008 № 532 – СТ.

числе информационных систем органов власти, автоматизированных систем управления, функционирующих в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сферы и иных сфер финансового рынка, топливно-энергетического комплекса, в области атомной энергетики, оборонной, ракетно-космической, горнодобывающей, металлургической, химической и иных отраслей промышленности. По сути, «кибертерроризм» – это использование киберпространства для террористической деятельности. Аналогичным образом можно определить и иные иногда встречающиеся термины:

- «кибершпионаж» – шпионаж с использованием киберпространства;
- «кибервойна» – война в киберпространстве;
- «кибернадзор» – введение строгого общественного контроля в киберпространстве.

Наконец, следует остановиться еще на одном важном термине, который широко стал применяться в различных научных школах и, в частности, учеными Санкт-Петербурга, специализирующимися в области безопасности информации – на термине «киберфизическая система» (от англ. cyber-physical system – CPS) [9–12]. Это понятие возникло в связи с интеграцией вычислительных ресурсов и управляемых с их помощью физических процессов. В такой системе датчики, оборудование и информационные системы соединены на протяжении всей цепочки создания продукции или предоставления услуг с возможным выходом за рамки одного предприятия или бизнеса. Элементы этой системы взаимодействуют друг с другом с помощью стандартных интернет-протоколов для прогнозирования, самонастройки и адаптации к изменениям.

С учетом изложенного под киберфизической системой сегодня понимают сложную распределенную систему, состоящую из совокупности вычислительных и физических элементов, которая постоянно получает данные из окружающей среды и использует их для управления физическими и вычислительными процессами. Эти системы уже достаточно широко стали применяться в промышленном производстве и робототехнике, в здравоохранении, энергетике, сельском хозяйстве, в интенсивно развивающемся сегодня «интернет вещей» (реализации концепций «умного дома», «умного города» и т.п.). «Вычислительные элементы» в таких системах – это компьютеры и иные цифровые устройства, что и обусловливает применение префикса «кибер».

Таким образом, появление и широкое применение терминов с префиксом «кибер» является вполне объективным фактом, отражающим широкое внедрение в практику цифровых технологий. Применение этих терминов позволяет сузить рассматриваемое информационное пространство до той части, которая связана с обработкой цифровой информации и применением для этого цифровых устройств. Они не заменяют в полном смысле и не отменяют существующие термины, распространяемые на все информационное пространство, а лишь конкретизируют предметную область.

Литература

1. *Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей / А. С. Марков // Вопросы кибербезопасности. 2022. № 1 (47), с. 2–9. DOI:10.21681/2311-3456-2022-1-2-9*
2. *Добродеев А. Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века/ А. Ю. Добродеев// Вопросы кибербезопасности. 2021. № 4 (44), с. 61–72. DOI:10.21681/2311-3456-2021-4-61-72*
3. *Стародубцев Ю. И. Структурно-функциональная модель киберпространства/ Ю. И. Стародубцев, П. В Закалкин, С. А Иванов // Вопросы кибербезопасности. 2021. № 4 (44), с. 16–24. DOI:10.21681/2311-3456-2021-4-16-24*
4. *Дылевский, И. Н. О взглядах администрации США на киберпространство как новую сферу ведения военных действий/ И. Н. Дылевский, С. И. Базылев, О. В. Заливхин и др. // Военная мысль. 2020. №10, с. 22–29.*
5. *Карцхия А. А., Макаренко Г. И., Сергин М. Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31), с. 18–23. DOI:10.21681/2311-3456-2019-3-18-23*
6. *Архипова Е. А. Современное понимание терминов «кибернетическая безопасность» и «информационная безопасность» // Yung Scientis, 2019, № 12 (76), pp. 315–320. DOI:10.32839/2304-5809/2019-12-76-67*
7. *Башкиров Н. Взгляды военного и политического руководства США на защиту инфраструктуры от киберугроз // Зарубежное военное обозрение. 2018, № 12, с. 13–17.*
8. *Журавель В. П. Противодействие угрозе кибертерроризма // Зарубежное военное обозрение. 2018, № 55, с. 12–16.*
9. *Мещеряков Р. В., Исхаков С. Ю. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем // Вопросы кибербезопасности. 2022. № 5 (51), с. 82–99. DOI:10.21681/2311-3456-2022-5-82-99*
10. *Коршунов Г. И. Моделирование физических сред для оптимизации цифрового управления в киберфизических системах // НиКСС. – 2023. – № 1 (41), с. 23–28. DOI: 10.21685/2307-4205-2023-1-3*
11. *Бурый А. С. Информационные структуры умного города на основе киберфизических систем / А. С. Бурый, Д. А. Ловцов // Правовая информатика. – 2022. – № 4. – С. 15–26. DOI: 10.21681/1994-104-2022-4-15-26*
12. *Фатин А. Д., Павленко Е. Ю. Анализ моделей представления киберфизических систем в задачах обеспечения информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2020. – № 2. с. 109–121.*
13. *Язов В. О научных специальностях «кибербезопасность» и «методы и системы защиты информации, информационная безопасность» // Вопросы кибербезопасности. 2022. №2 (48). С. 5–6.*

CYBERSECURITY TERMS AND DEFINITIONS

Yazov Yu. K.[6]

Keywords: *digital information, Information space, Cyberspace, Digital technology, Cyber threats, Cyber-Physical Systems (CPS).*

The goal of article: *is disclosure content of terms with the prefix «cyber» and assessment validity of their use in domestic national practice.*

The method of research: *is semantic analysis, comparison and contrast, ontology of concepts and their system analysis.*

The result of the research: *is widespread use of terms with the prefix «cyber» and the absence of their definitions in domestic national documents. A brief analysis of the proposals of specialists to define such terms as «cyberspace», «cybersecurity», etc. has defined. It is noted that these definitions do not show exactly how the terms with the prefixes «cyber» differ from terms used today, such as information security threat, network attack, etc., and why «new» terms can and should be used. It is noted that the prefix «cyber» shows their involvement with computers, including the Internet, information and telecommunication systems, etc. In this case, there is an important sign of such involvement: in devices, systems, processes, phenomena, to which these words with the prefix «cyber» are related, information in digital form is processed (created, transmitted, received, recorded, destroyed, etc.). Based on the above, definitions of such terms as «cyberspace», «cybersecurity», «cyber threat», «cyberattack» are provided.*

References

1. *Markov A. S. Kiberbezopasnost' i informacionnaja bezopasnost' kak bifurkacija nomenklatury nauchnyh special'nostej/ A. S. Markov // Voprosy kiberbezopasnosti. 2022. № 1 (47), s. 2–9. DOI:10.21681/2311-3456-2022-1-2-9*
2. *Dobrodeev A. Ju. Kiberbezopasnost' v Rossijskoj Federacii. Modnyj termin ili prioritetnoe tehnologicheskoe napravlenie obespechenija nacional'noj i mezhdunarodnoj bezopasnosti XXI veka/ A. Ju. Dobrodeev // Voprosy kiberbezopasnosti. 2021. № 4 (44), s. 61–72. DOI:10.21681/2311-3456-2021-4-61-72*
3. *Starodubcev Ju. I. Strukturno-funkcional'naja model' kiberprostranstva/ Ju. I. Starodubcev, P. V. Zakalkin, S. A. Ivanov// Voprosy kiberbezopasnosti. 2021. № 4 (44), s. 16–24. DOI:10.21681/2311-3456-2021-4-16-24*
4. *Dylevskij, I. N. O vzgljadah administracii SShA na kiberprostranstvo kak novuju sferu vedenija voennyh dejstvij/ I. N. Dylevskij, S. I. Bazylev, O. V. Zalivhin i dr. // Voennaja mysl'. 2020. № 10, s. 22–29.*
5. *Karchija A. A., Makarenko G. I., Sergin M. Ju. Sovremennye trendy kiberugroz i transformacija ponjatija kiberbezopasnosti v uslovijah cifrovizacii sistemy prava // Voprosy kiberbezopasnosti. 2019. № 3 (31), s. 18–23. DOI:10.21681/2311-3456-2019-3-18-23*
6. *Arhipova E. A. Sovremennoe ponimanie terminov «kiberneticheskaja bezopasnost'» i «informacionnaja bezopasnost'»/ E. A. Arhipova // Yung Scientis, 2019, № 12 (76), pp. 315–320.*
7. *Bashkirov N. Vzgljady voennogo i politicheskogo rukovodstva SShA na zashhitu infrastruktury ot kiberugroz // Zarubezhnoe voennoe obozrenie. 2018., № 12, s. 13–17.*
8. *Zhuravel' V. P. Protivodejstvie ugroze kiberterrorizma // Zarubezhnoe voennoe obozrenie. 2018., № 5, s. 12–16.*
9. *Meshherjakov R. V., Ishakov S. Ju. Issledovanie indikatorov komprometacii dlja sredstv zashhity informacionnyh i kiberfizicheskih sistem // Voprosy kiberbezopasnosti. 2022. № 5 (51), s. 82–99. DOI:10.21681/2311-3456-2022-5-82-99*
10. *Korshunov G. I. Modelirovanie fizicheskih sred dlja optimizacii cifrovogo upravlenija v kiberfizicheskih sistemah // NiKSS. – 2023. – № 1 (41), s. 23–28. DOI: 10.21685/2307-4205-2023-1-3.*
11. *Buryj A. S. Informacionnye struktury umnogo goroda na osnove kiberfizicheskih sistem / A. S. Buryj, D. A. Lovcov // Pravovaja informatika. – 2022. – № 4. – S. 15–26. DOI: 10.21681/1994-104-2022-4-15-26*
12. *Fatin A. D., Pavlenko E. Ju. Analiz modelej predstavlenija kiberfizicheskih sistem v zadachah obespechenija informacionnoj bezopasnosti // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2020. – № 2. s. 109–121.*
13. *Jazov V. K. O nauchnyh special'nostjah «kiberbezopasnost'» i «metody i sistemy zashhity informacii, informacionnaja bezopasnost» // Voprosy kiberbezopasnosti. 2022. № 2 (48). S. 5–6.*

6 Yuri K. Yazov, Dr.Sc. of Technical Sciences, Professor, Chief Researcher of the State Research and Testing Institute for Technical Information Protection Problems of the Federal Service for Technical and Export Control of Russia, Voronezh, Russia. E-mail: yazoff_1946@mail.ru

МОДЕЛЬ КВАНТОВЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ НАЦИОНАЛЬНЫХ БЛОКЧЕЙН-ЭКОСИСТЕМ И ПЛАТФОРМ

Петренко С. А.[1], Балябин А. А.[2]

DOI: 10.21681/2311-3456-2025-1-7-17

Цель исследования: *разработка математической модели квантовых угроз безопасности информации на основе сетей Петри для национальных блокчейн-экосистем и платформ «Экономики данных» Российской Федерации.*

Методы исследования: *методы системного анализа, методы теории сетей Петри, методы теории вероятностей и математической статистики, методы теории устойчивости сложных систем.*

Полученные результаты: *модель ранее неизвестных квантовых угроз безопасности информации на основе сетей Петри для национальных блокчейн-экосистем и платформ «Экономики данных» Российской Федерации.*

Научная новизна: *представлена и обоснована математическая модель квантовых угроз безопасности на основе сетей Петри, которая позволила задать метрику и меру обеспечения киберустойчивости для типовой блокчейн-системы в условиях новых кибератак злоумышленников с применением квантового компьютера.*

Ключевые слова: *угрозы безопасности информации, квантовые угрозы безопасности, блокчейн-экосистемы и платформы, кибербезопасность, киберустойчивость, методы анализа и синтеза квантово-устойчивого блокчейн.*

Введение

В настоящее время наблюдается беспрецедентный рост угроз безопасности информации в отношении объектов критической информационной инфраструктуры Российской Федерации, в том числе национальных блокчейн-экосистем и платформ [1, 2].

Общее количество инцидентов информационной безопасности (ИБ) возросло на 64% по отношению к аналогичному показателю предыдущего года (см. рис. 1) [3].

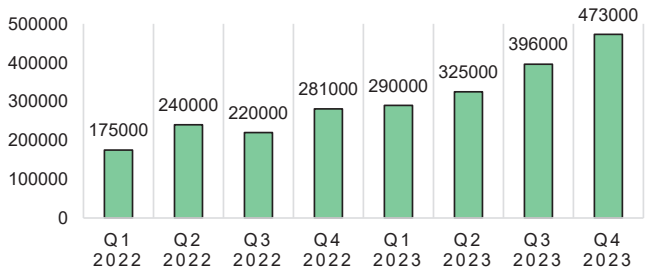


Рис. 1. События ИБ по кварталам в 2022-2023 гг.

Сегодня технологии блокчейн нашли различное применение в области криптовалют [4], смарт-контрактов [5], интернета вещей (IoT) [6], систем электронного голосования [7] и др. Криптографические преобразования, лежащие в основе технологии блокчейн, обеспечивают один из фундаментальных принципов информационной безопасности – неотказуемость, – а распределенная децентрализованная архитектура позволяет всем участникам сети верифицировать хранящиеся в ней записи без необходимости в едином «удостоверяющем центре» [8]. Несмотря на это, наблюдается рост количества инцидентов, связанных с атаками на блокчейн-платформы. Так в результате атаки на криптобиржу MtGox злоумышленниками было похищено более 450 млн долларов США [9], а всего суммарно было похищено с различных криптобирж порядка 2 млрд долларов США [10]. При этом большинство атак злоумышленников на блокчейн экосистемы и платформы осуществляется с применением классических СуперЭВМ архитектуры фон Неймана. Однако в 2023-2024 гг. были впервые зафиксированы атаки злоумышленников с применением квантового компьютера [11].

Криптостойкость алгоритмов цифровой подписи и хэширования, лежащих в основе технологии блокчейн, обеспечивается сложностью задач разложения большого числа на простые сомножители и дискретного логарифмирования. Однако применение квантовых алгоритмов, таких как алгоритм Шора, позволяет экспоненциально сократить время решения данных задач. Это представляет собой новую угрозу для блокчейн-платформ, для противодействия которой требуется внедрение квантово-устойчивых криптографических преобразований [12].

1 Петренко Сергей Анатольевич, доктор технических наук, профессор, руководитель группы, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Россия. Orcid.org/0000- 0003-0644-1731. E-mail: Petrenko.SA@talantiuspeh.ru

2 Балябин Артём Алексеевич, младший научный сотрудник, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Россия. E-mail: Balyabinю.AA@ talantiuspeh.ru

В целом рост количества и сложности кибератак на блокчейн экосистемы и платформы является общемировой тенденцией. Существующие платформы блокчейн уже не обладают требуемой киберустойчивостью в условиях роста угроз безопасности, в том числе квантовых, а применяемых классических методов и средств защиты зачастую недостаточно для предотвращения катастрофических последствий кибератак.

Особенности структуры и поведения блокчейн-экосистем и платформ

Функционирование типовой блокчейн-системы можно поэтапно представить следующим образом:

1) создание транзакции;
2) верификация и валидация транзакции;
3) формирование блока транзакций;
4) подтверждение блока транзакций по алгоритму консенсуса;
5) добавление блока в распределенный реестр.

Транзакции в блокчейн объединяются в блоки, как показано на рис. 2. Каждый блок состоит из заголовка и основой части, в которой содержатся записи обо всех входящих в этот блок транзакциях. Каждый вновь создаваемый блок транзакций хранит в себе хэш предыдущего блока так, что цепочку блоков транзакций возможно восстановить вплоть до первого блока в системе, называемого генезис-блоком.

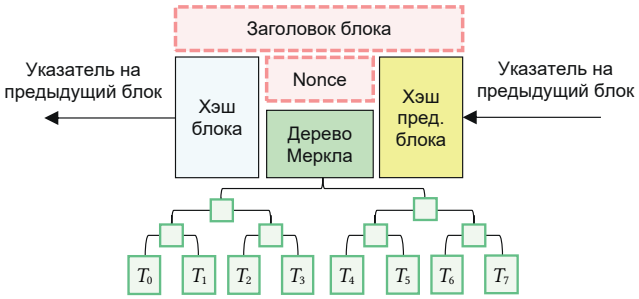


Рис. 2. Представление блокчейн в виде цепочки блоков

При формировании блока транзакций в блокчейн используется один из алгоритмов консенсуса. Наиболее распространенными алгоритмами консенсуса являются [13]:

- *Proof of Work (PoW);*
- *Proof of Stake (PoS);*
- *Delegated Proof of Stake (DPoS).*

Типовая блокчейн-система представляет собой распределенный реестр, между узлами которого осуществляется сетевое взаимодействие, поэтому в ее архитектуре возможно выделить уровни, аналогичные уровням сетевой модели OSI, включающие сверху вниз: уровень приложений, уровень сервисов, уровень протоколов, уровень сети и уровень инфраструктуры [14]. Укрупненная архитектура типовой блокчейн-системы представлена на рис. 3.

Таким образом, к особенностям национальных блокчейн-экосистем и платформ можно отнести:

- высокая сложность структуры и поведения;
- преимущественно вычислительный характер обработки данных;
- беспрецедентный рост угроз безопасности информации;
- высокие требования к безопасности и киберустойчивости и др.

Данные особенности необходимо учитывать при разработке модели квантовых угроз безопасности информации для национальных блокчейн-экосистем и платформ.

Предлагаемый способ решения задачи

Состояния типовой блокчейн-системы предлагается моделировать с помощью математического аппарата сетей Петри [15]:

$$N = (P,T,F,M_0), \quad (1)$$

где $P = \{p_1,...,p_i,...,p_n\}$ – конечное множество позиций, $n > 0$; $T = \{t_1,...,t_j,...,t_m\}$ – конечное множество переходов,

Уровень приложений	dApp Browsers	Decentralized Applications	Application Hosting	Programming Languages	
Сервисы и решения	Multi signatures	Data Feeds	Off-chain Computing	Governance, DAOs	State Channels
	Oracles	Wallets	Digital Assets	Smart Contracts	Digital IDs
Уровень протоколов	Consensus Algorithms	Side Chains	Permissioned and Permissionless	EVMs	
Уровень сети	RPLx	Roll Your Own	Block Delivery Networks	Trusted Execution Environment	Peer-to-Peer
Уровень инфраструктуры	Mining	Network	Virtualization	Nodes	Tokens	Storage

Рис. 3. Укрупненная архитектура типовой блокчейн-системы

$m > 0$, $P \cap T = \varnothing$; F – функция инцидентности, $F \subseteq (P \times T) \cup (T \times P)$; M_0 – первоначальная маркировка, $M_0 : P \longrightarrow \{1,2,3,...\}$.

При этом следует отметить, что одними из самых серьезных угроз являются угрозы эксплуатации ранее неизвестных уязвимостей «нулевого дня» (0-day) и НДВ. Как известно, такие уязвимости возникают вследствие наличия программных ошибок, меняющих поведение программы. Схема жизненного цикла уязвимости «нулевого дня» приведена на рис. 4.

В случае с блокчейн-платформами, к новым, ранее неизвестным уязвимостям могут быть отнесены архитектурные уязвимости алгоритмов, связанные с недостаточной их стойкостью в условиях воздействий с применением квантовых вычислений.

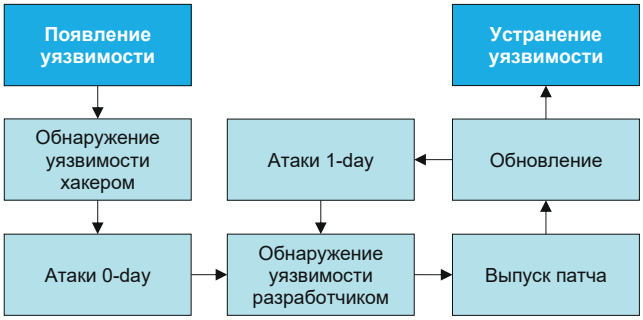


Рис. 4. Схема жизненного цикла уязвимости «нулевого дня»

Функционирование системы блокчейн опирается на допущения о ничтожно малой вероятности коллизии хэш-функций и невозможности подбора требуемого

Таблица 1.

Квантовые преобразователи

Наименование преобразователя	Обозначение	Матричное представление
Однокубитные вентили		
Вентиль Паули X	X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Вентиль Паули Y	Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Вентиль Паули Z	Z	$\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$
Вентиль Адамара	H	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Фазовый сдвиг π/4	S	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
Фазовый сдвиг π/8	T	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
Вентиль CNOT	$CNOT$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Многокубитные вентили		
Вентиль Controlled-Z	CZ	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
Вентиль SWAP	$SWAP$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

значения односторонней функции за разумное время [16, 17].

Однако данные допущения справедливы лишь для фон Неймановских компьютерных систем, одновременно обрабатывающих лишь одно состояние. Квантовые же компьютеры оперируют состояниями кубитов $|\psi\rangle$ на комплексной плоскости, при этом состояния кубитов $|0\rangle$ и $|1\rangle$ соответствуют значениям бит 0 и 1. Так квантовый компьютер, состоящий из N кубитов, способен оперировать 2^N квантовыми состояниями одновременно.

Для выполнения практических вычислений на квантовом компьютере к кубитам применяется ряд линейных преобразований, которые в широком смысле соответствуют решениям уравнения Шредингера. В табл. 1 представлены основные квантовые преобразователи, их обозначения и представление в матричной форме.

В квантовых вычислениях также применяются некоторые известные алгоритмы, которые позволяют значительно сократить время решения вычислительно-сложных криптографических задач.

Квантовый алгоритм Дойча-Йожи используется для определения того, к какому типу относится функция $f: \{0,1\}^n \longrightarrow \{0,1\}$ – постоянному или сбалансированному [18]. Известно, что сбалансированная булева функция на всей области определения возвращает значения 0 и 1 одинаковое количество раз. Для вычислений в алгоритме применяется квантовый оракул $U_f: |x,y\rangle \longrightarrow |x,y \oplus f(x)\rangle$. Последовательность шагов вычисления выглядит следующим образом:

1) начальное состояние с $n + 1$ кубитами: $|\psi_0\rangle = |0\rangle^{\oplus n} \otimes |1\rangle$;
2) преобразование Адамара над n входными кубитами приводит их в состояние суперпозиции:
$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^{2^n-1} |x\rangle \oplus |1\rangle;$$
3) применение квантового оракула U_f и получение результата:
$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \oplus |1\rangle;$$
4) повторное преобразование Адамара над n входными кубитами и измерение состояния кубитов.

Если при измерении все значения кубитов оказались равными 0, то функция $f(x)$ является постоянной, иначе – сбалансированной.

Квантовый алгоритм Шора применяется при решении задачи разложения целого числа N на простые сомножители p и q так, что $N = p \times q$. Последовательность шагов вычисления выглядит следующим образом:

1) к n входными кубитам в начальном состоянии $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ применяется квантовое преобразование Фурье;
2) поиск периода r функции $f(x) = a^x \bmod N$, где a – случайно выбранное число, взаимно простое с N.

Квантовый алгоритм Шора способен решать задачу вычисления дискретного логарифма за полиномиальное время, в частности, временная сложность факторизации числа N оценивается как $O(\log^2 N \log\log N \log\log N)$ [19].

Квантовый алгоритм Гровера применяется для решения задачи поиска элемента в неупорядоченном множестве. Математически это можно записать в виде функции $f: \{0,1\}^n \longrightarrow \{0,1\}$, при этом алгоритм Гровера решает задачу поиска x, такого, что $f(x) = 1$ [20]. Последовательность шагов вычисления выглядит следующим образом:

1) начальное состояние с n кубитами: $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$;
2) применение квантового оракула U_f для поиска состояний, удовлетворяющих условию $f(x) = 1$;
3) применение оператора диффузии Гровера D, переход к шагу 2;
4) измерение состояния кубитов и определение значения x.

Временная сложность решения задачи на множестве мощности N оценивается как $O(\sqrt{N})$, что означает возможность решения на квантовом компьютере NP-полной задачи с квадратичным приростом скорости по сравнению с решением аналогичной задачи на компьютере с фон Неймановской архитектурой.

Применение квантовых алгоритмов позволяет значительно ускорить решение ряда вычислительно-сложных задач, что приводит к возникновению отдельного класса уязвимостей архитектурного характера, эксплуатация которых представляет угрозу для блокчейн-экосистем и платформ КИИ РФ. Для наглядности в табл. 2 и 3 приведено сравнение вычислительной сложности некоторых алгоритмов решения задач факторизации числа, состоящего из $N = \log_2 n$ символов, где n – количество двоичных разрядов числа, и дискретного логарифмирования.

Таблица 2.

Временная сложность решения задачи факторизации

Наименование алгоритма	Оценка временной сложности
Алгоритм Ферма	$O\left(N^{\frac{1}{3}}\right)$
Алгоритм квадратичного решета	$O(e^{(1+0(1))\sqrt{\log n \log\log n}})$
Алгоритм решета числового поля	$O(n \log n \log N)$
Алгоритм Шора	$O(\log^3 N)$

Таблица 3.

Временная сложность решения задачи дискретного логарифмирования

Наименование алгоритма	Оценка временной сложности
Алгоритм Адлемана	$O\left(c^{\ln p^{\frac{1}{2}}}\right)$
Алгоритм COS	$O(e^{(\log p \log\log p)^{\frac{1}{2}}})$
Алгоритм решета числового поля	$O(n \log n \log N)$
Алгоритм Шора	$O(\log^3 N)$

Формирование перечня актуальных угроз безопасности

Стратифицированное представление блокчейн-платформ по уровням возникновения уязвимостей, эксплуатируемых в ходе осуществления атак, представлено на рис. 5.

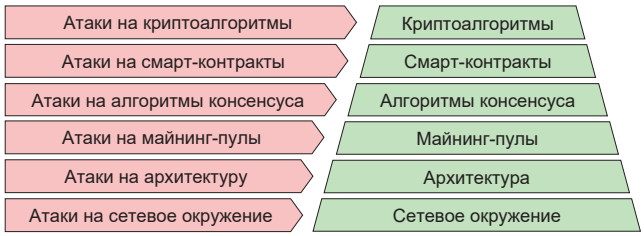


Рис. 5. Стратификация блокчейн-платформ по уровням возникновения эксплуатируемых уязвимости

Уязвимости криптографических алгоритмов. Большинство современных блокчейн-платформ (Bitcoin, Ethereum, Litecoin, Dash, Ripple, Cardano и др.) используют для генерации ключевой пары алгоритм цифровой подписи на основе эллиптических кривых (ECDSA). Криптостойкость таких алгоритмов основана на допущении о сложности вычисления дискретного логарифма на эллиптической кривой, то есть решения уравнения вида:

$$S = nT(\mathrm{mod}\ m) \qquad (2)$$

относительно n, где S, T – известные точки на эллиптической кривой, соответствующие зашифрованному и начальному сообщениям. Временная сложность дискретного логарифмирования на эллиптической кривой с помощью ρ-алгоритма Полларда составляет $O(\sqrt{n})$, где n – длина ключа в битах, в то время как применение квантового алгоритма Шора позволяет свести ее к $O(\log^3 n)$. Это может позволить злоумышленнику, имеющему квантовый вычислитель и открытый ключ, отыскать соответствующий ему закрытый ключ из ключевой пары и осуществить атаку подмены личности [21].

Другим примером уязвимостей криптографических алгоритмов является недостаточная криптостойкость применяемых в блокчейн-платформах хэш-функций (SHA256, Ethash, SCrypt, Equihash, X11 и др.) к атаке нахождения коллизии с помощью квантового алгоритма Гровера. В этом случае злоумышленник может сгенерировать вредоносный блок, обладающий такой же хэш-суммой, как и изначальный, и осуществить атаку 51 %, двойного расходования и эгоистичного майнинга [22].

Уязвимости смарт-контрактов. Смарт-контракты, используемые в таких блокчейн-платформах, как Ethereum, считаются одним из самых уязвимых элементов блокчейн [5, 23]. К причинам возникновения уязвимостей данного уровня относятся недостатки, связанные с зависимостью временных меток, порядком следования транзакций, реентерантностью и необработанными исключениями, что может позволить злоумышленнику осуществить атаку повторного воспроизведения смарт-контракта.

Уязвимости алгоритмов консенсуса. Алгоритмы консенсуса (PoW, PoS, DPoS и др.) являются одними из центральных элементов блокчейн-платформ и выполняют функции верификации блоков. В зависимости от конкретных типов алгоритмов консенсуса возможны реализации таких атак, как атака 51 %, Финни и атака двойного расходования [13, 24].

Уязвимости майнинг-пулов. Вычислительная сложность майнинга в современных блокчейн-платформах (Bitcoin, Ethereum и др.) может быть достаточно высока, что заставляет узлы объединять вычислительные мощности в пулы. С другой стороны, это представляет опасность для блокчейн-экосистемы, поскольку вычислительная мощность одного пула может превысить вычислительную мощность остальной сети блокчейн, что позволит злоумышленнику, имеющему возможность управления пулом, осуществить такие атаки, как атака 51 %, двойного расходования и удержания блока [25].

Уязвимости архитектуры. К архитектурным недостаткам блокчейн-систем можно отнести недостатки, связанные с некорректной идентификацией узлов, перезапуском системы, отсутствием ограничений размеров блока [26]. Используя эти недостатки, злоумышленник может осуществить атаки, такие как атака информационного затмения и DDoS-атака.

Уязвимости сетевого окружения. Поскольку блокчейн-платформа представляет собой одноранговую сеть взаимосвязанных узлов, распространение информации по которой осуществляется с некоторой задержкой, то она может быть уязвима для таких атак, как атака Сивиллы, двойного расходования и DNS-атака [26].

Учитывая рассмотренные уязвимости, сформируем перечень актуальных угроз устойчивости блокчейн-экосистем и платформ КИИ РФ, как показано

Таблица 4.

Перечень актуальных угроз устойчивости блокчейн-экосистем и платформ КИИ РФ

Уязвимости по уровням возникновения Атаки	Криптоалгоритмы	Смарт-контракты	Алгоритмы консенсуса	Майнинг-пулы	Архитектура	Сетевое окружение
Атака 51%	+	–	+	+	–	–
Атака подмены личности	+	–	–	–	–	–
Атака Сивиллы	–	–	–	–	–	+
Атака информационного затмения	–	–	–	–	+	+
Атака эгоистичного майнинга	+	–	+	+	–	–
Атака двойного расходования	+	–	+	+	–	–
Атака Финни	+	–	+	–	–	–
DDoS-атака	–	–	–	–	+	+
DNS-атака	–	–	–	–	–	+
Атака BGP-hijacking	–	–	–	–	+	+
Атака удержания блока	+	–	–	+	–	–
Атака на баланс	+	–	+	+	–	+
Атака повторного воспроизведения	–	+	–	–	+	–

в табл. 4. Символы «+» и «–» означают, что данная уязвимость соответственно может или не может эксплуатироваться при атаке на определенный уровень блокчейн-платформы.

Отметим, что большинство кибератак осуществляется с территорий иностранных государств, что подразумевает наличие удаленного доступа к объектам критической информационной инфраструктуры (КИИ) РФ и сетевой вектор воздействия. Значимую угрозу представляют нарушители, обладающие высоким потенциалом, в распоряжении которых имеются достаточные ресурсы для подготовки и осуществления кибератак с использованием средств эксплуатации известных и ранее неизвестных уязвимостей блокчейн-экосистем и платформ:

- специальные службы иностранных государств;
- террористические и экстремистские организации;
- организованные хакерские группировки.

Моделирование кибератак злоумышленников на блокчейн-экосистемы

Типовая схема компьютерной атаки в соответствии с MITRE ATT&CK имеет 14 этапов (тактик) и более 400 техник [27], однако, в реальных кибератаках могут задействоваться не все этапы. На рис. 6 представлена схема типового целенаправленного ИТВ на блокчейн-платформу КИИ РФ, состоящего из 5 этапов, характерных для подавляющего большинства целенаправленных ИТВ.

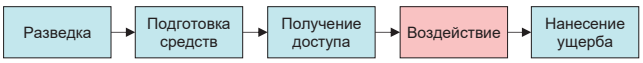


Рис. 6. Обобщенная схема ИТВ на типовую блокчейн-платформу КИИ РФ

Рассмотрим подробнее этап непосредственного воздействия на целевую систему, а также примеры кибератак злоумышленников на типовые блокчейн-платформы.

Атака 51 %. Данная атака характерна для блокчейн-платформ, использующих алгоритмы консенсуса типа PoW, PoS, DPoS, и предполагает наличие у злоумышленника 51 % или более вычислительной мощности блокчейн-платформы. Такое превосходство достижимо несколькими способами:

- увеличение количества вычислителей в пуле;
- применение квантового алгоритма Гровера.

Применение злоумышленником квантового алгоритма Гровера для поиска коллизий хэш-функций может позволить ему значительно быстрее подбирать значение параметра *Nonce* создаваемого блока и формировать произвольные вредоносные блоки

с требуемыми хэш-суммами. Сформируем модель данной атаки на основе сети Петри.

- Предусловия (условия осуществимости атаки):
  - P_1 – злоумышленник обладает 51 % или более вычислительной мощности сети блокчейн:
    - P_{11} – для алгоритмов консенсуса типа PoW:
      - P_{111} – злоумышленник контролирует более 50 % вычислительной мощности блокчейн-платформы;
      - P_{112} – злоумышленник обладает вычислительными ресурсами квантового компьютера;
    - P_{12} – злоумышленник обладает более 50 % долей владения для алгоритмов консенсуса типа PoS;
    - P_{13} – злоумышленник обладает более 50 % прав голоса для алгоритмов консенсуса типа DPoS;
  - P_2 – злоумышленник знает хэш-сумму предыдущего блока;
- Переходы (шаги осуществления атаки):
  - T_1 – синтез вредоносного блока с требуемой хэш-суммой без передачи его в блокчейн;
  - T_2 – синтез вредоносной цепочки блоков, более длинной, чем существующая;
  - T_3 – передача созданной вредоносной цепочки блоков в блокчейн;
- Постусловия (возможные направления развития атаки):
  - P_3 – блокировка транзакций;
  - P_4 – препятствование деятельности иных узлов блокчейн;
  - P_5 – обращение транзакций для подготовки атаки двойного расходования;
  - P_6 – принуждение узлов блокчейн-платформы к присоединению к вычислительным мощностям злоумышленника.

Полученная модель атаки 51 % на основе сети Петри представлена на рис. 7.

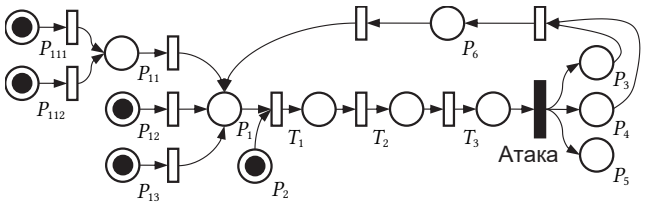


Рис. 7. Модель сети Петри для атаки 51 %

Атака двойного расходования. Одной из задач алгоритмов консенсуса является обеспечение невозможности дублирования транзакций (двойного расходования средств). Так, если $B_0,\ldots,B_i,\ldots,B_N$ – существующая цепочка блоков и целью злоумышленника является дублирование транзакции, содержащейся в блоке B_i, то ему придется заново сформировать блок B_i', не содержащий данной транзакции, а также более длинную цепочку, состоящую из блоков B_j', v с соответствующими хэш-суммами, где n – длина существующей цепочки блоков. Классическими вычислительными средствами данная атака практически не реализуема, однако, злоумышленник, обладающий возможностью осуществления квантовых вычислений, может применить алгоритм Гровера для нахождения коллизий хэш-функций. Сформируем модель данной атаки на основе сети Петри.

- Предусловия (условия осуществления атаки):
  - P_1 – злоумышленник обладает достаточными вычислительными ресурсами:
    - P_{11} – классическими;
    - P_{12} – квантовыми;
  - P_2 – транзакция записана в блок B_i и подтверждена получателем;
- Переходы (шаги осуществления атаки):
  - T_1 – синтез цепочки блоков B_i', $j = \overline{(i, n+1)}$, где блок B_i' не содержит предыдущей транзакции и распространение новой цепочки в блокчейн;
- Постусловия (возможные направления развития атаки):
  - P_3 – повторное использование средств злоумышленником.

Полученная модель атаки двойного расходования на основе сети Петри представлена на рис. 8.

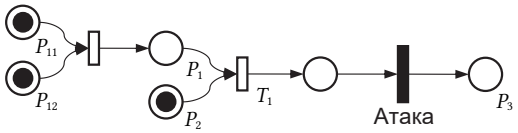


Рис. 8. Модель сети Петри для атаки двойного расходования

Атака подмены личности. Правом владения цифровых активов в блокчейн наделены обладатели закрытого ключа, а с помощью открытого ключа это право возможно проверить. Для данной атаки злоумышленнику необходимо восстановить закрытый ключ по известному открытому ключу одним из способов:

- кража данных о ключевой паре (например, в результате предварительного ИТВ);
- применение квантового алгоритма Шора для решения задачи дискретного логарифмирования за полиномиальное время.

Восстановив закрытый ключ, злоумышленник сможет действовать от имени его владельца. Сформируем модель данной атаки на основе сети Петри.

- Предусловия (условия осуществления атаки):
  - P_1 – злоумышленник обладает сведениями о параметрах эллиптической кривой для восстановления ключевой пары алгоритма ECDSA;
  - P_2 – злоумышленник обладает достаточными квантовыми вычислительными ресурсами для решения задачи дискретного логарифмирования;
  - P_3 – злоумышленник осуществил вспомогательное ИТВ и получил сведения о ключевой паре;
- Постусловия (возможные направления развития атаки):
  - P_4 – злоумышленник применил квантовый алгоритм Шора, решил задачу дискретного логарифмирования и получил закрытый ключ из ключевой пары;
  - P_5 – выполнение операций с цифровыми активами от имени владельца закрытого ключа.

Полученная модель атаки подмены личности на основе сети Петри представлена на рис. 9.

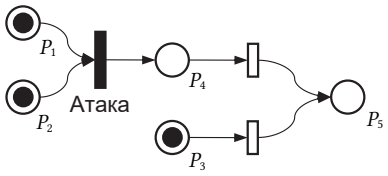


Рис. 9. Модель сети Петри для атаки подмены личности

Оценка киберустойчивости блокчейн-систем

Как правило, под устойчивостью некоторой технической системы понимают ее способность сохранять значения параметров своего функционирования в заданных пределах в условиях дестабилизирующих воздействий. Применительно к блокчейн-системам такими дестабилизирующими воздействиями являются кибератаки злоумышленников, в том числе с применением квантового компьютера. Проводя аналогию с динамическими системами, будем оценивать устойчивость функционирования блокчейн-системы в условиях кибератак злоумышленников по показателю вероятности P нахождения невосстанавливаемой системы в работоспособном состоянии в течение заданного времени t:

$$P(t) = e^{-\lambda t}, \quad (3)$$

где λ – интенсивность потока ИТВ.

Здесь мерой устойчивости является число в отрезке [0,1], где 0 обозначает абсолютно неустойчивую, а 1 – абсолютно устойчивую системы.

Примем допущение о том, что поток нарушений является простейшим. Интенсивность потока нарушений λ постоянна и зависит от вероятности искажений, которая, в свою очередь, пропорциональна количеству перебираемых хэш-сумм $N_{хэш}$ в единицу времени:

$$\lambda(t) \sim P_{иск} = const, P_{иск} = \frac{N_{хэш}}{T}. \quad (4)$$

Результаты оценки устойчивости функционирования типовой блокчейн-системы в условиях кибератак злоумышленников по показателю вероятности нахождения системы в работоспособном состоянии в зависимости от времени при различных значения $P_{иск}$ представлены на рис. 10.

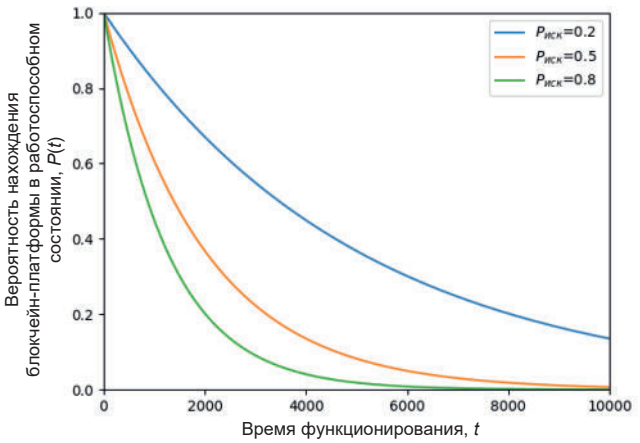


Рис. 10. Результаты оценки устойчивости функционирования типовой блокчейн-системы в условиях кибератак злоумышленников

Вероятность нахождения блокчейн-платформы КИИ РФ в работоспособном состоянии с течением времени снижается так, что $\lim_{t\to\infty} P(t) = 0$. При уменьшении количества хэш-сумм $N_{хэш}$, проверяемых в единицу времени, снижается вероятность искажения $P_{иск}$, а снижение устойчивости с течением времени замедляется. Полученные результаты позволяют подтвердить гипотезу о снижении киберустойчивости блокчейн-экосистем и платформ в условиях целенаправленных кибератак злоумышленников.

Выводы

В настоящей работе была поставлена задача разработки новой модели квантовых угроз безопасности информации на основе сетей Петри на примере некоторой типовой блокчейн-экосистемы и платформы. Приведено возможное формализованное описание источников угроз безопасности информации, сформирован перечень актуальных угроз безопасности информации. Проведено моделирование квантовых угроз безопасности, что позволило определить возможные метрику и меру обеспечения киберустойчивости блокчейн-систем в условиях кибератак злоумышленников с применением квантового компьютера.

Результаты экспериментов позволили выявить ряд количественных закономерностей снижения киберустойчивости блокчейн-экосистем и платформ «Экономики данных» РФ в условиях атак злоумышленников с применением квантового компьютера.

Статья подготовлена по результатам Проекта ФТС-2024-2.3-VY-1160-5744 «Технологии противодействия ранее неизвестным квантовым киберугрозам» в рамках реализации мероприятия 2.3 государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус».

Литература

1. *Балябин, А. А., Петренко С. А., Костюков А. Д. Модель угроз безопасности и киберустойчивости облачных платформ КИИ РФ // Защита информации. Инсайд. 2024. № 5 (119). С. 26–34.*
2. *Марков А. С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. 2023. № 1 (53). С. 2–12. DOI: 10.21681/2311-3456-2023-1-2-12.*
3. *Балябин, А. А. Модель облачной платформы КИИ РФ с кибериммунитетом в условиях информационно-технических воздействий // Защита информации. Инсайд. 2024. № 5 (119). С. 35–44.*
4. *Verma A. et al. Blockchain for Industry 5.0: Vision, Opportunities, Key Enablers, and Future Directions // IEEE Access. 2022. Vol. 10. Pp. 69160–69199. DOI: 10.1109/ACCESS.2022.3186892.*
5. *Zou W. et al., Smart Contract Development: Challenges and Opportunities // IEEE Transactions on Software Engineering. 2021. Vol. 47. No. 10. Pp. 2084–2106. DOI: 10.1109/TSE.2019.2942301.*
6. *Ali M. S., Vecchio M., Pincheira M., Dolui K., Antonelli F., Rehmani M. H. Applications of blockchains in the internet of things: A comprehensive survey // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 2. Pp. 1676–1717. DOI: 10.1109/COMST.2018.2886932.*
7. *Vladucu M. -V., Dong Z., Medina J., Rojas-Cessa R. E-Voting Meets Blockchain: A Survey // IEEE Access. 2023. Vol. 11. Pp. 23293–23308. DOI: 10.1109/ACCESS.2023.3253682.*
8. *Petrenko S., Khismatullina E. Cyber-resilience concept for Industry 4.0 digital platforms in the face of growing cybersecurity threats // Software Technology: Methods and Tools, 51st International Conference, TOOLS 2019, Innopolis, Russia, October 15–17, 2019. 420 p. DOI: 10.1007/978-3-030-29852-4.*
9. *Петренко А. С., Петренко С. А. Оценка квантовой угрозы для современных блокчейн-систем // Информационные системы и технологии в моделировании и управлении: Сборник трудов VII Международной научно-практической конференции, Ялта, 24–25 мая 2023 года. 2023. С. 171–173.*
10. *Петренко А. С., Ломако А. Г., Петренко С. А. Анализ современного состояния исследований проблемы квантовой устойчивости блокчейна. Часть 1 // Защита информации. Инсайд. 2023. № 3 (111). С. 38–46.*
11. *Петренко А. С., Петренко С. А., Костюков А. Д., Ожиганова М. И. Модель квантовых угроз безопасности для современных блокчейн-платформ // Защита информации. Инсайд. 2022. № 3 (105). С. 10–20.*
12. *Петренко А. С., Петренко С. А. Метод оценивания квантовой устойчивости блокчейн-платформ // Вопросы кибербезопасности. 2022. № 3 (49). С. 2–22. DOI 10.21681/2311-3456-2022-3-2-22.*
13. *Lashkari B., Musilek P. A Comprehensive Review of Blockchain Consensus Mechanisms // IEEE Access. 2021. Vol. 9. Pp. 43620–43652. DOI: 10.1109/ACCESS.2021.3065880.*
14. *Xie J., Tang H., Huang T., Yu F., Xie R., Liu J., Liu Y. A survey of blockchain technology applied to smart cities: Research issues and challenges // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 3. Pp. 2794–2830. DOI: 10.1109/COMST.2019.2899617.*
15. *Shahriar M. A. et al. Modelling Attacks in Blockchain Systems using Petri Nets // 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China. 2020. Pp. 1069–1078. DOI: 10.1109/TrustCom50675.2020.00142.*
16. *Younis M. M., Salim Jamil A., Abdulrazzaq A. H., Ahmed Mawla N., Khudhair R. M., Vasiliu Y. Progress and Challenges in Quantum Computing Algorithms for NP-Hard Problems // 2024 36th Conference of Open Innovations Association (FRUCT), Lappeenranta, Finland. 2024. Pp. 460–468. DOI: 10.23919/FRUCT64283.2024.10749878.*
17. *Молдовян А. А., Молдовян Н. А. Новые формы скрытой задачи дискретного логарифмирования // Труды СПИИРАН 2019. Т. 2, № 18. С. 504–529. DOI: 10.15622/sp.18.2.504-529.*
18. *Savo G. Glisic; Beatriz Lorenzo. Quantum Search Algorithms // Artificial Intelligence and Quantum Computing for Advanced Wireless Networks, Wiley. 2022. Pp. 499–542. DOI: 10.1002/9781119790327.ch11.*
19. *Петренко А. С., Романченко А. М. Перспективный метод криптоанализа на основе алгоритма Шора // Защита информации. Инсайд. 2020. № 2 (92). С. 17–23.*
20. *Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis // Voprosy Kiberbezopasnosti. 2023. No. 1 (53). Pp. 100–115. DOI 10.21681/2311-3456-2023-1-100-115.*
21. *Borges F., Reis P. R., Pereira D. A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography // IEEE Access. 2020. Vol. 8. Pp. 142413–142422. DOI: 10.1109/ACCESS.2020.3013250.*
22. *Kearney J. J., Perez-Delgado C. A. Vulnerability of blockchain technologies to quantum attacks // Array. 2021. Vol. 10. P. 100065. DOI: 10.1016/j.array.2021.100065.*
23. *Kushwaha S. S., Joshi S., Singh D., Kaur M. Lee H. -N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract // IEEE Access. 2022. Vol. 10. Pp. 6605–6621. DOI: 10.1109/ACCESS.2021.3140091.*
24. *Sayeed S., Marco-Gisbert H. Assessing blockchain consensus and security mechanisms against the 51 % attack // Applied Sciences. 2019. Vol. 9. No. 9. P. 1788. DOI: 10.3390/app9091788.*
25. *Fernandez-Carames T. M., Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks // IEEE Access. 2020. Vol. 8. Pp. 21091–21116. DOI: 10.1109/ACCESS.2020.2968985.*
26. *Mollajafari S.; Bechkoum K. Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy // Sustainability 2023. Vol. 15 (18). 13401. DOI: 10.3390/su151813401.*
27. *Al-Shaer R., Spring J. M., Christou E. Learning the Associations of MITRE ATT&CK Adversarial Techniques // 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France. 2020. Pp. 1–9. DOI: 10.1109/CNS48642.2020.9162207.*

A MODEL OF QUANTUM THREATS TO INFORMATION SECURITY FOR NATIONAL BLOCKCHAIN ECOSYSTEMS AND PLATFORMS

Petrenko S. A.[3], Balyabin A. A.[4]

Keywords: *threats to information security, quantum threats to security, blockchain ecosystems and platforms, cybersecurity, cyber resilience, methods of analysis and synthesis of quantum-resistant blockchain.*

The purpose of the research: *development of a mathematical model of quantum threats to information security based on Petri nets for national blockchain ecosystems and platforms of the «Data Economy» of the Russian Federation.*

The method of the research: *methods of system analysis, methods of Petri net theory, methods of probability theory and mathematical statistics, methods of the theory of stability of complex systems.*

The result of the research: *a mathematical model of quantum threats to security based on Petri nets is presented and substantiated, which made it possible to set a metric and measure of ensuring cyber resilience for a typical national blockchain system in the face of new cyber attacks by intruders using a quantum computer.*

References

1. *Balyabin A. A., Petrenko S. A., Kostyukov A. D. Model' ugroz bezopasnosti i kiberustoychivosti oblachnykh platform KII RF // Zashchita informatsii. Insayd. 2024. № 5 (119). Pp. 26–34.*
2. *Markov A. S. Vazhnaya vekha v bezopasnosti otkrytogo programmnogo obespecheniya // Voprosy kiberbezopasnosti. 2023. № 1 (53). Pp. 2–12. DOI: 10.21681/2311-3456-2023-1-2-12.*
3. *Balyabin A. A. Model' oblachnoy platformy KII RF s kiberimmunitetom v usloviyakh informatsionno-tekhnicheskikh vozdeystviy // Zashchita informatsii. Insayd. 2024. № 5 (119). Pp. 35–44.*
4. *Verma A. et al. Blockchain for Industry 5.0: Vision, Opportunities, Key Enablers, and Future Directions // IEEE Access. 2022. Vol. 10. Pp. 69160–69199. DOI: 10.1109/ACCESS.2022.3186892.*
5. *Zou W. et al., Smart Contract Development: Challenges and Opportunities // IEEE Transactions on Software Engineering. 2021. Vol. 47. No. 10. Pp. 2084–2106. DOI: 10.1109/TSE.2019.2942301.*
6. *Ali M. S., Vecchio M., Pincheira M., Dolui K., Antonelli F., Rehmani M. H. Applications of blockchains in the internet of things: A comprehensive survey // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 2. Pp. 1676–1717. DOI: 10.1109/COMST.2018.2886932.*
7. *Vladucu M. -V., Dong Z., Medina J., Rojas-Cessa R. E-Voting Meets Blockchain: A Survey // IEEE Access. 2023. Vol. 11. Pp. 23293–23308. DOI: 10.1109/ACCESS.2023.3253682.*
8. *Petrenko S., Khismatullina E. Cyber-resilience concept for Industry 4.0 digital platforms in the face of growing cybersecurity threats // Software Technology: Methods and Tools, 51st International Conference, TOOLS 2019, Innopolis, Russia, October 15–17, 2019. 420 p. DOI: 10.1007/978-3-030-29852-4.*
9. *Petrenko A. S., Petrenko S. A. Otsenka kvantovoy ugrozy dlya sovremennykh blokcheyn-sistem // Informatsionnye sistemy i tekhnologii v modelirovanii i upravlenii : Sbornik trudov VII Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Yalta, May 24–25, 2023. Pp. 171–173.*
10. *Petrenko A. S., Lomako A. G., Petrenko S. A. Analiz sovremennogo sostoyaniya issledovaniy problemy kvantovoy ustoychivosti blokcheyna. Chast' 1 // Zashchita informatsii. Insayd. 2023. № 3 (111). Pp. 38–46.*
11. *Petrenko A. S., Petrenko S. A., Kostyukov A. D., Ozhiganova M. I. Model' kvantovykh ugroz bezopasnosti dlya sovremennykh blokcheyn-platform // Zashchita informatsii. Insayd. 2022. № 3 (105). Pp. 10–20.*
12. *Petrenko A. S., Petrenko S. A. Metod otsenivaniya kvantovoy ustoychivosti blokcheyn-platform // Voprosy kiberbezopasnosti. 2022. № 3 (49). Pp. 2–22. DOI 10.21681/2311-3456-2022-3-2-22.*
13. *Lashkari B., Musilek P. A Comprehensive Review of Blockchain Consensus Mechanisms // IEEE Access. 2021. Vol. 9. Pp. 43620–43652. DOI: 10.1109/ACCESS.2021.3065880.*
14. *Xie J., Tang H., Huang T., Yu F., Xie R., Liu J., Liu Y. A survey of blockchain technology applied to smart cities: Research issues and challenges // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 3. Pp. 2794–2830. DOI: 10.1109/COMST.2019.2899617.*
15. *Shahriar M. A. et al. Modelling Attacks in Blockchain Systems using Petri Nets // 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China. 2020. Pp. 1069–1078. DOI: 10.1109/TrustCom50675.2020.00142.*
16. *Younis M. M., Salim Jamil A., Abdulrazzaq A. H., Ahmed Mawla N., Khudhair R. M., Vasiliu Y. Progress and Challenges in Quantum Computing Algorithms for NP-Hard Problems // 2024 36th Conference of Open Innovations Association (FRUCT), Lappeenranta, Finland. 2024. Pp. 460–468. DOI: 10.23919/FRUCT64283.2024.10749878.*
17. *Moldovyan A. A., Moldovyan N. A. Novye formy skrytoy zadachi diskretnogo logarifmirovaniya // Trudy SPIIRAN 2019. No.5. Vol. 18. Pp. 504–529. DOI: 10.15622/sp.18.2.504-529.*

3 Sergei Petrenko, Dr.Sc. (in Tech.) (Grand Doctor, Full Professor), Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Orcid.org/0000- 0003-0644-1731, E-mail: Petrenko.SA@talantiuspeh.ru

4 Artyom Balyabin, Junior Researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, E-mail: Balyabinю.AA@ talantiuspeh.ru

18. *Savo G. Glisic; Beatriz Lorenzo. Quantum Search Algorithms // Artificial Intelligence and Quantum Computing for Advanced Wireless Networks, Wiley. 2022. Pp. 499–542. DOI: 10.1002/9781119790327.ch11.*
19. *Petrenko A. S., Romanchenko A. M. Perspektivnyy metod kriptoanaliza na osnove algoritma Shora // Zashchita informatsii. Insayd. 2020. № 2 (92). Pp. 17–23.*
20. *Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis // Voprosy Kiberbezopasnosti. 2023. No. 1 (53). Pp. 100–115. DOI 10.21681/2311-3456-2023-1-100-115.*
21. *Borges F., Reis P. R., Pereira D. A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography // IEEE Access. 2020. Vol. 8. Pp. 142413–142422. DOI: 10.1109/ACCESS.2020.3013250.*
22. *Kearney J. J., Perez-Delgado C. A. Vulnerability of blockchain technologies to quantum attacks // Array. 2021. Vol. 10. P. 100065. DOI: 10.1016/j.array.2021.100065.*
23. *Kushwaha S. S., Joshi S., Singh D., Kaur M. Lee H. -N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract // IEEE Access. 2022. Vol. 10. Pp. 6605–6621. DOI: 10.1109/ACCESS.2021.3140091.*
24. *Sayeed S., Marco-Gisbert H. Assessing blockchain consensus and security mechanisms against the 51 % attack // Applied Sciences. 2019. Vol. 9. No. 9. P. 1788. DOI: 10.3390/app9091788.*
25. *Fernandez-Carames T. M., Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks // IEEE Access. 2020. Vol. 8. Pp. 21091–21116. DOI: 10.1109/ACCESS.2020.2968985.*
26. *Mollajafari S.; Bechkoum K. Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy // Sustainability 2023. Vol. 15 (18). 13401. DOI: 10.3390/su151813401.*
27. *Al-Shaer R., Spring J. M., Christou E. Learning the Associations of MITRE ATT&CK Adversarial Techniques // 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France. 2020. Pp. 1–9. DOI: 10.1109/CNS48642.2020.9162207.*

STARLINK: ВЫЗОВЫ КИБЕРБЕЗОПАСНОСТИ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СПУТНИКОВОМУ ИНТЕРНЕТУ

Карцан И. Н.[1], Аверьянов В. С.[2], Красников М. Д.[3]

DOI: 10.21681/2311-3456-2025-1-18-27

Цель исследования: *исследование уязвимостей низкоорбитальной спутниковой группировки, а также методы противодействия и нейтрализации угроз, связанных с предоставлением несанкционированного доступа пользователям к сети Internet.*

Метод исследования: *аналитический обзор релевантной научной информации, метод оценки информационной защищённости.*

Результат исследования: *представлен аналитический обзор для проведения оценки помехозащищенности спутниковой группировки Starlink с применением технических параметров Signal-to-Noise Ratio. Выявлены общие уязвимости для серий космических аппаратов Starlink 1.0, Starlink 1.5, Starlink 2.0 и Starlink 2.0 mini. Показано технологическое устройство системы спутникового интернета Starlink, разработанной компанией SpaceX, включая информацию о защите от помех, взлома и кибератак. Рассмотрены методы создания помех с использованием фазового сдвига сигнала, адаптивных радиочастотных помех, когерентных и виртуальных помех, электромагнитных импульсов, рефлекторов и дефлекторов, резонансное рассеивание, а также использование бионических устройств и микродронов. На все рассматриваемые методы представлены как недостатки, так и преимущества. Выявлены методы создания помех с наиболее перспективным подходом.*

Практическая полезность *заключается в том, что на основе анализа методов создания помех предлагаются технические решения по эксплуатации уязвимостей сетевого оборудования и программного обеспечения.*

Ключевые слова: *фазовый сдвиг сигнала, адаптивные радиочастотные помехи, когерентные помехи, виртуальные помехи, электромагнитные импульсы, рефлектора, дефлектора, резонансное рассеивание, бионическое устройство, микродрон.*

Введение

Система спутниковой связи Starlink, от компании SpaceX, представляет собой технологическое решение по обеспечению глобального интернет-покрытия. В отличие от традиционных спутниковых систем, основа Starlink – низкоорбитальные космические аппараты (КА), что позволяет кратно уменьшить временные задержки информативного сигнала и увеличить скорость передачи данных. По мнению разработчика, технология обещает революционизировать доступ к интернету, обеспечив покрытие в удаленных регионах и труднодоступной местности.

Однако, наряду с преимуществами, Starlink вызывает серьезные опасения у ряда стран в области обеспечения национальной безопасности. Массированное развертывание КА на низкой околоземной орбите создает новые предпосылки по утечке конфиденциальной информации, похищенной хакерскими группировками у органов государственной власти, организаций сферы информационных технологий, транспорта, финансов, связи, торговли, здравоохранения, страхования и электронной коммерции [1, 2]. Актуальность исследования обусловлена малой степенью разработанности и исчерпывающих методов противодействия. Авторы ставят перед собой цель восполнить научный пробел, предоставив анализ критических уязвимостей сети связи Starlink, возможных методов перехвата и подмены данных, а также стратегий и тактик противодействия спутниковому интернету.

Рассмотрим текущую ситуацию перехода к фазе 2 на базе космических аппаратов класса Generation 2:

1. переход к спутникам второго поколения (Gen 2) характеризуются улучшенной пропускной способностью и совершенными технологиями связи. КА предназначены для значительного повышения производительности сети Starlink;
2. улучшенные возможности. Спутники Gen 2 обладают повышенной пропускной способностью

1 Карцан Игорь Николаевич, доктор технических наук, доцент, главный научный сотрудник ФГБНУ «Аналитический центр», Москва, Россия. E-mail: kartsan2003@mail.ru, ORCID 0000-0003-1833-4036.

2 Аверьянов Виталий Сергеевич, начальник отдела Информационной безопасности Красноярского краевого клинического онкологического диспансера имени А. И. Крыжановского, Красноярск, Россия. E-mail: averyanov124@mail.ru, ORCID: 0000-0001-6069-2537.

3 Красников Максим Дмитриевич, студент кафедры «БИТ» ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева», Красноярск, Россия. E-mail: maks.krasnikov.76@bk.ru

и улучшенными характеристиками для обеспечения связи, включая технологию Direct to Cell по предоставлению широкополосного доступа в сеть интернет, и услуги мобильной связи для удаленной и труднодоступной местности;

3. масштабируемость сети. Вторая фаза включает в себя увеличение числа низкоорбитальных КА, позволяя обеспечить покрытие при увеличенной пропускной способности каналов связи. В перспективе при растущем спросе на услуги связи общее количество спутников Starlink на орбите кратно возрастёт;
4. запуски и достижения. SpaceX осуществляет регулярные пуски, включая миссии с большим числом спутников на борту. Несмотря на отдельные неудачи, такие как инцидент 11 июля 2024 года, общая тенденция указывает на успешное наращивание орбитальной группировки.

Преимущества и цели фазы 2 и Generation 2:

- расширение глобального покрытия за счет увеличения числа спутников второго поколения, позволяющих обеспечить стабильное и высокоскоростное интернет-подключение в удаленных и малообеспеченных регионах, где традиционная инфраструктура недостаточна;
- увеличение пропускной способности за счет новых спутников, разработанных с учетом возросшего спроса на данные и подключение, что позволит увеличить общее количество пользователей, которым предоставлена услуга;
- улучшение качества связи при технологических улучшениях во второй фазе, что поможет уменьшить задержки и повысить надежность предоставляемых услуг.

В последние месяцы проект Starlink продолжает активно развиваться. SpaceX уже запустила множество спутников на низкую околоземную орбиту, и значительная часть этих спутников оснащена технологией Direct to Cell, позволяющей использовать их как вышки сотовой связи, обеспечивая покрытие в зонах без традиционной инфраструктуры.

Таблица 1.

Общие характеристики КА Starlink 1.0, 1.5, 2.0, 2.0 mini

Характеристика	Starlink 1.0	Starlink 1.5	Starlink 2.0	Starlink 2.0 mini
Масса	~260 кг	~300 кг	~1250 кг	~800 кг
Размер	2.8 м x 1.1 м	2.8 м x 1.1 м	7 м x 2.8 м	4.1 м x 2.7 м
Орбита	550 км	550 км	340-614 км	340-614 км
Пропускная способность	10-20 Гбит/с	20-30 Гбит/с	100-200 Гбит/с	50-100 Гбит/с
Частотный диапазон	Ku, Ka	Ku, Ka	Ku, Ka, E	Ku, Ka
Продолжительность жизни	5-7 лет	5-7 лет	7-10 лет	7-10 лет
Солнечные панели	2 панели (~60 м^2)	2 панели (~60 м^2)	4 панели (~100 м^2)	3 панели (~80 м^2)
Навигация и ориентация	Реактивные колёса, ионный двигатель	Реактивные колёса, ионный двигатель	Реактивные колёса, ионный двигатель	Реактивные колёса, ионный двигатель
Связь	Фазированные антенные решётки	Фазированные антенные решётки	Фазированные антенные решётки	Фазированные антенные решётки
Антенны	1 большая антенна	1 большая антенна	4 антенны	3 антенны
Энергетический потенциал	Средний	Средний	Высокий	Средний
Криптозащита	AES-256	AES-256	AES-256	AES-256
EIRP	23 dBW (200 Вт)	30 dBW (1000 Вт)	40 dBW (10,000 Вт)	35 dBW (3,162 Вт)
Коэффициент усиления антенны (G)	316.23	1000	10000	3162
Расстояние (R)	500000 м			
Температура шума (T)	300 K			

1. Анализ характеристик системы спутниковой связи Starlink

Космические аппараты Starlink представляют собой спутники на низкой околоземной орбите (LEO), разработанные компанией SpaceX для предоставления глобальных услуг широкополосного интернета. В таблице 1 приведены тактико-технические характеристики (ТТХ) спутников Starlink включая необходимую информацию о защите от помех, взлома и кибератак.

Для оценки помехозащищенности КА Starlink применим параметр Signal-to-Noise Ratio (SNR), который показывает отношение мощности полезного сигнала к мощности шума (помех) [3]. Высокое значение SNR указывает на высокую устойчивость к помехам. Формула для расчета SNR:

$$SNR = \frac{P_r}{N}, \quad (1)$$

где P_r – мощность полезного сигнала на приемной антенне, N – мощность шума (помех).

Для проведения анализа используем обозначения:

- EIRP (Effective Isotropic Radiated Power). Мощность, излучаемая спутником, определяется как продукт передаваемой мощности и коэффициента усиления антенны;
- C/N (Carrier-to-Noise ratio). Отношение мощности несущего сигнала к мощности шума;
- G/T (Gain-to-Noise Temperature). Коэффициент, определяющий эффективность антенны приемника относительно температуры шума.

Проведем оценку помехозащищенности для разных версий спутников Starlink после расчетов мощности на приёмнике (P_r):

$$P_r = \frac{EIRP \cdot G}{4\pi R^2}. \quad (2)$$

Расчетов мощности шума (N):

$$N = kTB, \quad (3)$$

где (k) — постоянная Больцмана (1.38×10^{-23}J/K).

Отношение несущей к шуму (C/N):

$$\frac{C}{N_{dB}} = 10 \cdot \log_{10}(\frac{P_r}{N}). \quad (4)$$

Коэффициент усиления к температуре шума (G/T):

$$\frac{G}{T_{dB}} = 10 \cdot \log_{10}(\frac{G}{T}). \quad (5)$$

По полученным результатам проведен следующий анализ:

Starlink 1.0 имеет базовый уровень защиты от высокочастотных помех, делая её уязвимой в условиях высоких плотностей сигнала. Подавление сигнала возможно при наличии помех в том же частотном диапазоне, как в Ku- и Ka- диапазонах. Основные ограничения связаны со слабой антенной и меньшей эквивалентной изотропно излучаемой мощностью (EIRP), что снижает способность поддерживать сильный сигнал при наличии помех;

Starlink 1.5 – улучшенные антенны и управление частотами снижают вероятность помех, однако сигнал всё ещё будет заглушен сильными источниками помех в близлежащих частотах. Увеличенная мощность и улучшенные антенны позволяют значительно улучшить качество связи и устойчивость к помехам;

Starlink 2.0 – существенно улучшена помехозащищенность. Широкий частотный диапазон и мощные антенны позволяют более эффективно управлять спектром и избегать помех. Заглушить сигнал значительно сложнее, требуется более мощный источник помех;

Starlink 2.0 mini – сигнал защищен достаточно хорошо, но из-за меньшей мощности (в сравнении с полной версией 2.0) будет снижение эффективности примерно на 10–15 % в условиях очень сильных помех. Версия mini предназначена для использования в условиях, где размер и вес имеют значение, сохраняя при этом значительную часть функциональности полной версии.

Общие уязвимости.

1. Физическая уязвимость. Возможность кинетических атак или воздействия космического мусора.
2. Зависимость от наземных станций. Атаки на наземные станции управления приводят к потере телеметрической информации.
3. Электромагнитные помехи. Энергетические вспышки на Солнце и других источниках временно ухудшают качество услуг связи.

Эволюция спутников Starlink от версии 1.0 до 2.0 mini показывает значительное улучшение в производительности и устойчивости к помехам. Улучшенные антенны, повышенная EIRP и расширенные частотные диапазоны позволяют справляться с более сложными условиями предоставления услуг связи минимизируя влияние внешних помех. Однако остаются уязвимости, связанные с физическими атаками и электромагнитными помехами, которые необходимо учитывать при разработке и эксплуатации спутниковых систем.

Система спутникового интернета Starlink от компании SpaceX приобрела значительную популярность благодаря своей способности обеспечивать высокоскоростной доступ в интернет в отдаленных и труднодоступных регионах. Однако, наряду с очевидными преимуществами, рост популярности Starlink вызывает обеспокоенность у различных государственных и коммерческих структур по всему миру. В условиях современных геополитических и экономических реалий вопрос контроля над информационными потоками становится особенно актуальным. В связи с этим

возникают предложения по разработке и внедрению методов борьбы с незаконной эксплуатацией системы связи Starlink. Ограничительные меры направлены как на частичное, так и на полное блокирование доступа к её услугам.

Основные методы противодействия включают:

1. методы подавления сигнала [4]. Использование специализированного оборудования для создания помех и блокировки сигнала спутников, что делает невозможным подключение абонентских терминалов к сети;
2. кибератаки [4, 5]. Проведение кибератак на инфраструктуру Starlink с целью выведения из строя отдельных элементов сети и нарушения её функционирования;
3. юридические меры [4, 6]. Принятие законов и нормативных актов, ограничивающих или запрещающих использование спутникового интернета в определенных регионах или для определенных категорий пользователей;
4. физическое уничтожение [7]. Использование противоспутникового оружия для уничтожения КА на орбите.

2. Методы противодействия, их преимущества и недостатки

Рассмотрим несколько инновационных, теоретических методов, которые могли бы быть использованы для создания помех, но при этом они требуют высокой технической сложности и значительных ресурсов [8, 9].

2.1. Фазовый сдвиг

Фазовый сдвиг – это метод, используемый для создания помех в сигнале, поступающем от спутников, изменяя фазу волны, что приводит к искажению информации и ухудшению качества сигнала. Это один из эффективных методов для заглушения или блокировки спутникового интернета, включая системы Starlink. Принцип работы фазового сдвига основан на изменении фазы волны сигнала, что приводит к интерференции. Когда две волны с одинаковой частотой и амплитудой встречаются с разными фазами, они могут создавать зоны усиления и затухания сигнала. Этот принцип лежит в основе фазового сдвига для создания помех.

Для создания фазового сдвига необходимы генератор сигнала создающий сигнал той же частоты, что и целевой сигнал (сигнал спутника Starlink), фазовый модулятор, который изменяет фазу сигнала, созданного генератором, антенна для излучения фазово-сдвинутого сигнала в направлении целевого сигнала.

Основные формулы, связанные с фазовым сдвигом, включают фазовый угол и частотные параметры. Фазовый угол:

$$\Delta\phi = \phi_2 - \phi_1, \quad (6)$$

где $\Delta\phi$ – разница фаз, ϕ_2 и ϕ_1 – фазы двух встречающихся волн.

Фазовая скорость:

$$v_p = \frac{\omega}{k}, \quad (7)$$

где v_p – фазовая скорость, ω – угловая частота, k – волновое число.

Интерференция волн, если две волны с амплитудой A и фазами ϕ_2 и ϕ_1 встречаются, результирующая амплитуда A_r определяется как:

$$A_r = 2A\cos(\frac{\Delta\phi}{2}). \quad (8)$$

Преимущества метода фазового сдвига.

- ✓ Высокая эффективность. Фазовый сдвиг может существенно снизить качество сигнала и сделать интернет-соединение неработоспособным.
- ✓ Точность. Возможность точного управления фазой позволяет нацеливаться на конкретные сигналы и частоты.
- ✓ Гибкость, будет использован в различных условиях и сценариях.

Недостатки.

- ✓ Сложность реализации. Требует точного оборудования и настроек.
- ✓ Высокие затраты. Необходимы значительные финансовые вложения в оборудование и технологии.

2.2. Адаптивные радиочастотные помехи

Адаптивные радиочастотные помехи (АРЧП) представляют собой один из методов противодействия спутниковым системам связи, таким как Starlink. Данный метод направлен на создание помех в радиочастотном диапазоне, в котором работают спутники связи, с целью нарушения их работы [10].

Основные принципы работы АРЧП.

1. Изучение целей. Для успешного подавления систем связи необходимо понимать их технические характеристики, такие как рабочие частоты, тип модуляции, протоколы передачи данных, и режимы работы.
2. Излучение помех. АРЧП подразумевает генерацию и излучение радиосигналов, которые могут создавать помехи в диапазоне частот, используемых целевой системой. Эти помехи могут быть как узкополосными (на определенной частоте), так и широкополосными (охватывающими широкий спектр частот).
3. Адаптивность. АРЧП включает в себя способность адаптироваться к изменениям в работе системы связи. Например, если система изменяет частоту передачи для обхода помех, то генератор помех также должен уметь оперативно изменять свои параметры.

4. Интеллектуальное управление. Современные системы АРЧП используют алгоритмы машинного обучения и искусственного интеллекта для анализа сигнала и динамического формирования помех. Это позволяет более эффективно противодействовать сложным и адаптивным системам связи.

Методы создания радиочастотных помех.

1. Шумовые помехи. Генерация белого шума или шума с определенными характеристиками для заполнения всего частотного диапазона, используемого системой связи.
2. Модулированные помехи. Генерация помех, модулированных аналогично сигналам целевой системы, чтобы затруднить их распознавание и фильтрацию.
3. Направленные помехи. Использование направленных антенн для создания помех в конкретном направлении, минимизируя при этом воздействие на другие системы.
4. Пульсирующие помехи. Создание помех с переменной мощностью и частотой для затруднения их фильтрации и адаптации системы связи к ним.

Для расчета эффективности адаптивных радиочастотных помех (АРЧП) против спутниковых систем связи, таких как Starlink, необходимо учитывать несколько ключевых параметров и использовать определенные формулы.

Основные параметры.

- ✓ Мощность передатчика помех (P_j). Мощность сигнала, генерируемого устройством помех.
- ✓ Мощность сигнала спутника (P_s). Мощность сигнала, передаваемого спутником.
- ✓ Расстояние до спутника (d_s). Расстояние от генератора помех до спутника.
- ✓ Эффективность антенны передатчика помех (G_j). Усиление антенны устройства помех.
- ✓ Эффективность антенны спутника (G_s). Усиление антенны спутника.
- ✓ Полоса частот сигнала (B_s). Ширина полосы частот передаваемого сигнала.
- ✓ Полоса частот помех (B_j). Ширина полосы частот генерируемых помех.
- ✓ Уровень шума на приемнике спутника (N_0). Удельная спектральная плотность мощности шума на приемнике спутника.

Основные формулы. Соотношение сигнал/шум (SNR) на входе приемника спутника:

$$SNR_s = \frac{P_s G_s}{Re\, B_s}. \quad (9)$$

Соотношение помех/сигнал (J/S) на входе приемника спутника:

$$J/S = \frac{P_i G_i}{P_s G_s} \cdot \frac{B_s}{B_j}. \quad (10)$$

Уровень помех на входе приемника спутника:

$$P_{i,s} = \frac{P_i G_i}{(4\pi d_s)^2}. \quad (11)$$

Для успешного подавления сигнала необходимо, чтобы соотношение помех к сигналу (J/S) было больше, чем определенный порог, который зависит от чувствительности приемника спутника.

2.3. Электромагнитные импульсы

Электромагнитный импульс (ЭМИ) представляет мощный выброс электромагнитной энергии, который может вызвать временные или постоянные повреждения электронных систем, включая спутниковые системы связи, такие как Starlink. ЭМИ создается как естественным путем (например, солнечные вспышки), так и искусственно (например, ядерные взрывы или специальные генераторы ЭМИ).

ЭМИ основан на быстром высвобождении энергии, создающем сильное электромагнитное поле. Это поле индуцирует высокие напряжения и токи в проводниках, что может повредить или разрушить электронные компоненты [11].

Ядерный ЭМИ (NEMP) возникает при ядерных взрывах на больших высотах. Образующийся гамма-луч вызывает эмиссию вторичных электронов, что создает интенсивное электромагнитное поле.

Неядерный ЭМИ (NNEMP) будет создан при помощи специальных устройств, таких как генераторы микроволновых импульсов (HPM) или взрывные магниты (FCG).

Основные параметры ЭМИ:

1. амплитуда поля (E). Интенсивность электромагнитного поля, измеряемая в Вольтах на метр (В/м);
2. длительность импульса (τ). Время существования импульса;
3. полоса частот (B). Спектральный диапазон импульса;
4. энергия импульса (W). Общая энергия, высвобождаемая в ходе импульса;
5. расстояние до цели (d). Расстояние от источника ЭМИ до поражаемой цели.

Для получения данных проводится расчет интенсивности поля на заданном расстоянии от источника $E(d) = \frac{E_0}{d}$. Индуцированное напряжение в проводнике длиной L:

$$V = E(d) \cdot L. \quad (12)$$

Индуцированный ток при сопротивлении R:

$$\mathrm{I} = \frac{V}{R} = \frac{E(d) \cdot L}{R}. \quad (13)$$

КА, включая спутники Starlink, уязвимы к ЭМИ из-за своей чувствительной электроники и недостаточной защиты от мощных импульсов. ЭМИ может вызвать следующие эффекты:

1. нарушение работы систем связи и навигации. Временные сбои или постоянное повреждение радиочастотной аппаратуры;
2. повреждение электроники. Выход из строя микропроцессоров, память и другие электронные компоненты;
3. сбой питания. Нарушение работы систем питания, приводящее к отключению спутника.

Защитные меры:

- ✓ Экранирование. Использование защитных экранов и материалов для поглощения или отражения ЭМИ;
- ✓ Фильтрация. Установка фильтров на входах и выходах электронных систем для блокировки высокочастотных импульсов;
- ✓ редундантность систем. Дублирование ключевых систем и компонентов для повышения надежности.

2.4. Рефлекторы и дефлекторы

Рефлекторы и дефлекторы используются для управления направлением электромагнитных волн, таких как сигналы со спутников, в другую сторону. Такие устройства могут быть полезны для защиты от нежелательных сигналов или для манипуляции сигналами связи [12]. Рассмотрим использование дронов и наземных устройств с отражающими или отклоняющими поверхностями.

Основные концепции рефлекторов и дефлекторов.

- ✓ Рефлекторы отражают электромагнитные волны. Они могут быть пассивными (не требуют внешнего питания) или активными (используют внешнее питание для усиления или изменения характеристик сигнала).
- ✓ Дефлекторы отклоняют направление распространения электромагнитных волн без полного отражения. Фазированные решетки (используют множество элементов антенн, фазировка которых позволяет изменять направление излучаемого сигнала). Диэлектрические призмы (применяют изменения показателя преломления для отклонения сигнала).

Для использования рефлекторов и дефлекторов могут быть использованы как дроны, так и наземные устройства.

Дроны могут нести на себе отражающие или отклоняющие поверхности для манипуляции сигналами спутников. Такие дроны могут быть использованы в ситуациях, где необходимо быстро и гибко изменить направление сигнала.

Наземные устройства могут быть более мощными и долговечными по сравнению с дронами и использоваться для постоянного отклонения или отражения сигналов.

Преимущества:

- ✓ Гибкость. Возможность быстрой настройки и перенастройки направления сигнала;
- ✓ Мобильность. Дроны могут перемещаться, обеспечивая адаптивное управление сигналом;
- ✓ Масштабируемость. Возможность использования нескольких устройств для увеличения зоны покрытия.

Недостатки:

- ✓ Энергозатраты. Дроны требуют энергии для полета и управления рефлекторами/дефлекторами;
- ✓ точность позиционирования. Необходимо точное управление дронами для эффективного отражения/отклонения сигналов;
- ✓ сложность конструкции. Фазированные решетки и другие сложные устройства требуют точной настройки и калибровки.

2.5. Резонансное рассеяние

Резонансное рассеяние – это явление, при котором электромагнитные волны (свет, радиоволны и т.д.) взаимодействуют с частицами, атомами или молекулами таким образом, что происходит их эффективное рассеяние. В контексте борьбы с спутниковыми системами связи, такими как Starlink, резонансное рассеяние будет использовано для создания помех или отклонения сигналов. Рассмотрим, как это работает и как можно применить данное явление на практике.

Резонансное рассеяние возникает, когда частота электромагнитного волнового сигнала совпадает с собственной частотой колебаний частиц или молекул в материале. Это вызывает сильное взаимодействие и приводит к эффективному рассеянию волны. При применении резонансного рассеивания в спутниковых системах связи используются устройства и материалы, которые резонируют на частотах, используемых спутниками [13].

Преимущества:

- ✓ Точность. Резонансное рассеяние позволяет точно настраивать взаимодействие с сигналами на заданных частотах;
- ✓ Эффективность. Высокая эффективность рассеяния на резонансных частотах;
- ✓ Гибкость. Возможность создания метаматериалов и резонаторов с нужными характеристиками.

Недостатки:

- ✓ сложность разработки. Создание метаматериалов и резонаторов требует сложных технологий и точного проектирования;
- ✓ ограниченность диапазона. Резонансное рассеяние эффективно на узком диапазоне частот, что требует точной настройки под конкретные задачи;
- ✓ Стоимость. Высокая стоимость материалов и технологий.

2.6. Когерентные помехи

Когерентные помехи создаются путем генерации сигнала с теми же характеристиками (частота, фаза, амплитуда), что и целевой сигнал, но с измененными параметрами для создания интерференции. В результате целевой сигнал становится искаженным или подавленным. Когерентные помехи работают на основе принципа интерференции, где два сигнала с одинаковыми частотами и фазами могут складываться, образуя конструктивную или деструктивную интерференцию [14].

Когерентные помехи могут быть использованы для создания помех спутниковым сигналам, направленным на приемные станции или терминалы пользователей.

Преимущества:

- ✓ высокая эффективность. Возможность точного подавления целевого сигнала;
- ✓ Адаптивность. Возможность изменения параметров сигнала помех в реальном времени для поддержания интерференции.

Недостатки:

- ✓ точность синхронизации. Необходимость точной синхронизации по частоте и фазе с целевым сигналом;
- ✓ сложность реализации. Требуются сложные технологии для создания и поддержания когерентных помех;
- ✓ Контрмеры. Спутники и приемные станции могут использовать методы для защиты от когерентных помех, такие как изменение частот или фазирование сигналов.

2.7. Бионические устройства и микродроны для создания помех

Бионические устройства и микродроны – это малые, высокотехнологичные устройства, которые могут перемещаться в атмосфере и создавать помехи на микроскопическом уровне [15]. Такие устройства могут использоваться для различных целей, включая создание помех спутниковым системам связи, таким как Starlink.

Бионические устройства используют принципы биологии и инженерии для выполнения определенных задач. Они могут включать в себя элементы, которые имитируют природные системы, такие как крылья насекомых для полета.

Микродроны – это миниатюрные летательные аппараты, которые могут быть оснащены различными сенсорами и средствами связи для выполнения специфических задач. Они могут летать в воздухе, перемещаться в тесных пространствах и создавать целенаправленные помехи.

Варианты создания помех спутниковой связи:

1. запуск микродронов. Несколько микродронов запускаются вблизи целевой зоны;
2. Синхронизация. Дроны синхронизируются для создания когерентных РЧ-помех на частоте спутникового сигнала;
3. создание помех. Передатчики на дронах начинают генерировать помехи, вызывая интерференцию с целевым сигналом;
4. ЭМИ-атака. Некоторые дроны запускают ЭМИ для временного выведения из строя приемного оборудования;
5. оптические помехи. Дроны с лазерами нацеливаются на оптические сенсоры спутников для создания засветки и помех.

Преимущества:

- ✓ Мобильность. Микродроны могут перемещаться в различные точки для создания локализованных помех;
- ✓ Незаметность. Малый размер и способность к маневрированию делают их трудными для обнаружения и нейтрализации;
- ✓ Адаптивность. Микродроны могут быстро адаптироваться к изменениям в окружающей среде и задачах.

Недостатки:

- ✓ Энергозависимость. Ограниченное время полета из-за небольших размеров и емкости батарей;
- ✓ комплексность управления. Требуется высокоточная система управления и координации для эффективной работы;
- ✓ Контрмеры. Возможность разработки технологий для обнаружения и нейтрализации микродронов.

2.8. Виртуальные помехи

Виртуальные помехи включают использование программных методов для создания помех или искажения работы приемных устройств [16, 17]. Это будет достигнуто через хакерские атаки, внедрение вредоносного программного обеспечения (ПО), манипуляции с программным обеспечением, работающим на приемных устройствах, или через сетевые атаки, направленные на инфраструктуру спутниковой связи.

Хакерские атаки направлены на уязвимости в программном обеспечении приемных устройств или сетевой инфраструктуры спутниковых систем. Они могут включать:

- ✓ Взлом. Получение несанкционированного доступа к системам;
- ✓ DoS/DDoS атаки. Атаки отказа в обслуживании, которые перегружают систему и делают её недоступной;
- ✓ MITM атаки. Атаки типа «человек посередине», перехват и изменение данных в реальном времени.

Вредоносное ПО (malware) будет использовано для создания помех или искажения работы приемных устройств. Это будет достигнуто через:

- ✓ Трояны. Программы, скрывающиеся под видом легитимного ПО;
- ✓ Вирусы. Программы, которые распространяются и внедряются в другие программы;
- ✓ Черви. Самовоспроизводящиеся программы, распространяющиеся через сеть.

Вариант алгоритма атаки на систему спутниковой связи:

1. Разведка. Хакеры проводят разведку для выявления уязвимых систем и приемных устройств;
2. Фишинг. Рассылка фишинговых писем с целью получения данных доступа к административным панелям;
3. внедрение вредоносного ПО. Использование полученных данных для установки вредоносного ПО на приемные устройства;
4. создание помех. Вредоносное ПО изменяет параметры обработки сигналов, создавая помехи;
5. удаленный контроль. Установка бэкдоров для возможности дальнейших манипуляций и атак.

Преимущества:

- ✓ Скрытность. Трудно обнаружить программные атаки, особенно если они хорошо замаскированы;
- ✓ Удаленность. Возможность проведения атак из любой точки мира;
- ✓ Гибкость. Атаки могут быть адаптированы и изменены в зависимости от ситуации.

Недостатки:

- ✓ техническая сложность. Требуется высокий уровень технической экспертизы;
- ✓ законодательные ограничения. Проведение таких атак может нарушать законы и международные соглашения;
- ✓ риски обнаружения. Если атака будет обнаружена, это может привести к серьезным последствиям.

Выводы

Исследование содержит всестороннюю оценку методов по созданию паразитных помех спутниковой системы связи Starlink. Каждый из предложенных методов проанализирован с точки зрения технической реализуемости, эффективности и потенциальных последствий. Особое внимание уделено бионическим устройствам и микродронам, а также виртуальным помехам, так как они представляют наиболее перспективные подходы, однако и другие методы имеют свои достоинства и могут быть успешно применены в комбинации.

Методы создания помех можно условно разделить на несколько категорий: физические, электронные и кибермеотоды. Каждый из них обладает своими уникальными характеристиками и требует специфических технических средств и условий для реализации.

Физические методы включают в себя использование дронов, лазеров и других устройств для прямого вмешательства в работу спутников. Применение дронов для создания помех позволяет осуществлять мобильные и точные атаки на спутниковую связь. Лазеры могут быть использованы для ослепления оптических сенсоров спутников, что приведет к временной потере связи.

Электронные методы создания помех основаны на использовании радиочастотных генераторов и других электронных устройств. Эти методы позволяют создавать когерентные и некогерентные помехи, которые значительно ухудшают качество связи. Применение низкочастотных генераторов и микродронов, оснащенных передатчиками, предоставляет возможность для широкомасштабного воздействия на спутниковую систему.

Кибермеотоды включают в себя использование вредоносного программного обеспечения, фишинг и атаки на программное обеспечение. Эти методы направлены на нарушение работы наземных станций управления и приемных устройств, что может привести к потере контроля над спутниками или снижению качества передачи данных.

В целом, работа демонстрирует, что создание помех спутниковой системе Starlink вполне возможно реализовать различными способами. Однако каждый из предложенных методов требует детальной проработки и учета всех возможных последствий, как технических, так и правовых. Комплексный подход, сочетающий различные методы, представляется наиболее эффективным для достижения поставленных целей.

Литература

1. *Рябов А. В., Алексеев А. Е. Направления повышения помехоустойчивости систем радиосвязи // Охрана, безопасность, связь. 2022, № 7-1, с. 117–122.*
2. *Яковишин А., Кузнецов И., Дроздов И., Письменский Д. Перспективы развития информационной безопасности: глобальные вызовы и стратегии защиты // Информационные ресурсы России. 2024, № 2 (197), с. 93–103. DOI: 10.52815/0204-3653_2024_2197_93*
3. *Карцан И. Н., Кобозев Д. С. Аспекты безопасности спутниковой связи // Естественные и технические науки. 2024, № 6 (193), с. 310–312.*

4. Пашаев Ф. Г., Зейналов Д. И., Наджафов Г. Т. Разработка программно-технических средств защиты технологических процессов от киберугроз // Проблемы информационной безопасности. Компьютерные системы. 2024, № 2 (59), с. 104-116. DOI: 10.48612/jisp/p79a-z1nu-71vk
5. Никифоров И. А. Роль искусственного интеллекта в кибербезопасности // Сборник научных трудов вузов России «Проблемы экономики, финансов и управления производством». 2024, № 54, с. 230–237.
6. Логинов Е. А. Роль и значимость искусственного интеллекта в обеспечении информационной безопасности // Научный аспект. 2024, Т. 21, № 5, с. 2805–2809.
7. Аверьянов В. С., Карцан И. Н. Методы оценки защищенности автоматизированных систем на базе квантовых технологий согласно CVSS V2.0/V3.1 // Защита информации. Инсайд. 2023, № 1 (109), с. 18–23.
8. Данилюк А. И., Гладких Д. С., Мельник В. Н., Полищук В. Р. Факторы, оказывающие воздействие на системы связи в условиях боевых действий // Тенденции развития науки и образования. 2024, № 107-9, с. 167–170. DOI: 10.18411/trnio-03-2024-489
9. Ромащенко М. А., Васильченко Д. В., Белецкая С. Ю. Использование искусственных нейронных сетей для оценки воздействия электромагнитных помех // Радиотехника. 2023, Т. 87, № 8, с. 21–27. DOI: 10.18127/j00338486-202308-04
10. Дементьев А. Н., Новиков А. Н., Арсеньев К. В., Куркин А. Н., Жуков А. О., Карцан И. Н. Метод обработки сигналов в адаптивной антенной решетке // Южно-Сибирский научный вестник. 2023, № 4 (50), с. 60–63. DOI: 10.25699/SSSB.2023.50.4.009
11. Zhang D., Cheng E., Wan H., Zhou X., Chen Y. Prediction of Electromagnetic Compatibility for Dynamic Datalink of UAV // IEEE Transactions on Electromagnetic Compatibility. 2019, Vol. 61, № 5, pp. 1474–1482. DOI:10.1109/TEMC.2018.2867641
12. Петренко А. С., Петренко С. А., Ожиганова М. И. О киберустойчивости и безопасности изобразительных нейросетей // Защита информации. Инсайд. 2023, № 6 (114), с. 50–54.
13. Ожиганова М. И. Архитектура безопасности киберфизической системы // Защита информации. Инсайд. 2022, № 2 (104), с. 5–9.
14. Ожиганова М. И., Калита А. О. Анализ и применение алгоритмов машинного обучения для идентификации вредоносного программного кода // Информатизация и связь. 2019, № 5, с. 51–56.
15. Калита А. О., Ожиганова М. И., Тищенко Е. Н. Основы организации адаптивных систем защиты информации // НБИ технологии. 2019, Т. 13, № 1, с. 11–15. DOI: 10.15688/NBIT.jvolsu.2019.1.2.
16. Ромащенко М. А., Васильченко Д. В., Пухов Д. А. Современное состояние задач повышение помехоустойчивости канала управления беспилотных авиационных систем на основе искусственного интеллекта // Вестник Воронежского государственного технического университета. 2023, Т. 19, № 6, с. 142–146. DOI: 10.36622/VSTU.2023.19.6.022
17. Zhang R., Cui J. Application of Convolutional Neural Network in multi-channel Scenario D2D Communication Transmitting Power Control // 2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL), Chongqing, China, 2020, pp. 668–672. DOI:10.1109/CVIDL51233.2020.000-3

STARLINK: CYBERSECURITY CHALLENGES AND COUNTERMEASURES FOR THE SATELLITE INTERNET

Kartsan I. N.[4], Averyanov V. S.[5], Krasnikov M. D.[6]

Keywords: *signal phase shift, adaptive RF interference, coherent interference, virtual interference, electromagnetic pulses, reflector, deflector, resonant scattering, bionic device, microdrone.*

Purpose of the research: *investigation of vulnerabilities of low-orbit satellite constellation, as well as methods of counteraction and neutralization of threats related to providing unauthorized access to the Internet to users.*

Research method: *analytical review of relevant scientific information, information security assessment method.*

Research result: *the analytical review is presented to assess the interference immunity of the Starlink satellite constellation using Signal-to-Noise Ratio technical parameters. Common vulnerabilities for the Starlink 1.0, Starlink 1.5, Starlink 2.0 and Starlink 2.0 mini-series of spacecraft are identified. The technological design of the Starlink satellite Internet system developed by SpaceX is shown, including information on defenses against jamming, hacking, and cyberattacks. Interference techniques utilizing signal phase shifting, adaptive RF interference, coherent and virtual interference, electromagnetic pulses, reflectors and deflectors, resonant scattering, and the use of bionic devices and microdrones are discussed. Both disadvantages and advantages are presented for all the methods considered. Interference techniques with the most promising approach are identified.*

Practical usefulness *lies in the fact that, based on the analysis of interference techniques, technical solutions for exploiting vulnerabilities in network hardware and software are proposed.*

References

1. Ryabov A. V., Alekseev A. E. Directions of increasing the immunity of radio communication systems // Safety, security, communications. 2022, № 7-1, s. 117–122.
2. Yakovishin A., Kuznetsov I., Drozdov I., Pismensky D. Perspectives of information security development: global challenges and protection strategies // Information Resources of Russia. 2024, № 2 (197), s. 93–103. DOI: 10.52815/0204-3653_2024_2197_93

4 Igor N. Kartsan, Dr.Sc., Associate Professor, Chief Scientist Analytical Center, Moscow, Russia, E-mail: kartsan2003@mail.ru, ORCID 0000-0003-1833-4036.
5 Vitaliy S. Averyanov, Head of Information Security Department, Krasnoyarsk Regional Clinical Oncologic Dispensary named after A.I. Kryzhanovsky, Krasnoyarsk, Russia. E-mail: averyanov124@mail.ru, ORCID: 0000-0001-6069-2537.
6 Maksim D. Krasnikov, student of the BIT Department, FSBEI VO «Siberian State University of Science and Technology named after Academician M.F. Reshetnev», Krasnoyarsk, Russia. E-mail: maks.krasnikov.76@bk.ru

3. *Kartsan I. N., Kobozev D. S. Aspects of satellite communication security // Natural and Technical Sciences. 2024, № 6 (193), s. 310–312.*
4. *Pashayev F. G., Zeynalov D. I., Najafov G. T. Development of software and hardware means of protection of technological processes from cyber threats // Problems of information security. Computer Systems. 2024, № 2 (59), s. 104–116. DOI: 10.48612/jisp/p79a-z1nu-71vk*
5. *Nikiforov I. A. The role of artificial intelligence in cyber security // Collection of scientific papers of Russian universities «Problems of economics, finance and production management». 2024, № 54, s. 230–237.*
6. *Loginov E. A. The role and significance of artificial intelligence in ensuring information security // Scientific Aspect. 2024, Vol. 21, No. 5, s. 2805–2809.*
7. *Averyanov V. S., Kartsan I. N. Methods of evaluation of automated systems security on the basis of quantum technologies according to CVSS V2.0/V3.1 // Zashhita informacii. Insajd. 2023, № 1 (109), s. 18–23.*
8. *Danilyuk A. I., Gladkikh D. S., Melnyk V. N., Polishchuk V. R. Factors affecting the communication systems under combat conditions // Tendencies of Science and Education Development. 2024, № 107-9, s. 167–170. DOI: 10.18411/trnio-03-2024-489*
9. *Romashchenko M. A., Vasilchenko D. V., Beletskaya S. Yu. Using artificial neural networks to assess the impact of electromagnetic interference // Radiotekhnika. 2023, Vol. 87, No. 8, s. 21–27. DOI: 10.18127/j00338486-202308-04*
10. *Dementiev A. N., Novikov A. N., Arseniev K. V., Kurkin A. N., Zhukov A. O., Kartsan I. N. Signal processing method in the adaptive antenna array // South Siberian Scientific Bulletin. 2023, № 4 (50), c. 60–63. DOI: 10.25699/SSSB.2023.50.4.009*
11. *Zhang D., Cheng E., Wan H., Zhou X., Chen Y. Prediction of Electromagnetic Compatibility for Dynamic Datalink of UAV // IEEE Transactions on Electromagnetic Compatibility. 2019, Vol. 61, № 5, pp. 1474–1482. DOI:10.1109/TEMC.2018.2867641*
12. *Petrenko A. S., Petrenko S. A., Ozhiganova M. I. About cyber resistance and security of image neural networks // Zashhita informacii. Insajd. 2023, № 6 (114), s. 50–54.*
13. *Ozhiganova M. I. Security architecture of cyber-physical system // Zashhita informacii. Insajd. 2022, № 2 (104), s. 5–9.*
14. *Ozhiganova M. I., Kalita A. O. Analysis and application of machine learning algorithms for identification of malicious software code // Informatization and communication. 2019, № 5, s. 51–56.*
15. *Kalita A. O., Ozhiganova M. I., Tishchenko E. N. Fundamentals of organization of adaptive information protection systems // NBI Technologies. 2019, Vol. 13, No. 1, s. 11–15. DOI: 10.15688/NBIT.jvolsu.2019.1.2*
16. *Romashchenko M. A., Vasilchenko D. V., Pukhov D. A. Current state of the problems of improving noise immunity of the control channel of unmanned aircraft systems based on artificial intelligence // Bulletin of Voronezh State Technical University. 2023, Vol. 19, No. 6, s. 142–146. DOI: 10.36622/VSTU.2023.19.6.022*
17. *Zhang R., Cui J. Application of Convolutional Neural Network in multi-channel Scenario D2D Communication Transmitting Power Control // 2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL), Chongqing, China, 2020, pp. 668–672. DOI:10.1109/CVIDL51233.2020.000-3*

МЕТОДИКА ВЫБОРА ЭФФЕКТИВНЫХ КОНТРМЕР ДЛЯ ПОВЫШЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Басан Е. С.[1], Силин О. И.[2], Фирсова М. Г.[3]

DOI: 10.21681/2311-3456-2025-1-28-40

Цель работы *состоит в разработке методики повышения отказоустойчивости киберфизической системы за счет применения контрмер в зависимости от выявленных угроз при воздействии на нее атак.*

Метод исследования: *разрабатываемая методика строится на основе концептуальной модели, которая описывает киберфизические параметры и структурно-функциональные характеристики системы, а также позволяет определить актуальные угрозы, влияющие на киберфизическую систему. Методика формально описывает угрозы, представляющие опасность для киберфизических систем, оценивает риски этих угроз и предлагает эффективные контрмеры для снижения риска возникновения угроз. Для иерархического представления знаний о киберфизических параметрах и угрозах используется онтологических подход. Онтология позволяет описать соотношение воздействующих на структурно-функциональные характеристики угроз, а также выявить контрмеры, которые способствуют минимизации рисков информационной безопасности.*

Результаты исследования: *разработана методика, которая на основе анализа структурно-функциональных характеристик системы и их критичности позволяет выявить актуальные угрозы и подобрать эффективные контрмеры для их минимизации. Проведен анализ основных параметров киберфизических систем, составлена концептуальная модель, которая позволяет описать структуру киберфизической системы. В результате анализа основных параметров киберфизических систем были определены такие, которые наиболее подвержены кибератакам. Также был создан перечень контрмер, которые позволяют минимизировать риски безопасности, что повышает отказоустойчивость киберфизической системы. Итогом работы является перечень атак, которые являются актуальными для киберфизических систем, а также ряд контрмер, которые позволяют минимизировать выявленные кибератаки, при этом контрмеры разделены на три категории.*

Научная новизна: *применение онтологического подхода для описания киберфизических параметров и структурно-функциональных характеристик киберфизической системы, что позволило выявить наиболее подверженные атакам и оценить риски безопасности.*

Ключевые слова: *интернет вещей, сенсоры, кибератака, угрозы, уязвимости, структурно-функциональные характеристики, средства передачи данных, меры противодействия, инцидент.*

Введение

Киберфизическая система (КФС) представляет собой взаимосвязь физических и программных компонентов, которые управляются и контролируются компьютерными алгоритмами. В архитектуру КФС входят сенсоры, микроконтроллеры, инструменты обработки данных, средства передачи данных и интерфейс пользователя. При этом КФС подвержены широкому спектру кибератак. Существует шесть классов кибератак, которым подвержены КФС и их компоненты, а именно: глушение каналов передачи данных, перехват сообщений, удаление сообщений, внедрение сообщений, подделка сообщений и атака на контроллеры системы. Всесторонний обзор мер противодействия важен, поскольку меры противодействия могут не ограничиваться конкретным перечнем атак. Знание широкого спектра существующих контрмер может подготовить систему и к существующим, и к новым кибератакам.

Рассмотрим существующие методы и методики анализа угроз КФС и Интернета вещей.

Авторами статьи [1] делается попытка выделить известные угрозы на разных уровнях архитектуры Интернета вещей (Internet of Things – IoT) с учетом возможности реализации атак. Авторы представляют развернутую методологию реализации атак на IoT, а также необходимые меры повышения информационной безопасности. Авторы предлагают руководство по разработке методологии обеспечения безопасности IoT на основе отраслевых документов, которая включает в себя оценку рисков, применение

1 Басан Елена Сергеевна, кандидат технических наук, доцент кафедры Безопасности информационных технологий им. О. Б. Макаревича Института компьютерных технологий и информационной безопасности Южного федерального университета, г. Таганрог, Россия. E-mail: ebasan@sfedu.ru

2 Силин Олег Игоревич, ассистент кафедры Безопасности информационных технологий им. О. Б. Макаревича Института компьютерных технологий и информационной безопасности Южного федерального университета, г. Таганрог, Россия. E-mail: silin@sfedu.ru

3 Фирсова Мария Геннадьевна, ассистент кафедры Безопасности информационных технологий им. О. Б. Макаревича Института компьютерных технологий и информационной безопасности Южного федерального университета, г. Таганрог, Россия. E-mail: mshulika@sfedu.ru

средств информационной безопасности, повышающих конфиденциальность, целостность и доступность системы, а также метод расчета рисков. Основная цель оценки состоит в том, чтобы определить все инциденты безопасности, которые могут произойти в организации, и впоследствии инициировать процесс обработки риска, чтобы минимизировать ущерб от таких событий. Отсутствие автоматизации процесса в данном случае является серьезным недостатком. Кроме того, при оценке не учитываются риски, связанные с объектом, которым «управляет» Интернет вещей.

Авторы [2] рассматривают различные подходы применения онтологического инжиниринга для Интернета вещей и его необходимость. Авторы отметили, что вопросы интеграции онтологий для обеспечения безопасности Интернета вещей обсуждаются в научных работах многих авторов. В одной из рассмотренных авторами работ была предложена распределенная система на основе онтологии для удовлетворения требований конфиденциальности учреждений здравоохранения. Также в статье говорится, что сегодня существуют различные онтологические модели для распознавания угроз в системе Интернета вещей. Описанный инструмент IoTChecker для определения аномалий в конфигурациях безопасности Интернета вещей использует несколько онтологий Интернета вещей для распознавания угроз.

Также в разных странах существуют нормативные документы, которые могут применяться для анализа угроз и формирования мер противодействия для КФС.

В [3] авторы исследовали использование КФС в качестве агентов при проведении кибератак. В некоторых из этих сценариев атак КФС сначала должна стать целью атаки для захвата, прежде чем взятую под контроль КФС можно будет превратить в агента атаки. При этом атака может быть совершена не только в киберпространстве, но и на физическом уровне. В работе также представлен ряд контрмер для предотвращения выявленных атак. Некоторые из этих контрмер включают в себя физические механизмы.

Акцентируя внимание на мониторинге безопасности КФС, авторы [4] предлагают подход корреляции событий безопасности в КФС на основе генерации графов. Подход состоит из четырех этапов: предварительная обработка данных, анализ сходства событий, генерация графа и классификация узлов. Подход предполагает проведение семи видов атак, а затем дальнейший анализ событий безопасности. Для анализа сходства событий используется алгоритм BIRCH (сбалансированное итеративное сокращение и кластеризация с использованием иерархий), который позволяет выполнять иерархическую кластеризацию на больших наборах данных. Затем формируется RSE-график, который может отображать взаимосвязь между репрезентативными событиями. В итоге узлы графа классифицируются с помощью сверточных нейронных сетей графа (GCN), которые учитывают локальную окрестность узла в графе для составления прогнозов. Экспериментальная часть показала, что подход может быть использован для построения графа репрезентативных событий безопасности и обнаружения состояний безопасности, что впоследствии поможет при прогнозировании рисков безопасности системы.

В работе [5] автор рассматривает технологии кибербезопасности для КФС и фреймворки управления рисками. Обзор существующих подходов управления рисками кибербезопасности показал, что ни один из фреймворков явно не рассматривает экосистему безопасности КФС, существует лишь несколько исследований, применяющих количественную оценку к кибератакам и их последствиям. Именно это, по мнению автора, должно нас мотивировать на разработку структуры методики обеспечения кибербезопасности, управления и минимизации рисков КФС, которая улучшает существующие подходы.

Необходимо отметить, что большинство исследований на сегодняшний день являются теоретическими, учеными только делаются попытки изучения и выявления общих принципов обеспечения безопасности КФС и определения угроз и требований по безопасности, характерных для такой инфраструктуры.

В данной работе представлены две разработанные методики для анализа безопасности КФС: методика оценки рисков безопасности и методика выбора эффективных контрмер, приведены примеры их применения.

1. Методики оценки рисков безопасности киберфизических систем

Первым этапом при выборе контрмер для обеспечения безопасности и повышения отказоустойчивости КФС является выявление и оценка рисков безопасности системы. Рассмотрим существующие схемы диагностики инцидентов безопасности и проактивную методику оценки рисков, а также опишем разработанную в данном исследовании методику оценки рисков для КФС на основе вышесказанного.

1.1. Диагностика инцидентов безопасности для киберфизических систем

Схема диагностики состоит из нескольких шагов. Причинно-следственная связь первого типа использует знания предметной области о взаимодействиях компонентов системы для выявления потенциальных причин. Наличие списка потенциальных причин дает больше шансов обнаружить подозрительные

события. На втором этапе идет анализ следов с целью обнаружения потенциальных причин. Однако после второго этапа нельзя точно утверждать, какая из обнаруженных причин является действительной. В результате на третьем этапе требуется анализ фактической причинности, чтобы различать актуальные и неактуальные причины. Для диагностики КФС необходимо сначала описать взаимодействия между его программным обеспечением и физическими компонентами [6].

Продемонстрируем работу предлагаемой схемы диагностики на экспериментальном образце беспилотной автоматизированной системы (БАС). Атака на систему Global Positioning System (GPS) приводит к ложному показанию GPS БАС и потери координат местоположения. Применение схемы заключается в поэтапном анализе данных обратной связи БАС. Также атака может вывести GPS систему из строя, что можно понять по анализу показаний данной системы. К таким показаниям чаще всего относится высота полета БАС (рис. 1).

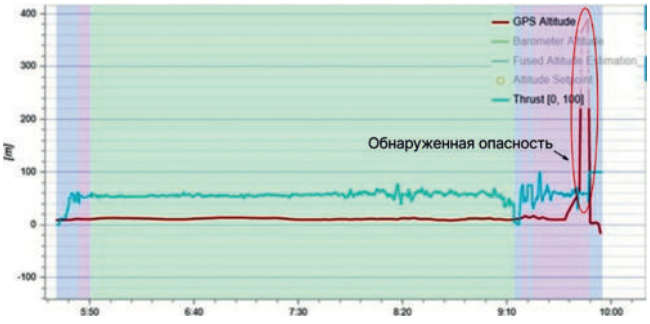


Рис. 1. Показания высоты полета БАС при проведенной атаке

Изучив график, можно сделать вывод, что после проведения атаки на GPS систему, начинают колебаться показания высоты и оборотов, далее по показаниям системы GPS выделяется резкий набор высоты, хотя фактически БАС не набирает ее, а остается на прежней высоте, что можно понять, просмотрев показания оборотов двигателей.

Также эта атака может вывести GPS-систему из строя, что тоже можно понять по данным от системы (рис. 2).

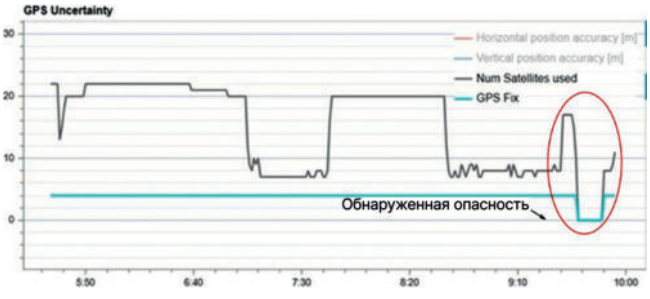


Рис. 2. Показания GPS системы

На графике серой линией обозначено количество используемых GPS спутников, синей линией соответственно их сопряженность с системой БАС. Проанализировав график, можно сделать вывод о том, что после атаки на GPS-систему количество используемых спутников начало изменяться в отрицательном и положительном направлении, в итоге на некоторое время сравнялось с нулем, тем самым БАС потерял фиксацию и вышел из строя на некоторый промежуток времени, за счет чего наблюдалось ошибочное показание системы GPS.

1.2. Проактивная методика оценки риска

В предлагаемой методике оценивается риск нарушения безопасности на основе компонентных моделей. Соответственно, общая оценка риска системы в целом является суммированием оценок риска ее компонентов. Схема предоставляет информацию о подверженности компонентов атакам на целостность, конфиденциальность или доступность компонента. В зависимости от уровня восприимчивости для каждой атаки каждому компоненту присваиваются значения от 0 до 1 (0 означает «не восприимчив», 1 соответствует «высоко восприимчив»). Для расчета риска удельные вероятности возникновения атаки умножаются на значение восприимчивости. Результат оценки риска по представленной схеме является многомерным [7]. В соответствии с общей задачей разные аспекты безопасности играют разные роли и должны быть соответствующим образом взвешены.

Рассмотрим результаты применения описанной методики на экспериментальном образце БАС. Базовая конфигурация оборудования включает в себя одну беспроводную линию связи, совместимую с IEEE 802.11b/g, пульт управления, всенаправленную антенну, связь не шифруется. Также БАС содержит одну камеру, не имеет носителей информации, использует инерциальную навигационную систему в качестве сенсорного оборудования, механизм обработки ошибок включает в себя только «режим экстренной посадки». Рассмотрим результаты оценки рисков для каждого компонента системы по свойствам целостности, конфиденциальности и доступности (табл. 1), которые получены в соответствии с рассмотренной методикой.

Результаты применения методики к данному БАС обоснованы использованием двух диапазонов связи (C-диапазона и Wi-Fi-b соответственно), наличием камеры, не участвующей в системе позиционирования. Также используется энергозависимое хранилище, потенциально приводящее к риску целостности и доступности. Механизм обработки ошибок включает в себя только экстренную посадку, в остальных случаях пилот должен справляться с неисправностями вручную.

Таблица 1.

Результаты оценки риска для прототипа БАС

Составная часть	Целостность	Конфиденциальность	Доступность
Система связи	1,1	2,3	1,5
Хранилище данных	0,9	0	0,9
Датчики	3,6	0	1,8
Обработка ошибок	0,9	0,9	0,9
Общий итог	6,5	3,2	5,1
Система связи	1,1	2,3	1,5

1.3. Разработка методики оценки риска для киберфизических систем

Разработанная в данном исследовании методика представляет собой схематично описанную цепочку последовательностей воздействия конкретной группы атак на киберфизические параметры (КФП) системы, неверные показания которых могут привести к определенным последствиям.

Пользователь выбирает определенную группу атак из следующих: получение доступа, подделка, отказ в обслуживании, атаки на целостность. После этого по онтологической схеме (рис. 3) определяется влияние этой группы на КФП, затем на основе выбранных КФП выбираются структурно-функциональные характеристики (СФХ), которые они составляют. При выборе характеристик схема определяет перечень предстоящих последствий в случае неисправности этих систем. Затем определяется вероятность того, что каждое воздействие повлияет на три основных параметра. Таким образом, с помощью схемы можно

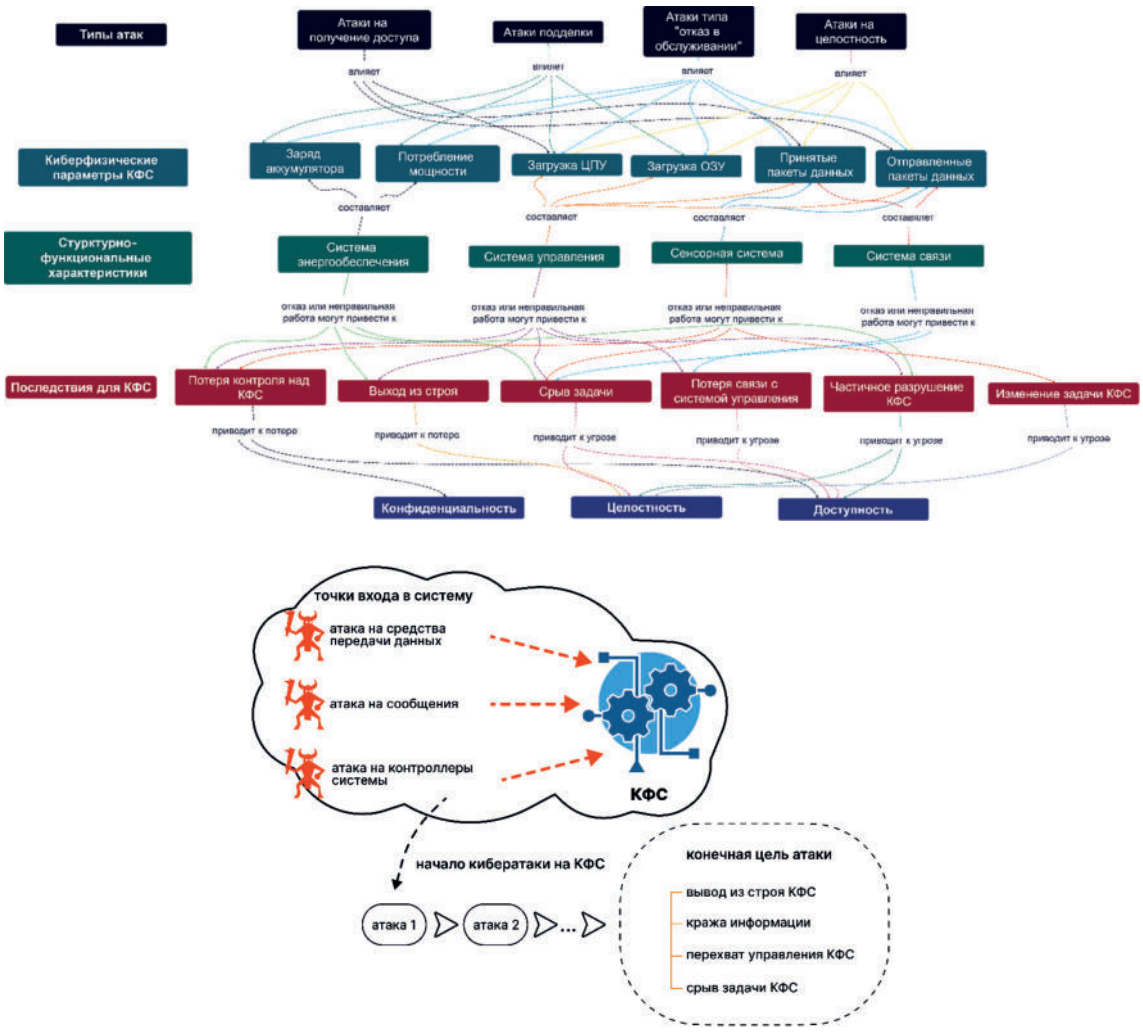


Рис. 3. Методика оценки рисков

Таблица 2.

Методика оценки рисков

Параметр	Обозначение	Формула	Результат
коэффициент влияния атаки	Z	$Z = \frac{\sum K_z}{K}$ (1)	Критичный (1) Высокий (0,8) Средний (0,5) Низкий (0,2)
общее количество КФП	K		
КФП, подверженный влиянию атаки	K_z		
коэффициент отказа системы	X	$Z = \frac{\sum X_z}{X_o}$ (2)	
количество последствий в результате влияния атаки	X_v		
общее число последствий	X_o		

определить от воздействия атак на КФП до суммарной вероятности потери конфиденциальности, целостности и доступности [8].

Методика позволяет рассчитать коэффициенты влияния атаки и отказа системы (табл. 2). Коэффициент влияния атаки (Z) представляет собой отношение КФП, подверженных влиянию атаки (K_z), к общему количеству КФП (K). Коэффициент отказа системы (X) представляет собой отношение количества последствий в результате влияния атаки (X_v) к общему числу последствий (X_o). Коэффициенты имеют четыре уровня критичности, которые лежат в диапазоне от 0 до 1. Границы уровней определены исходя из теоретического анализа.

С помощью схемы (рис. 3) проанализируем тип атаки «На получение доступа». Данный тип атак оказывает влияние на пять КФП: загрузка центрального процессора (ЦПУ), число зафиксированных спутников, уровень GPS шума, принятые пакеты данных, отправленные пакеты данных.

В итоге произведя расчеты с помощью формулы (1) можно сделать вывод, что влияние этой атаки на КФП является 0,35. Подвергшиеся влиянию атаки КФП составляют три системы БАС: система управления, система навигации, система связи.

Далее определяем, к каким последствиям приводит отказ или неправильная работа системы управления БАС. Рассчитываем по формуле (2) коэффициент

Таблица 3.

Влияние подгрупп атак на киберфизические параметры БАС

КФП	Атаки на получение доступа	Атаки подделки	Атаки типа «Отказ в обслуживании»	Атаки на целостность
Заряд аккумулятора		+	+	
Потребление мощности		+	+	
Загрузка ЦПУ	+	+	+	+
Загрузка ОЗУ		+	+	+
Число	6,5	3,2	5,1	
зафиксированных	1,1	2,3	1,5	
спутников	+	+		
Координаты БПЛА		+	+	+
Долгота		+	+	+
Широта		+	+	+
Высота полета			+	
Скорость полета		+	+	+
Уровень шумов	+		+	
Вибрация БПЛА			+	+
Принятые пакеты данных	+		+	+
Отправленные пакеты данных	+		+	+

опасности отказа системы, затем с помощью схемы можно рассчитать риски для конфиденциальности, целостности и доступности путем непосредственного влияния каждого из последствий на них. Ниже представлены расчеты влияния атак на КФП БАС по данной методике (табл. 3) и уровень опасности при воздействии определенных типов атак (табл. 4). Чем выше значение, тем больше уровень опасности.

Таблица 4.

Уровень опасности типов атак

Подгруппы атак	Уровень опасности
Атаки на получение доступа	0,36
Атаки подделки	0,64
Атаки типа «Отказ в обслуживании»	0,93
Атаки на целостность	0,64
Атака типа «Spoofing»	0,64
Атака типа «Tampering»	0,64
Атака типа «Repudiation»	0,28
Атака типа «Information Disclosure»	0,35
Атака обратного инжиниринга	0,35
Атака типа «SkyJack»	0,35

Разработанная методика охватывает распространенные атаки на КФП КФС и помогает выявить и оценить риски безопасности, которые могут возникнуть в результате атаки. Кроме того, методика позволяет определить меры противодействия для снижения рисков безопасности, а также рассчитать эффективность их применения.

2. Методика выбора эффективных контрмер

При рассмотрении мер противодействия кибератакам основное внимание уделяется атакам, которые нацелены на КФС, но не используют КФС в качестве агентов атаки на другие цели.

Сначала кибератаки классифицируются на основе типа точки входа, которая может быть средством передачи данных, сообщением или контроллером системы. В соответствии с этой классификацией существует шесть категорий атак, которые будут описаны далее. Базируясь на данной классификации, была проанализирована существующая литература на предмет контрмер для таких категорий атак.

Можно выделить три типа контрмер: классические, резервные и специальные. Классические препятствуют началу кибератаки. Так можно постоянно выполнять мониторинг и обработку информационного потока, чтобы заблаговременно обнаружить деструктивное воздействие. Когда классические контрмеры неэффективны, резервные предупреждают оператора либо пользователя КФС об атаке. К примеру, использование более чем одного типа датчиков для каждого критического измерения повысит отказоустойчивость системы и не даст начавшейся кибератаке вывести из строя КФС. После обнаружения атаки специальные меры способствуют снижению ущерба. Если заранее создать предопределенные процедуры управления КФС, то во время атаки система перейдет в автономную работу или отключится.

2.1. Кибератаки

Кибератака – это наступательное действие со злым умыслом, влияющее на вычислительные и коммуникационные функции. Хотя атаки могут привести к некоторым дополнительным сбоям в требованиях кибербезопасности, такие сбои могут не быть конечной целью злоумышленника. Через серию последовательных сбоев в кибербезопасности злоумышленник может стремиться в итоге вывести из строя или перехватить управление КФС, поставить под угрозу выполнение задачи или просто украсть собранную информацию (рис. 4). Таким образом, кибератака может представлять собой сложный многоэтапный процесс.

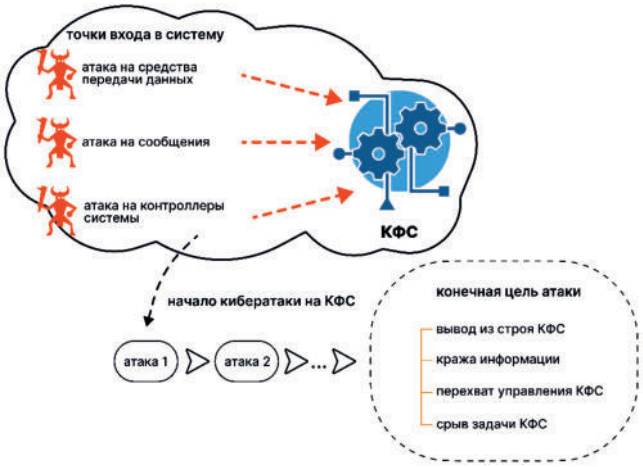


Рис. 4. Иллюстрация кибератаки на КФС

Как говорилось ранее, кибератаки классифицируются на основе типа точки входа в систему, в нашем случае это средства передачи данных, сообщения или контроллеры системы. Таким образом, мы выделили шесть категорий кибератак (рис. 5):

1) глушение канала передачи данных;
2) перехват сообщений;
3) удаление сообщений;
4) внедрение сообщений;
5) подмена сообщений;
6) атаки на контроллеры системы.

Глушение канала осуществляется путем создания более мощного радиосигнала, который значительно превышает мощность легитимных сигналов в целевом канале. В результате полезные сигналы подавляются

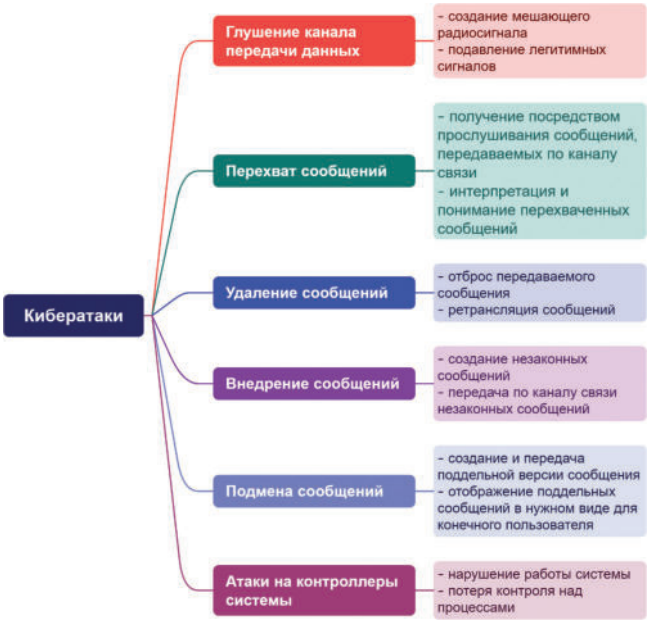


Рис. 5. Схема представлений данных о кибератаках

и проявляются только как шум в приемниках. Такая атак направлена на то, чтобы сделать канал связи недоступным для получателя. Следовательно, глушение каналов – это форма атаки типа «отказ в обслуживании» на физическом уровне.

Перехват сообщений – это пассивная атака, при которой злоумышленник получает посредством прослушивания сообщения, передаваемые по каналу связи. В этой атаке противник должен интерпретировать и понимать перехваченные сообщения. Целью атаки может быть перехват данных о системе. Кроме того, злоумышленник может получить другую вторичную информацию из перехваченных сообщений.

Удаление сообщения – это злонамеренное действие, которое отбрасывает сообщение, которое должно было быть передано предполагаемому получателю. Эта атака осуществляется злоумышленником, который предполагает ретранслировать сообщение, когда отправитель и предполагаемый получатель не находятся в пределах досягаемости каждого из них. По сравнению с перехватом сообщений эта атака может быть менее сложной, поскольку для этого злоумышленнику нужно просто отбросить сообщение.

Внедрение сообщений – это форма кибератаки, при которой создаются незаконные сообщения, а затем передаются через канал управления.

Подмена сообщений – это злонамеренный акт создания и передачи поддельной версии сообщения, а также их отображение в том виде, в котором они передаются от законного отправителя. В этом контексте злоумышленник является незаконным отправителем поддельного сообщения.

Контроллеры КФС отвечают за управление процессами, сетевые коммуникации, управление устройствами и т.д. Атаки на контроллеры могут привести к нарушению работы системы, потере контроля над процессами или даже физическим повреждениям.

2.2 Разработка набора контрмер

В литературе [9]–[16] предложен ряд мер противодействия различным кибератакам на КФС. В результате анализа контрмеры были разделены на три категории в зависимости от функциональных возможностей – классические, резервные и специальные, которые имеют свои функциональные возможности (рис. 6).

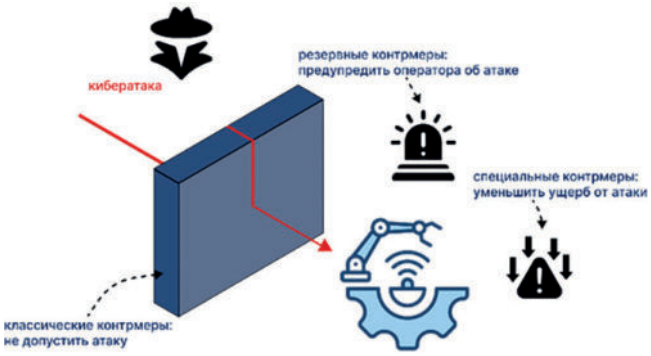


Рис. 6. Функциональные возможности различных контрмер кибератакам

Классические контрмеры позволяют предотвратить начало кибератаки. Когда классические меры противодействия не дали результата и атака была успешно начата, важными становятся резервные контрмеры для предупреждения оператора КФС о такой атаке. После обнаружения наличия атаки специальные контрмеры помогают уменьшить негативное воздействие и ограничить ущерб (табл. 5).

Также следует выделить еще одну категорию контрмер – профилактические. Профилактические контрмеры работают тремя способами:

1) ввести строгий контроль доступа к системе, чтобы только авторизованный персонал и программный агент могли устанавливать контакт с КФС;
2) защищать конфиденциальность, целостность и подлинность информации таким образом, чтобы никакие поддельные или ошибочные данные и команды не принимались;
3) использовать только системную прошивку и программные компоненты без уязвимостей.

Не все три метода предотвращения применимы ко всем кибератакам. Например, в качестве контрмеры против атаки на контроллеры системы в [17] и [18] необходимо спроектировать и внедрить в КФС только сенсоры с приемлемыми характеристиками в пределах ожидаемого рабочего диапазона. Но такая контрмера бесполезна для других атак. Кроме

Таблица 5.

Виды контрмер

Кибератаки	Контрмеры		
	Классические	**Резервные**	**Специальные**
Глушение канала передачи данных	Когнитивное радио, для переключения между каналами	Несколько приемников с разными частотами работы оборудования	Предопределенная процедура управления КФС для автономной работы или отключения
Перехват сообщений	Шифрование информации	Совместное использование радиосвязи и оптических каналов связи	Перенаправление злоумышленника на фальшивую цель
Удаление сообщения	Постоянный мониторинг и обработка информационного потока	Несколько приемников и передатчиков	Предопределенная процедура управления КФС для автономной работы или отключения
Внедрение сообщений	Проверка сообщений и использование шифрования информации	Несколько приемников и передатчиков	Атака с глушением канала как средство защиты
Подмена сообщений	Проверка сообщений, использование аутентификации и использование шифрование информации	Использование более чем одного типа датчиков для каждого критического измерения	Атака с глушением канала как средство защиты
Атаки на контроллеры системы	Строгая аутентификация узла для допуска только доверенных программ для предотвращения атак вирусов и вредоносных программ	Использование более чем одного типа датчиков для каждого критического измерения	Предопределенная процедура управления КФС для автономной работы или отключения

того, контроллеры системы должны быть оснащены функциями защиты от несанкционированного доступа, чтобы предотвратить открытие дополнительных точек входа для атак. Другим примером является использование устойчивых к помехам схем передачи, таких как расширение спектра с прямой последовательностью и расширение спектра со скачкообразной перестройкой частоты для предотвращения атак с глушением каналов. Такая контрмера обычно бесполезна для других атак, которые не запускаются на физическом уровне.

Кроме того, сообщения аутентификации и ассоциации, которые по умолчанию передаются в открытом виде, должны быть зашифрованы, чтобы предотвратить прослушивание беспроводной сети, которое предшествует атаке. Шифрование сообщения может защитить его конфиденциальность и, таким образом, предотвратить атаку с перехватом сообщений (рис. 7).

Рис. 7. Использование шифрования в качестве контрмер

Помимо криптографических методов, конфиденциальность информации также может быть достигнута с помощью методов защиты физического уровня. В контексте средств передачи данных авторы [19] предложили защищаться от полнодуплексного подслушивания путем передачи на физическом уровне сигналов искусственного шума вместе с информационными сигналами. Разработана схема определения оптимального коэффициента распределения мощности между искусственным шумом и информационными сигналами, при котором комбинация вероятности прекращения передачи и вероятности нарушения секретности минимизируется.

2.3. Разработка методики выбора эффективных контрмер

Методика представляет собой схематично описанную последовательность выбора эффективных контрмер для защиты КФС от атак противника [20]. Данную методику можно представить в виде концептуальной модели (рис. 8).

После определения типа кибератаки из схемы определяются контрмеры, которые можно использовать для предотвращения или смягчения последствий.

Методика позволяет рассчитать вероятность наступления того или иного последствия, а также успешность применения контрмер (табл. 6). Вероятность наступления последствия представляет собой отношение поврежденных в результате атаки систем к общему числу систем. Степень защиты после применения контрмер представляет собой отношение эффективных контрмер к общему числу контрмер. Коэффициенты имеют четыре уровня критичности, которые лежат в диапазоне от 0 до 1. Границы уровней определены исходя из теоретического анализа. Эффективность контрмер определяется показателями K и W, где значение W должно быть больше значения K, что означает степень защиты выше вероятности возникновения последствия. Если степень защиты будет ниже вероятности возникновения последствия, то каждая успешно примененная контрмера снижает вероятность наступления последствия на 10 %.

Проверим разработанную методику на экспериментальном образце БАС. Базовая конфигурация оборудования включает в себя полетный контроллер Pixhawk 4, одну беспроводную линию связи, совместимую с IEEE 802.11b/g [21], пульт управления, всенаправленную антенну, связь не шифруется. Также БАС содержит одну камеру, не имеет носителей информации, в качестве сенсорного оборудования используется ИНС. Механизм обработки ошибок

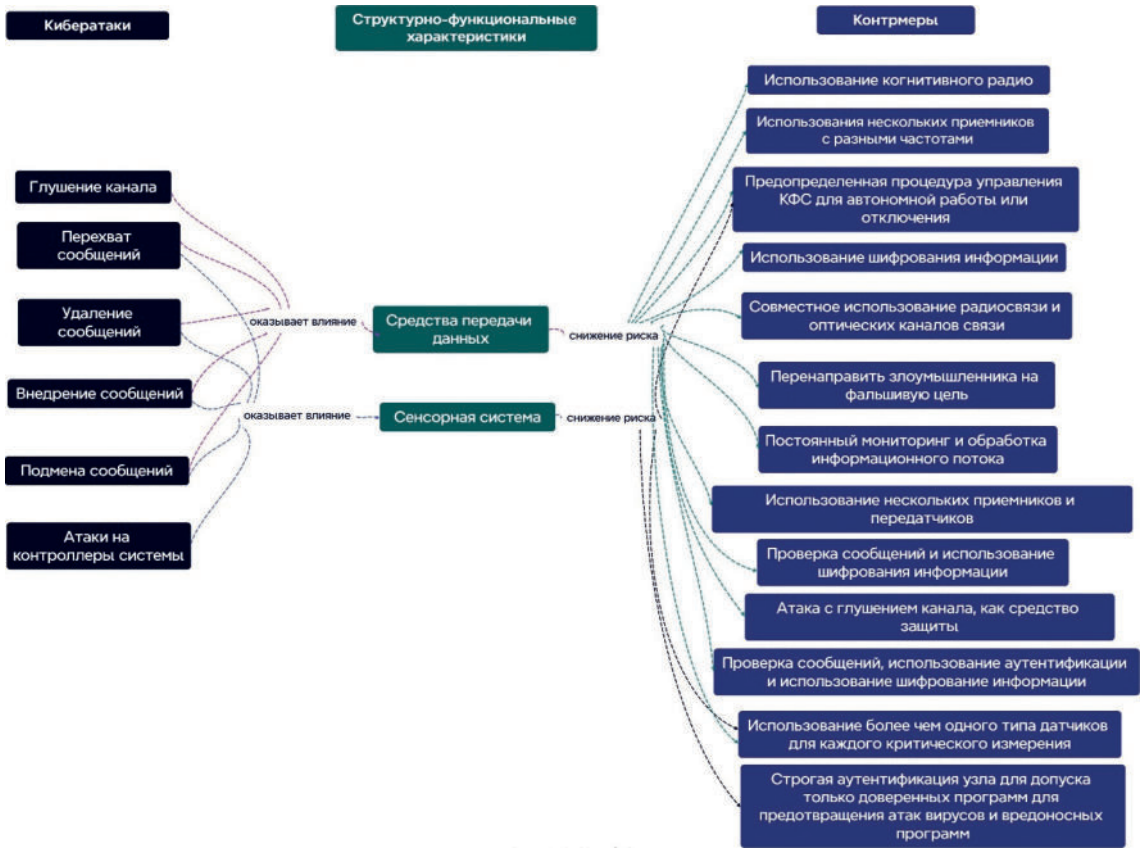


Рис. 8. Методика выбора эффективных контрмер

Таблица 2.

Методика оценки рисков

Параметр	Обозначение	Формула	Результат
вероятность наступления последствия	K	$K = \frac{\sum p_z}{P}$ (3)	Критичный (1)
поврежденные в результате атаки системы	P		Высокий (0,8)
общее число систем	p		
степень защиты после применения контрмер	W	$W = \frac{\sum t}{T}$ (4)	Средний (0,5)
эффективные контрмеры	t		Низкий (0,2)
общее число контрмер	T		

включает в себя только «режим земли». Для данного БАС характерны следующие угрозы:

- подмена сигнала GPS [22];
- подмена сообщения [23];
- глушение канала [24].

С помощью методики оценки угроз рассчитаем коэффициент опасности данных угроз, затем определим последствия, возникающие в результате угроз. На примере угрозы «Потеря контроля над БАС» рассмотрим предлагаемые контрмеры. Согласно методике снижения вероятности угрозы в данном случае стоит использовать следующие контрмеры:

- резервирование каналов связи,
- предопределенная процедура управления КФС для автономной работы или отключения,
- использование более чем одного типа датчиков для каждого критического процесса,
- шифрование каналов связи,
- использование систем обнаружения аномалий.

При угрозе подмены сигнала GPS вероятность наступления такого последствия, как «срыв задачи» будет равна:

$$K = \frac{4}{5} = 0{,}8.$$

В переводе на процентное соотношение – 80 %, для снижения риска с помощью схемы определим эффективные контрмеры и рассчитаем степень снижения риска:

$$W = \frac{7}{10} = 0{,}7.$$

После успешного применения контрмер вероятность возникновения снижается на 70%, в нашем случае K > W, значит вероятность наступления данного последствия после применения контрмер остается, но сводится к 10%, что позволяет сделать вывод об эффективности выбранных контрмер, в случае их успешного применения.

Вероятность наступления такого последствия как «Выход из строя» равна:

$$K = \frac{3}{5} = 0{,}6.$$

Что в процентном соотношении составляет 60%, рассчитаем степень снижения риска после применения контрмер:

$$W = \frac{5}{10} = 0{,}5.$$

После применения контрмер K > W, что означает если все контрмеры были успешно реализованы вероятность наступления последствия сводится к 10 %. В реальных условиях каждая успешно примененная контрмера снижает угрозу возникновения на 10 %.

Также при угрозе «подмена сигнала GPS» возможно такое последствие как «Частичное разрушение КФС», рассчитаем вероятность наступления для этого последствия:

$$K = \frac{4}{5} = 0{,}8.$$

В процентном соотношении – 80%, рассчитаем степень защиты после применения контрмер:

$$W = \frac{4}{10} = 0{,}4.$$

Применение контрмер в этом случае позволяет снизить риск возникновения последствия на 40 % и сводит вероятность возникновения к 40 %, вдвое меньше, чем до применения, что позволяет сделать выводы об эффективности контрмер в случае их успешного применения.

Заключение

Выбор эффективных контрмер для повышения отказоустойчивости КФС требует комплексного подхода. В результате работы был проведен анализ основных параметров КФС, и были выбраны те компоненты, которые имеют наибольшую вероятность наличия уязвимостей. Знания о наличии уязвимостей дают понимание о возможных векторах атак, которые может использовать злоумышленник для дестабилизации работы системы.

По результатам анализа литературы был составлен перечень контрмер в зависимости от вида кибератаки, которая может быть проведена на КФС. Перечень контрмер был разделен на три вида в зависимости

от функциональных возможностей системы. Приведенный перечень носит рекомендательный характер и может быть использован на усмотрение пользователей и операторов КФС.

Результатом методики является концептуальная модель, которая включает в себя перечень возможных кибератак на КФС, структурно-функциональные характеристики, на которые влияют приведенные кибератаки, и набор контрмер для минимизации рисков безопасности и повышения отказоустойчивости системы. Важно отметить, что эффективность контрмер может различаться в зависимости от конкретной системы и ситуации.

Данная методика показывает себя эффективней аналогов за счет возможностей расчета коэффициентов опасности, предсказаний вероятных последствий и предложения эффективных контрмер для снижения рисков. Простота расчетов и пошаговое использование делает методику более легкой в использовании и менее время затратной. Методика имеет возможность совершенствования и расширения за счет добавления новых атак и возможных угроз, а также добавления актуальных контрмер.

Разработанная методика была протестирована на экспериментальном стенде собранного БАС. Результат методики позволил авторам понять, что необходимо конкретизировать перечень СФХ системы, а также составить перечень вероятных рисков, которые могут наступить в результате реализации кибератак.

Работа выполнена при поддержке Совета по грантам Президента Российской Федерации. Стипендия Президента Российской Федерации молодым ученым и аспирантам (Конкурс СП-2022) № СП-858.2022.5 и Внутреннего гранта студенческим научным объединениям Южного федерального университета.

Литература

1. *I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, «Anatomy of Threats to the Internet of Things,» in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636–1675, Secondquarter 2019, doi: 10.1109/COMST.2018.2874978*
2. *Qaswar F., Rahmah M., Raza M. A., Noraziah A., Alkazemi B., Fauziah Z., Hassan M. K. A., Sharaf A. Applications of Ontology in the Internet of Things: A Systematic Analysis. Electronics. 2023; 12(1):111. https://doi.org/10.3390/electronics12010111*
3. *Jean-Paul Y., Hassan N., Ola S. Security analysis of drones systems: Attacks, limitations, and recommendations internet of things // Sensors. – 2020 Vol. 11, No. 100218 – P. 1–38.*
4. *Levshun, D., Kotenko, I. Intelligent Graph-Based Correlation of Security Events in Cyber-Physical Systems. In: Kovalev, S., Kotenko, I., Sukhanov, A. (eds) Proceedings of the Seventh International Scientific Conference «Intelligent Information Technologies for Industry» (IITI'23). IITI 2023. Lecture Notes in Networks and Systems, vol 777. Springer, Cham. https://doi.org/10.1007/978-3-031-43792-2_12*
5. *Lee I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet. 2020; 12(9):157. https://doi.org/10.3390/fi12090157*
6. *Ramanathan, L., Nandhini, R. S. (2022). Cyber-Physical System—An Architectural Review. In: Joshi, A., Mahmud, M., Ragel, R. G., Thakur, N. V. (eds) Information and Communication Technology for Competitive Strategies (ICTCS 2020). Lecture Notes in Networks and Systems, vol 191. Springer, Singapore. https://doi.org/10.1007/978-981-16-0739-4_13*
7. *A. Tantawy, S. Abdelwahed, A. Erradi, K. Shaban, Model-based risk assessment for cyber physical systems security, Computers & Security, Volume 96, 2020, 101864, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.101864*
8. *Мельник Э. В., Сафроненкова И. Б., Таранов А. Ю. Онтологический подход к решению задачи перераспределения вычислительной нагрузки в распределенной системе мониторинга с мобильными компонентами на базе распределённого реестра // Известия ЮФУ. Технические науки. 2023.; N 5(2023).; С. 163–173.; DOI 10.18522/2311-3103-2023-5-163-173*
9. *Elias G. T., Tala T. K., Hamed T. G. A secure Blockchain-based communication approach for UAV networks // Proceedings of the IEEE International Conference on Electro Information Technology (EIT). – Chicago, 2020. – P. 411–415.*
10. *Ammar A., Muhammad M., Kashif M. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs // Sensors. 2021. Vol. 196, No. 4. P. 108–217.*
11. *Ghiasi M. et al. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future // Electric Power Systems Research. 2023. Vol. 215. p. 108975.*
12. *Wöhnert, Kai Hendrik & Wöhnert, Sven-Jannik & Thiel, Tobias & Weißbach, Rüdiger & Skwarek, Volker. Secure Cyber-Physical Object Identification in Industrial IoT-Systems. Procedia Manufacturing. 51. 1221–1228. 10.1016/j.promfg.2020.10.171*
13. *D. M., Thompson., Sean, B., Maynard., Atif, Ahmad, Ahmad. «Cyber-threat intelligence for security decision-making: A review and research agenda for practice». Computers & Security, 132 (2023).:103352–103352. doi: 10.1016/j.cose.2023.103352*
14. *Rakesh S., Atefeh O., Sajjad A. Machine-learning-enabled intrusion detection system for cellular connected UAV networks // Sensors. – 2021. – Vol. 10, No.1549. – P. 1–28.*
15. *Mihalache, S. F., Pricop, E., Fattahi, J. (2019). Resilience Enhancement of Cyber-Physical Systems: A Review. In: Mahdavi Tabatabaei, N., Najafi Ravadanegh, S., Bizon, N. (eds) Power Systems Resilience. Power Systems. Springer, Cham. https://doi.org/10.1007/978-3-319-94442-5_11*

16. *Thulasiraman P., Haakensen T., Callanan A. «Countering Passive Cyber Attacks Against Sink Nodes in Tactical Sensor Networks Using Reactive Route Obfuscation», Elsevier Journal of Network and Computer Applications, Vol. 132, pp. 10–21, April 2019. DOI: 10.1016/j.jnca.2019.01.028*
17. *Zhang, Dongdong & Li, Chunjiao & Goh, Hui Hwang & Ahmad, Tanveer & Zhu, Hongyu & Liu, Hui & Wu, Thomas. (2022). A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems. Renewable Energy. 189. 1383–1406. 10.1016/j.renene.2022.03.096*
18. *Zheng, Yu & Li, Zheng & Xu, Xiaolong & Qingzhan, Zhao. (2021). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks. 8, 422–435. DOI: 10.1016/j.jnca.2019.01.028*
19. *Li, Guangxia & Shen, Yulong & Zhao, Peilin & Lu, Xiao & Liu, Jia & Liu, Yangyang & Hoi, Steven. (2019). Detecting Cyberattacks in Industrial Control Systems Using Online Learning Algorithms. Neurocomputing. 364, 338–348. DOI: 10.1016/j.neucom.2019.07.031*
20. *J. Leško, M. Schreiner, D. Megyesi and L. Kovács, «Pixhawk PX-4 Autopilot in Control of a Small Unmanned Airplane», 2019 Modern Safety Technologies in Transportation (MOSATT), Kosice, Slovakia, 2019, pp. 90–93, doi: 10.1109/MOSATT48908.2019.8944101*
21. *Basan, E., Lapina, M., Lesnikov, A., Basyuk, A., Mogilny, A. Trust Monitoring in a Cyber-Physical System for Security Analysis Based on Distributed Computing. In: Alikhanov, A., Lyakhov, P., Samoylenko, I. (eds) Current Problems in Applied Mathematics and Computer Science and Systems. APAMCS 2022. Lecture Notes in Networks and Systems, vol 702. Springer, Cham. https://doi.org/10.1007/978-3-031-34127-4_42*
22. *Basan, E.; Basan, A.; Nekrasov, A.; Fidge, C.; Sushkin, N.; Peskova, O. GPS-Spoofing Attack Detection Technology for UAVs Based on Kullback–Leibler Divergence. Drones 2022, 6, 8. https://doi.org/10.3390/drones6010008*
23. *Basan, E.; Basan, A.; Nekrasov, A. Method for Detecting Abnormal Activity in a Group of Mobile Robots. Sensors 2019, 19, 4007. https://doi.org/10.3390/s19184007*
24. *Basan, E.; Basan, A.; Mushenko, A.; Nekrasov, A.; Fidge, C.; Lesnikov, A. Analysis of Attack Intensity on Autonomous Mobile Robots. Robotics 2024, 13, 101. https://doi.org/10.3390/robotics13070101*

A METHODOLOGY FOR SELECTING EFFECTIVE COUNTERMEASURES TO INCREASE THE FAULT TOLERANCE OF CYBERPHYSICAL SYSTEMS

Basan E. S.[4], Silin O. I.[5], Firsova M. G.[6]

Keywords: *internet of things, sensors, cyberattack, threats, vulnerabilities, structural and functional characteristics, means of data transmission, countermeasures, incident.*

The aim of the work *is to develop a methodology for increasing the fault tolerance of a cyberphysical system through the use of countermeasures, depending on the identified threats when exposed to attacks on it.*

Research method: *the developed methodology is based on a conceptual model that describes the cyberphysical parameters and structural and functional characteristics of the system, and also allows you to identify current threats affecting the cyberphysical system. The methodology formally describes the threats that pose a danger to cyber-physical systems, assesses the risks of these threats and suggests effective countermeasures to reduce the risk of threats. An ontological approach is used to hierarchically represent knowledge about cyberphysical parameters and threats. The ontology allows us to describe the ratio of threats affecting the structural and functional characteristics, as well as to identify countermeasures that help minimize information security risks.*

Research results: *a methodology has been developed that, based on the analysis of the structural and functional characteristics of the system and their criticality, allows identifying current threats and selecting effective countermeasures to minimize them. An analysis of the main parameters of cyber-physical systems was conducted, a conceptual model was compiled that allows describing the structure of the cyber-physical system. As a result of the analysis of the main parameters of cyber-physical systems, those that are most susceptible to cyber-attacks were identified. A list of countermeasures was also created that minimize security risks, which increases the fault tolerance of the cyber-physical system. The result of the work is a list of attacks that are relevant for cyber-physical systems, as well as a number of countermeasures that minimize the identified cyber-attacks, while the countermeasures are divided into three categories.*

Scientific novelty: *the use of an ontological approach to describe the cyber-physical parameters and structural and functional characteristics of a cyber-physical system, which made it possible to identify those most susceptible to attacks and assess security risks.*

4 Elena S. Basan, Ph.D. (in Tech.), Associate Professor of the Department of Information Technology Security named after O. B. Makarevich, Institute of Computer Technology and Information Security, Southern Federal University, Taganrog, Russia. E-mail: ebasan@sfedu.ru

5 Oleg I. Silin, Assistant of the Department of Information Technology Security named after O. B. Makarevich, Institute of Computer Technology and Information Security, Southern Federal University «SFedU», Taganrog, Russia. E-mail: silin@sfedu.ru

6 Artyom Balyabin, Junior Researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, E-mail: Balyabinю.AA@ talantiuspeh.ru

References

1. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, «Anatomy of Threats to the Internet of Things,» in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636–1675, Secondquarter 2019, doi: 10.1109/COMST.2018.2874978
2. Qaswar F., Rahmah M., Raza M. A., Noraziah A., Alkazemi B., Fauziah Z, Hassan MKA, Sharaf A. Applications of Ontology in the Internet of Things: A Systematic Analysis. Electronics. 2023; 12(1):111. https://doi.org/10.3390/electronics12010111
3. Jean-Paul Y., Hassan N., Ola S. Security analysis of drones systems: Attacks, limitations, and recommendations internet of things // Sensors. – 2020 Vol. 11, No. 100218 – P. 1–38.
4. Levshun, D., Kotenko, I. Intelligent Graph-Based Correlation of Security Events in Cyber-Physical Systems. In: Kovalev, S., Kotenko, I., Sukhanov, A. (eds) Proceedings of the Seventh International Scientific Conference «Intelligent Information Technologies for Industry» (IITI'23). IITI 2023. Lecture Notes in Networks and Systems, vol 777. Springer, Cham. https://doi.org/10.1007/978-3-031-43792-2_12.
5. Lee I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet. 2020; 12(9):157. https://doi.org/10.3390/fi12090157
6. Ramanathan, L., Nandhini, R. S. (2022). Cyber-Physical System – An Architectural Review. In: Joshi, A., Mahmud, M., Ragel, R. G., Thakur, N. V. (eds) Information and Communication Technology for Competitive Strategies (ICTCS 2020). Lecture Notes in Networks and Systems, vol 191. Springer, Singapore. https://doi.org/10.1007/978-981-16-0739-4_13
7. A. Tantawy, S. Abdelwahed, A. Erradi, K. Shaban, Model-based risk assessment for cyber physical systems security, Computers & Security, Volume 96, 2020, 101864, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.101864
8. Mel'nik Je. V., Safronenkova I. B., Taranov A. Ju. Ontologicheskij podhod k resheniju zadachi pererаspredelenija vychislitel'noj nagruzki v raspredelennoj sisteme monitoringa s mobil'nymi komponentami na baze raspredeljonnogo reestra // Izvestija JuFU. Tehnicheskie nauki.; 2023.; N 5 (2023).; S. 163–173.; DOI 10.18522/2311-3103-2023-5-163-173
9. Elias G. T., Tala T. K., Hamed T. G. A secure Blockchain-based communication approach for UAV networks // Proceedings of the IEEE International Conference on Electro Information Technology (EIT). – Chicago, 2020. – P. 411–415.
10. Ammar A., Muhammad M., Kashif M. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs // Sensors. – 2021. – Vol. 196, No. 4. – P. 108–217.
11. Ghiasi M. et al. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future // Electric Power Systems Research. 2023. Vol. 215. p. 108975.
12. Wöhnert, Kai Hendrik & Wöhnert, Sven-Jannik & Thiel, Tobias & Weißbach, Rüdiger & Skwarek, Volker. Secure Cyber-Physical Object Identification in Industrial IoT-Systems. Procedia Manufacturing. 51. 1221-1228. 10.1016/j.promfg.2020.10.171
13. D. M., Thompson., Sean, B., Maynard., Atif, Ahmad, Ahmad. «Cyber-threat intelligence for security decision-making: A review and research agenda for practice». Computers & Security, 132 (2023).:103352–103352. doi: 10.1016/j.cose.2023.103352
14. Rakesh S., Atefeh O., Sajjad A. Machine-learning-enabled intrusion detection system for cellular connected UAV networks // Sensors. – 2021. – Vol. 10, No.1549. – P. 1–28.
15. Mihalache, S. F., Pricop, E., Fattahi, J. (2019). Resilience Enhancement of Cyber-Physical Systems: A Review. In: Mahdavi Tabatabaei, N., Najafi Ravadanegh, S., Bizon, N. (eds) Power Systems Resilience. Power Systems. Springer, Cham. https://doi.org/10.1007/978-3-319-94442-5_11
16. Thulasiraman P., Haakensen T., Callanan A. «Countering Passive Cyber Attacks Against Sink Nodes in Tactical Sensor Networks Using Reactive Route Obfuscation», Elsevier Journal of Network and Computer Applications, Vol. 132, pp. 10–21, April 2019. DOI: 10.1016/j.jnca.2019.01.028
17. Zhang, Dongdong & Li, Chunjiao & Goh, Hui Hwang & Ahmad, Tanveer & Zhu, Hongyu & Liu, Hui & Wu, Thomas. (2022). A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems. Renewable Energy. 189. 1383–1406. 10.1016/j.renene.2022.03.096
18. Zheng, Yu & Li, Zheng & Xu, Xiaolong & Qingzhan, Zhao. (2021). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks. 8, 422–435. DOI: 10.1016/j.dcan.2021.07.006
19. Li, Guangxia & Shen, Yulong & Zhao, Peilin & Lu, Xiao & Liu, Jia & Liu, Yangyang & Hoi, Steven. (2019). Detecting Cyberattacks in Industrial Control Systems Using Online Learning Algorithms. Neurocomputing. 364, 338–348. DOI: 10.1016/j.neucom.2019.07.031
20. J. Leško, M. Schreiner, D. Megyesi and L. Kovács, «Pixhawk PX-4 Autopilot in Control of a Small Unmanned Airplane», 2019 Modern Safety Technologies in Transportation (MOSATT), Kosice, Slovakia, 2019, pp. 90–93, doi: 10.1109/MOSATT48908.2019.8944101
21. Basan, E., Lapina, M., Lesnikov, A., Basyuk, A., Mogilny, A. Trust Monitoring in a Cyber-Physical System for Security Analysis Based on Distributed Computing. In: Alikhanov, A., Lyakhov, P., Samoylenko, I. (eds) Current Problems in Applied Mathematics and Computer Science and Systems. APAMCS 2022. Lecture Notes in Networks and Systems, vol 702. Springer, Cham. https://doi.org/10.1007/978-3-031-34127-4_42
22. Basan, E.; Basan, A.; Nekrasov, A.; Fidge, C.; Sushkin, N.; Peskova, O. GPS-Spoofing Attack Detection Technology for UAVs Based on Kullback–Leibler Divergence. Drones 2022, 6, 8. https://doi.org/10.3390/drones6010008
23. Basan, E.; Basan, A.; Nekrasov, A. Method for Detecting Abnormal Activity in a Group of Mobile Robots. Sensors 2019, 19, 4007. https://doi.org/10.3390/s19184007
24. Basan, E.; Basan, A.; Mushenko, A.; Nekrasov, A.; Fidge, C.; Lesnikov, A. Analysis of Attack Intensity on Autonomous Mobile Robots. Robotics 2024, 13, 101. https://doi.org/10.3390/robotics13070101

О ПОСТАНОВКЕ ЗАДАЧИ ОЦЕНИВАНИЯ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Воеводин В. А.[1]

DOI: 10.21681/2311-3456-2025-1-41-49

Цель исследования: *обосновать актуальность, сформулировать и формализовать научную задачу количественного оценивания устойчивости функционирования критической информационной инфраструктуры применительно к условиям воздействия угроз нарушения ее информационной безопасности.*

Методы исследования: *системный анализ, анализ научной проблемы, формализация научных знаний, методология научного исследования.*

Полученные результаты: *сформулирована вербальная и формальная постановки научной задачи.*

Научная новизна: *предлагается авторский подход к оцениванию динамики устойчивости функционирования критической информационной инфраструктуры в условиях воздействия угроз с учетом имеющегося ресурса.*

Практическая значимость: *постановка научной проблемы может служить основой для формулирования технического задания по разработке методов, моделей и средств количественного оценивания устойчивости функционирования объектов критической информационной структуры, функционирующих в условиях воздействия угроз.*

Ключевые слова: *угрозы нарушения информационной безопасности, система восстановления функциональности, критическая информационная инфраструктура, восстанавливаемость, защищенность от угроз, возобновляемый ресурс, невозобновляемый ресурс.*

Введение

Информационная инфраструктура того или иного объекта информатизации создается для удовлетворения определенных потребностей субъектов информационных отношений (обладателей информации и операторов информационных систем) и служит активным средством в их целенаправленной деятельности. Чтобы противостоять воздействию угроз безопасности информации обладатели информации и операторы информационных систем обязаны в силу закона принимать меры по защите информации. В силу закона отдельно выделяются критические информационные инфраструктуры (КИИ). Отношения, возникающие при обеспечении устойчивости функционирования КИИ в условиях воздействия угроз, регулируются ответствующими нормативными правовыми актами.

Противник с целью нарушить функциональность объектов КИИ осуществляет как физическое воздействие по ее элементам, так и воздействие посредством воздействия помех и компьютерных атак. В совокупности эти воздействия позиционируются как воздействия угроз безопасности информации (угроз).

В результате воздействия угроз функциональность отдельных элементов может быть нарушена или они могут быть уничтожены, что может привести к снижению устойчивости функционирования КИИ в целом ниже требуемого уровня. Генезис понятия «устойчивость функционирования КИИ» применительно к настоящей публикации рассматривается в [1].

Для обеспечения устойчивости КИИ выделяются соответствующие силы и средства, которые необходимо результативно распределить по задачам и времени. Для решения этой задачи органами управления требуется инструмент для количественного оценивания устойчивости функционирования объектов КИИ в различных условиях обстановки, в том числе и в условиях воздействия угроз.

Для успешного решения задач по оцениванию устойчивости КИИ требуется, чтобы методические потребности органов управления ИБ и соответствующий научно-методический аппарат находились в гармонии.

Применение экспериментального подхода, характерного для условий штатного применения, для оценивания устойчивости функционирования масштабных КИИ в условиях воздействия угроз требует значительного ресурса и часто неприменимо по экономическим соображениям. Поэтому основной исследовательской концепцией для оценивания

1 Воеводин Владислав Александрович, кандидат технических наук, доцент, МИЭТ, Москва, Россия, E-mail: vva541@mail.ru. AuthorID: 1012813, ORCID 0009-0003-9431-1685

устойчивости функционирования применительно к условиям воздействия угроз является экспертное и математическое моделирование.

Анализ существующего методического обеспечения

Анализ существующих нормативных правовых актов, методических документов, приказов исполнительных органов власти и национальных стандартов позволяет утверждать, что они в совокупности и по отдельности не содержат общепринятых методических рекомендаций по количественному оцениванию устойчивости КИИ применительно к условиям воздействия угроз.

Существующий инструмент оценивания устойчивости КИИ ориентирован на штатные условия и базируется на приложениях теории надежности. Методы теории надежности, основаны на анализе экспериментальных и эксплуатационных данных, постоянно развиваются. Результаты фундаментальных исследований теории надежности технических систем отражены достаточно полно и глубоко в фундаментальных публикациях Б. В. Гнеденко[2], И. А. Ушакова[3], В. А. Каштанова[4] и других, признанных в этой области ученых.

Однако для оценивания устойчивости КИИ, находящейся под воздействием угроз, применение методов теории надежности не всегда оправдано и корректно. Такое ограничение связано с необходимостью учесть при оценивании устойчивости редкость событий воздействия угроз, ограниченность интервала времени их наблюдения, динамичность обстановки и самих показателей, характеризующих исходные данные, влияние поведенческой неопределенности. Ограниченность методов теории надежности при исследовании живучести, безопасности, защищенности сложных систем и надежности программного обеспечения отмечалась И. А. Ушаковым в докладе «Надежность: прошлое, настоящее, будущее»[5].

Результаты методологического исследования особенностей количественного оценивания эффективности информационных систем и технологий применительно к штатным условиям функционирования приводятся Зегждой Д. П. [2, 3]. Авторский коллектив предлагает в основу оценивания положить вероятностный подход, что для условий воздействия угроз так же не всегда является приемлемым.

Отсутствие инструмента для количественного оценивания устойчивости КИИ, находящейся под воздействием угроз сдерживает развитие отношений в области обеспечения безопасности КИИ при воздействии угроз.

Анализ возможностей существующих научных методов

Исходными посылами, которые легли в основу анализа применимости существующих научных методов для оценивания устойчивости технических систем, функционирующих в условиях целенаправленных угроз, явились результаты осмысления деятельности по организации аудита информационной безопасности (ИБ). Почвой для такого осмысления явилось обобщение опыта преподавания учебных курсов магистратуры, в рамках которых изучались правовые и организационные основы аудита ИБ, организовывалась выпускная деловая игра по организации аудита автоматизированных систем.

Полученные общения позволили прийти к выводу о том, что существующий подход к аудиту ИБ в отношении объектов информатизации нацелен на оценивание их соответствия требованиям Регулятора, а не на количественном оценивании устойчивости их функционирования в различных условиях обстановки.

Деятельность по оцениванию устойчивости объектов КИИ, в отличии от деятельности по оценке соответствия требованиям, по своей сути является продуктивной, так как направлена каждый раз на получение объективно нового результата. Такая деятельность, в отличие от репродуктивной, нуждается в организации, то есть возникает необходимость в ее теоретическом осмыслении, а также в построении соответствующей методологии оценивания.

В основу существующего подхода к обеспечению устойчивости функционирования КИИ положены императивные нормы права. Деятельность регулируется преимущественно силой закона и подзаконных актов. Эта деятельность позиционируется как административная и относится к репродуктивной. Для организации такой деятельности инструмент для количественного оценивания устойчивости КИИ формально не требуется. К существующей инерционности и репродуктивности директивного подхода необходимо объективно добавить и то, что требования общедоступны и известны противнику (источнику угроз), который может целенаправленно планировать эффективное воздействие угроз в обход реализованных требуемых мер защиты.

Вместе с тем, опять же силой закона, обладателям информации и операторам информационных систем предписано: 1) обеспечить защиту информации; 2) не допускать воздействий на технические средства обработки информации, в результате которых

2 Гнеденко Б. В., Беляев Ю. К., Соловьев А. Д. Математические методы в теории надежности. – М.: Наука. 1965. – 524 с.

3 Ушаков И. А. Обобщенные показатели при исследовании сложных систем / И. А. Ушаков, Е. И. Литвак. – М.: Знание. 1985. – 128 с.

4 Каштанов В. А., Медведев А. И. Теория надежности сложных систем. 2-е изд., перераб. – М.: ФИЗМАТЛИТ. 2010. – 608 с.

5 Ушаков И. А. Надежность: прошлое, настоящее, будущее: пленарный доклад на открытии конференции «Математические методы в надежности» (MMR–2000), Бордо, Франция, 2000 // Надежность: Вопросы теории и практики: сетевой журн. 2016. №. 1(1). С. 17–27.

нарушается их функционирование; 3) осуществлять постоянный контроль за обеспечением уровня защищенности информации. Директивный подход в этом случае не применим, так как не обеспечивает эффективного применения соответствующих сил и средств. При исполнении перечисленных предписаний должны действовать диспозитивные нормы права, в соответствии с которыми обладателям информации и операторам информационных систем предоставляется право самостоятельно регулировать эти отношения и принимать соответствующие решения. Для самостоятельного регулирования таких отношений требуется инструмент, позволяющий решить задачу количественного оценивания устойчивости функционирования соответствующих объектов информатизации.

В настоящее время известен ряд подходов к решению задачи оценивания и обеспечения устойчивости объектов информатизации, функционирующих в условиях воздействия дестабилизирующих факторов различной физической природы. Некоторые из таких подходов, представляющие интерес для оценивания устойчивости КИИ, приведены в трудах Д. П. Зегжды [3], И. В. Котенко [4], И. Б. Саенко [5], С. А. Коноваленко [6], С. И. Макаренко [7], Ю. И. Стародубцева [8, 9], Ю. К. Язова [10–12], И. Б. Шубинского [13–15].

Основные усилия исследователей были направлены на развитие подходов оценивания устойчивости структурно-сложных технических систем на основе парадигмы структурной и функциональной устойчивости, когда критерий отказа системы и/или элемента является бинарным. На практике задача сводилась к определению за допустимое вычислительное время доли сохранившихся работоспособных состояний, когда из строя выходит фиксированное число элементов, при этом анализ живучести проводится на стыке анализа структурной и функциональной избыточности в сочетании с вероятностными моделями объектов оценивания.

Вопросы обеспечения устойчивости функционирования сложных систем рассматривались и в смежных областях. Так, критерии, методы анализа и синтеза технических и информационных систем, методы обеспечения и повышения надежности, эксплуатации в штатных условиях исследовались А. М. Половко совместно с С. В. Гуровым[6]. В качестве предмета исследования были рассмотрены невосстанавливаемые и восстанавливаемые, нерезервированные и резервированные системы длительного и короткого времени существования.

Обобщая результаты ретроспективного анализа, можно утверждать, что основные усилия исследователей были сосредоточены на оценивании устойчивости на основе исходных данных, которые характеризовали надежность элементов КИИ. Так или иначе при таком подходе к оцениванию требовались некие исторические данные (статистика). При оценивании характеристик устойчивости принималось допущение о стационарности случайного процесса, что позволяло не учитывать динамические характеристики процесса функционирования объекта оценивания, и использовать в качестве показателей усредненные оценки всего процесса. Усредненные оценки основывались на статистических наблюдениях, проводимых в стабильных условиях, которые для условий воздействия угроз чаще неприменимы из-за высокой погрешности. Обычно характеристики надежности оцениваются при проведении приемочных испытаний и приводятся в эксплуатационной документации.

Такой подход к оцениванию устойчивости в условиях воздействия угроз не всегда применим и корректен. На практике приходится иметь дело со случайными величинами, статистические характеристики которых непрерывно изменяются с течением времени либо вообще неизвестны и недоступны эксперту для наблюдения и эксперимента. Для оценивания устойчивости в этих условиях требуется специальный инструмент, который бы позволял получать оценки применительно к воздействию целенаправленных угроз, с учетом имеющегося ресурса и информационной неопределенности которая присуща противнику при планировании компьютерных атак.

Результаты проведенного анализа позволяют утверждать, что объективно наблюдается противоречивая ситуация, суть которой заключается в том, что, с одной стороны, органам управления для принятия решения требуется общепринятое методическое обеспечение для количественной оценки устойчивости функционирования КИИ, а с другой стороны, существующие научные методы и модели, без принятия грубых допущений, не могут быть использованы в качестве его теоретического фундамента.

Для разрешения противоречия требуется решить научную задачу по разработке системы методов, моделей и средств, позволяющих в графике работы органов управления ИБ получать оценки устойчивости функционирования объектов КИИ, которая бы легла методологическим фундаментом к формулированию требований к методическому обеспечению.

Анализ существующего теоретического задела подтверждает, что для условий воздействия целенаправленных угроз существуют лишь отдельные публикации, которые не объединены в единый методический аппарат, что в совокупности переводит поставленную научную задачу в статус научной проблемы.

6 Половко А. М., Гуров С. В. Основы теории надежности. – СПб.: БХВ-Петербург. 2006. – 704 с.

Вербальная постановка научной задачи

При оценивании устойчивости КИИ с помощью моделирования следует учитывать отдельные группы факторов, которые напрямую или косвенно влияют на ее обеспечение: 1) сценарии воздействия угроз; 2) характеристики надежности элементов; 3) защищенность элементов от воздействия угроз; 4) производственные возможности системы восстановления функциональности (СВФ) субъекта КИИ; 4) схему, отображающую условия обеспечения функциональности объекта оценивания (СОФ).

Для оценивания устойчивости объекта КИИ за основу была принята концепция условий работоспособного состояния, которая была применена для оценивания концептуальных направлений решения проблемы обеспечения устойчивости сложных технических систем [13–15].

Для формальной постановки научной проблемы факторы, определяющие условия функционирования КИИ, подразделяются на две группы: 1) факторы, которые могут контролироваться лицом, принимающим решение (ЛПР), и доступны ему для управления; 2) факторы, которые по различным причинам не могут быть контролируемы ЛПР; 3) факторы, которые выведены в ограничения.

При формулировании задачи принимается, что каждый элемент оцениваемого объекта на периоде воздействия угроз может принимать одно из трех состояний: 1) *функционален* – способен выполнять требуемые функции; 2) *поврежден* – восстановление функциональности возможно через допустимый период времени восстановления, при этом расходуется имеющийся ресурс СВФ; 3) *поражен* – восстановление функциональности не целесообразно или невозможно из-за ограниченности имеющегося ресурса СВФ, в том числе и времени. Последовательный переход из одного состояния в другое позиционируется как процесс функционирования элемента и объекта КИИ в целом.

При постановке задачи принимаются ограничения: 1) считается, что если элемент попадает в состояние «уничтожен», то он так и остается в этом состоянии до конца периода оценивания; 2) требования к конфиденциальности и целостности информации выполняются на всем протяжении периода оценивания не хуже заданных; 3) возможность поражения органов управления не учитывается, т. е. вероятность сохранения ими способности формировать управленческие решения принимается равной единице.

Требуется разработать методы, модели и средства, позволяющие с учетом принятых ограничений.

1. **На первом этапе** отобразить исходные данные, характеризующие: 1) возможные сценарии воздействия противника; 2) защищенность элементов от воздействия угроз; 3) семейство актуальных угроз; 4) выделенный для поддержания функциональности элементов ресурс; 5) надежность элементов для условий штатного применения (значения коэффициентов оперативной готовности); 6) восстанавливаемость элементов, в значения частных функций устойчивости элементов.
2. **На втором этапе** – отобразить: 1) семейство частных функций устойчивости элементов; 2) характеристики СВФ субъекта КИИ; 3) характеристики СОФ в значения функции устойчивости для всего оцениваемого объекта;

Для решения поставленной научной задачи предлагается обобщить методы теории надёжности, теории случайных функций, теории информационной безопасности на случаи, когда при оценивании устойчивость КИИ не представляется возможным принять допущения: 1) о массовости случайных явлений; 2) об эргодичности и стационарности оцениваемого случайного процесса; 3) об отсутствии поведенческой неопределенности; 4) о неограниченности ресурса СВФ.

Новизна полученных результатов заключается: 1) в усовершенствовании онтологии предметной области, позволяющей строить адекватные вербальные модели предмета исследования; 2) в оригинальной постановке научной задачи, позволяющей оценить устойчивость для условий воздействия угроз, когда методы математической статистики и теории вероятностей, которые нашли широкое применение для штатных условий, не могут быть применимы без грубых допущений; 3) в использовании для представления исходных данных и результатов оценивания не усредненные вероятностные характеристики, как это принято для штатных условий, а функции устойчивости, отражающие зависимость параметров исходных данных и получаемого результата от времени. Такой подход позволяет снять ограничение на стационарность и эргодичность исследуемого случайного процесса; 4) применение для оценивания устойчивости отдельных элементов методов теории управляемых полумарковских процессов с тремя возможными состояниями, что позволяет связать частные характеристики защищенности и восстанавливаемости элементов подверженных угрозам с частными оценками устойчивости их функционирования; 5) в приложении методов управляемых полумарковских процессов для оценивания устойчивости объекта КИИ в целом на основе частных оценок функций устойчивости элементов; 6) в приложении методологии для количественного оценивания эффективности планов восстановления функциональности объекта оценивания, элементы которой получили повреждения в результате воздействия угроз;

7) в приложении разработанных методов оценивания устойчивости для обоснования распределения затрат между мероприятиями по обеспечению защищенности и восстанавливаемости элементов.

Формальная постановка научной задачи

Пусть заданы исходные данные, характеризующие:

Управляемые факторы

1. Пусть задана структура СОФ оцениваемого объекта в момент времени t_0, соответствующий началу периода воздействия угроз $(0, T]$

$$S(t_0) = \{A(t_0), L(t_0)\},$$

где $A(t_0) = \{a_i(t_0)\}$ – семейство *узлов* СОФ, $a_i(t_0)$ – индикатор состояния i-го узла, $i = 1, 2, ..., N_A$; N_A – мощность семейства $A(t_0)$. Если узел $a_i(t_0)$ функционален, то $a_i(t_0) = 1$ и 0 в противном случае;

$L(t_0) = \{l_{i,j}(t_0)\}$ – семейство *ребер* СОФ, $l_{i,j}(t_0)$ – индикатор состояния i,j-го ребра, $i,j = 1, 2, ..., N_L$; $N_L = (N_A)^2$ – мощность семейства $L(t_0)$. Если ребро $l_{i,j}(t_0)$ функционально, то $l_{i,j}(t_0) = 1$ и 0 в противном случае;

Определено исходное семейство *элементов (узлов и ребер)* СОФ в момент времени t_0

$$E(t_0) = \{e_k(t_0)\} = A(t_0) \cup L(t_0) = \{\{a_i(t_0)\} \cup \{l_{i,j}(t_0)\}\},$$

где $k = 1, 2, ..., N_E$; N_E – мощность исходного семейства элементов $E(t_0)$, $e_k(t_0) \in E(t_0)$.

Функционирование подверженного воздействию угроз объекта оценивания характеризуется сменой состояний его элементов $e_k(t_0) \in E(t_0)$:

1) если k-й элемент на момент времени t сохранил функциональность, то $e_k(t) = 1$;
2) если k-й элемент был поврежден, то $e_k(t) = \tau_k(t)$, где $\tau_k(t)$ – время до окончания восстановления функциональности k-го элемента на момент времени t;
3) если k-й элемент был поражен в результате воздействия угрозы, то его идентификатору безвозвратно присваивается значение $e_k(t) = 0$.

Пусть известны первичные количественные оценки факторов, которые оказывают непосредственное влияние на устойчивость оцениваемого объекта:

2. Семейство актуальных угроз $U = \{u_m\}$, где u_m – идентификатор актуальной угрозы с индексом m, $m = 1, 2, ..., N_U$, N_U – мощность семейства актуальных угроз.

3. Семейство стационарных коэффициентов оперативной готовности элементов оцениваемого объекта

$$K_{Oг}(t_0, t_0 + t) \underset{\substack{t \in 0, T, \\ k = 1, 2, ..., N_E}}{=} \{\hat{k}_{Oгk}(t_0, t_0 + t)\},$$

где $\hat{k}_{Oгk}$ – стационарный коэффициент оперативной готовности k-го элемента на интервале $t \in (0, T]$. Физически $\hat{k}_{Oгk}$ отражает вероятность того, что элемент a_k проработает безотказно в течение заданного периода времени T, начиная с момента времени t_0.

4. Защищенность элементов оцениваемого объекта от воздействия актуальных угроз U

$$P(u) \underset{\substack{k = 1, 2, ...N_E, \\ m = 1, 2, ...N_U}}{=} \{p_{k,m^*}, \underset{\sim}{p}_{k,m^*}, \hat{p}_{k,m^*}\},$$

где $p_{k,m}$ – оценка вероятности сохранения функциональности элементом с индексом $e_k(t_0) \in E(t_0)$ при воздействии угрозы с индексом $u_m \in U$. Если угроза u_m для элемента $e_k(t_0)$ является не актуальной, то $p_{k,m} = 1$. Из всех актуальных угроз U для оценивания защищенности элемента с индексом e_k выбирается угроза из семейства актуальных с индексом u_{m^*}, при которой

$$p_{k,m^*} = \min_{\substack{k = 1, 2, ...N_E, \\ m = 1, 2, ...N_U}} p_{k,m},$$

где p_{k,m^*} – вероятность повреждения k-го элемента при воздействии угрозы u_{m^*}; $\hat{p}_{k,m^*}$ – вероятность поражения k-го элемента при воздействии угрозы u_{m^*};

$$\hat{p}_{k,m^*} = 1 - (p_{k,m^*} + \underset{\sim}{p}_{k,m^*}).$$

Учитывая, что элемент может находится только в одном из трех состояний следует, что $p_{k,m^*} + \hat{p}_{k,m} + \underset{\sim}{p}_{k,m^*} = 1$.

5. Оценка *требуемых* производственных *возможностей* для восстановления функциональности объекта оценивания после воздействия угроз $u \in U$

$$T(u) \underset{\substack{k = 1, 2, ...N_E, \\ m = 1, ...N_U}}{=} \{\tau_{k,m}\} \underset{\substack{k = 1, 2, ...N_E, \\ m = 1, ...N_U}}{=} \{\underset{\sim}{\tau}_{k,m}, \hat{\tau}_{k,m}\},$$

где $\underset{\sim}{\tau}_{k,m}$ – нижняя граница оценки *требуемого времени* восстановления функциональности элемента e_k, из всех актуальных угроз U выбирается угроза с индексом u_{m^*}, при которой

$$\underset{\sim}{\tau}_{k,m} = \underset{\sim}{\tau}_{k,m^*} = \max_{m = 1, 2, ...N_U} \underset{\sim}{\tau}_{k,m};$$

$\hat{\tau}_{k,m}$ – верхняя оценка *требуемого* времени восстановления функциональности $\hat{\tau}_{k,m}$ элемента e_k, из всех актуальных угроз U выбирается угроза с индексом u_{m^*}, при которой

$$\hat{\tau}_k = \hat{\tau}_{k,m^*} = \max_{m = 1, 2, ...N_U} \hat{\tau}_{k,m}.$$

6. Ресурсные возможности СВФ субъекта КИИ, выделенные для восстановления функциональности объекта оценивания в условиях воздействия угроз

$$\Theta \underset{\substack{i = 1, 2, ...N_D, \\ j = 1, 2, ...N_R}}{=} \{d_i, r_j\},$$

где d_i – число единиц d_i-го возобновляемого ресурса, d_i – классификатор i-го возобновляемого ресурса, $i = 1, 2, ..., N_D$, N_D – количество классификаторов возобновляемого ресурса; r_j – число единиц r_j-го невозобновляемого ресурса, r_j – классификатор j-го невозобновляемого ресурса, $j = 1, 2, ..., N_R$,

N_R – количество классификаторов (артикулов) невозобновляемого ресурса.

Обобщенная схема управляемых факторов приведена на рис. 1.

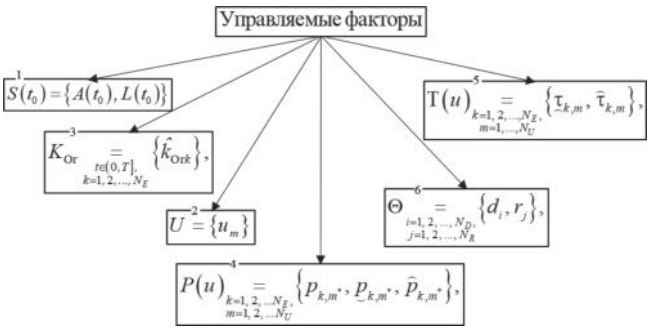


Рис. 1. Управляемые факторы, определяющие устойчивость объекта оценивания

Неуправляемые факторы

1. Параметры воздействия угроз по семейству элементов объекта оценивания

$$N(u) = \{\underset{\sim}{\eta}_{m,k,n}, \hat{\eta}_{m,k,n}\},$$

где $\underset{\sim}{\eta}_{m,k,n}$ – нижняя граница времени до n-го воздействия угрозы $u_m \in U$ по элементу a_k. Из всех актуальных угроз U для каждого воздействия n выбирается угроза с индексом $u_{m^*} \in U$, для которой

$$\underset{\sim}{\eta}_{m^*,k,n} = \min_{\substack{m=1,2,\ldots N_U,\\ n=1,\ldots N}} \underset{\sim}{\eta}_{m,k,n}$$

где $m = 1, \ldots, N_U$, N_U – число актуальных угроз; $k = 1, \ldots, N_E$; $k = 1, \ldots, N_E$, N_E – число элементов СОФ; $n = 1, \ldots, N_U$, N – прогнозируемое число воздействий угроз;

$\hat{\eta}_{m,k,n}$ – верхняя граница времени до k-го воздействия угрозы $u_m \in U$ по элементу a_k при воздействии угрозы n. Из всех актуальных угроз U для каждого воздействия n выбирается угроза с индексом $u_{m^*} \in U$ для которой

$$\hat{\eta}_{m^*,k,n} = \max_{\substack{m=1,2,\ldots N_U,\\ n=1,\ldots N}} \hat{\eta}_{m,k,n}$$

где $m = 1, \ldots, N_U$, N_U – число актуальных угроз; $k = 1, \ldots, N_E$; $k = 1, \ldots, N_E$, N_E – число элементов СОФ; $n = 1, \ldots, N_U$, N – прогнозируемое число воздействий угроз.

2. Оценка требуемых ресурсов для восстановления функциональности элемента, пораженного в результате воздействия угроз (формируется в результате технической разведки)

$$\hat{\Theta} = \{\hat{d}_{k,m,i}, \hat{r}_{k,m,j}\},$$

где $\hat{d}_{k,m,i}$ – требуемый возобновляемый ресурс i-го типа для восстановления функциональности поврежденного элемента k при воздействии угрозы $u_m \in U$, $i = 1, 2, \ldots, N_D$, N_D – число типов (классификаторов) возобновляемого ресурса. Из всех комбинаций индексов элементов k и угроз m $\langle k, m\rangle$ выбирается комбинация $\langle k^*, m^*\rangle$, при которой возобновляемый ресурс с индексом i имел бы максимальное число единиц учета

$$\hat{d}_i\langle k^*, m^*\rangle = \max_{\substack{k=1,2,\ldots N_E,\\ m=1,2,\ldots N_U}} \hat{d}_i\langle k, m\rangle,$$

где $\hat{r}_{k,m,j}$ – требуемый невозобновляемый ресурс j-го типа для восстановления функциональности поврежденного элемента k при воздействии угрозы $u_m \in U$, $j = 1, 2, \ldots, N_R$, N_R – число типов (классификаторов) невозобновляемого ресурса. Из всех комбинаций индексов элементов k и угроз m $\langle k, m\rangle$ выбирается комбинация $\langle k^*, m^*\rangle$, при которой невозобновляемый ресурс с индексом j имел бы максимальное число единиц учета

$$\hat{r}_j\langle k^*, m^*\rangle = \max_{\substack{k=1,2,\ldots N_E,\\ m=1,2,\ldots N_U}} \hat{r}_j\langle k, m\rangle.$$

3. $\text{К}_{\text{Тр}}$ – совокупность требований по обеспечению конфиденциальности.

4. $\text{Ц}_{\text{Тр}}$ – совокупность требований по обеспечению целостности.

Обобщенная схема неуправляемых факторов приведена на рис. 2.

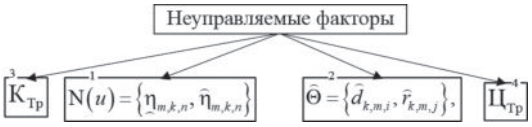


Рис. 2. Неуправляемые факторы, определяющие устойчивость объекта оценивания

Ограничения

1. При оценивании устойчивости объектов КИИ принимается, что возможность поражения элементов АСУ и ИС, на практике означает их стопроцентную готовность к информационному обмену.
2. Соответствие конфиденциальности информации требованиям на всем периоде воздействия угроз $t \in (0, T]$, $\text{К}(t) \underset{t\in(0,T]}{\in} \text{К}_{\text{Тр}}$, где $\text{К}(t)$ – совокупность требований по обеспечению конфиденциальности реализованных в момент времени $t \in (0, T]$.
3. Соответствие целостности информации требованиям на всем периоде воздействия угроз $t \in (0, T]$, $\text{Ц}(t) \in \text{Ц}_{\text{Тр}}$, где $\text{Ц}(t)$ – совокупность требований по обеспечению целостности информации реализованных в момент времени $t \in (0, T]$.

Рис. 3. Обобщённая схема ограничений, которые учитываются при оценке устойчивости

Требуется разработать

1. Семейство методов, моделей и средств математической обработки исходных данных (оператор) – $\mathcal{M}$, позволяющих получать количественные оценки показателей, характеризующих устойчивость функционирования элементов оцениваемого объекта, находящихся под воздействием угроз $u \in U$

$$\{\varphi_k(u,t)\} \underset{\substack{t\in(0,T]\\ u\in U\\ \text{К}(t)\in \text{К}_{\text{Тр}}\\ \text{Ц}(t)\in \text{Ц}_{\text{Тр}}}}{=} \mathcal{M}\{E(t_0), U, K_{\text{Ог}}, P(u), \text{Т}(u,t), \Theta(t), \text{Н}(u), \hat{\Theta}\},$$

где $\{\varphi_k(u,t)\}$ – семейство функций устойчивости, характеризующих устойчивость функционирования элементов объекта оценивания, находящихся под воздействием угроз $u \in U$, $\varphi_k(u,t)$ – частная функция устойчивости k-го элемента.

2. Семейство методов, моделей и средств математической обработки исходных данных (оператор) – $\mathcal{B}$, характеризующих семейство функций устойчивости отдельных элементов объекта оценивания $\varphi_k(u,t)$ и ее структуру $S(t)$ – и позволяющие получать количественную оценку, характеризующую устойчивость функционирования объекта оценивания в целом, находящуюся под воздействием угроз $u \in U$

$$\Phi(t) = \mathcal{B}\{\varphi_k(u,t), S(t), \hat{\Theta}\} =$$
$$= \mathcal{B}\{\mathcal{M}\{E(t_0), U, K_{\text{Ог}}, P(\text{u}), \text{Т}(u,t), \Theta(t), \text{Н}(u,t)\}, S(t), \hat{\Theta}\},$$

где $\Phi(t)$ – функция устойчивости объекта оценивания, находящейся под воздействием угроз, $\mathcal{B}$ – оператор, позволяющий отобразить семейство частных функций устойчивости элементов объекта оценивания в функцию устойчивости объекта оценивания в целом.

Функциональная схема математической модели оценивания устойчивости приведена на рис. 4. Исходные данные, характеризующие условия функционирования элементов объекта оценивания, добываются для каждого отдельного элемента при использовании как детерминированных методов, так и методов экспертного оценивания. Исходные данные вводятся для каждой частной математической модели элементов объекта оценивания. Зеленым цветом обозначены исходные данные, которые могут управляться ЛПР, красным цветом – неуправляемые исходные данные. Аналогично вводятся параметры, характеризующие ограничения. Каждая частная модель элементов в соответствии с линейными операторами $\mathcal{M}_i$ преобразует исходные данные в поле принятых ограничений в функции устойчивости отдельных элементов, которые являются исходными данными для расчета функции устойчивости объекта оценивания в целом $\Phi(t)$. Для чего значения функций устойчивости отдельных элементов, совместно с показателями, характеризующими СОФ и ресурсные возможности СВФ подаются на вход математической модели объекта оценивания, которая с помощью линейного оператора $\mathcal{B}$ осуществляет преобразование исходных данных в значения функции устойчивости объекта оценивания.

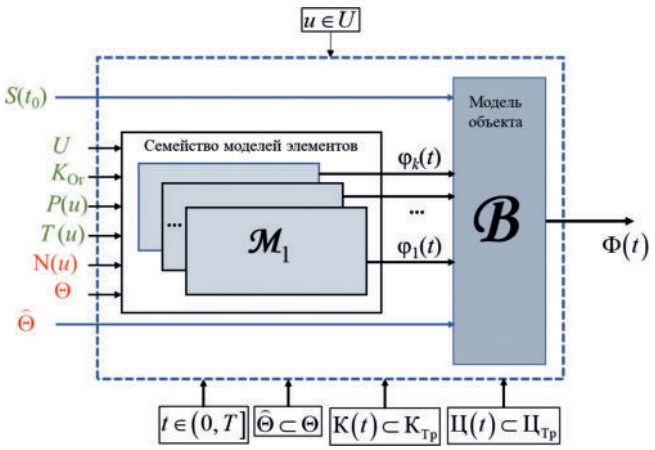


Рис. 4. Функциональная схема математической модели оценивания устойчивости

Зная количественные оценки экстремальных значений функции устойчивости и моментов времени их наступления, ЛПР представляется возможным обосновать принимаемое решение по обеспечению устойчивости функционирования объекта оценивания.

Выводы

В результате настоящего исследования предложены вербальная и формальная постановки научной задачи по оцениванию устойчивости функционирования объектов КИИ, элементы которых подвержены воздействию угроз их информационной безопасности. Обнаружена ограниченность существующих методов и моделей на решение задач оценивания устойчивости для условий штатной эксплуатации, которые без грубых допущений не могут быть применены для оценивания устойчивости функционирования КИИ, находящейся под воздействием угроз. Обнаружена противоречивая ситуация, когда возможности науки вступают в противоречие с потребностями практики и поставленная задача может позиционироваться как научная проблема, решение которой имеет важное экономическое значение. Для решения научной задачи были разработаны соответствующие методы и математические модели, которые опубликованы в [16–18]. Предполагается дальнейшие исследования направить на разработку формальных и экспертных методов формирования исходных данных.

При поддержке Фонда Потанина

Литература

1. *Воеводин В. А. Генезис понятия структурной устойчивости информационной инфраструктуры автоматизированной системы управления производственными процессами к воздействию целенаправленных угроз информационной безопасности. Вестник Воронежского института ФСИН России, 2023, № 2, апрель-июнь. – С. 30–41.*
2. *Зубков Е. А. Оценка киберустойчивости сетевой инфраструктуры с использованием распределенного механизма анализа и мониторинга / Е. А. Зубков, В. О. Ерастов, Д. П. Зегжда // Методы и технические средства обеспечения безопасности информации. – 2024. – № 33. – С. 14–16.*
3. *Зегжда Д. П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / под ред. Д. П. Зегжды. – М.: Горячая линия – Телеком. 2022. – 560 с.*
4. *Израилов К. Е. Оценивание и прогнозирование состояния сложных объектов: применение для информационной безопасности / К. Е. Израилов, М. В. Буйневич, И. В. Котенко, В. А. Десницкий // Вопросы кибербезопасности. – 2022. – № 6(52). – С. 2-21. – DOI 10.21681/23113456-6-2022-2-21.*
5. *Котенко И. В. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации / И. В. Котенко, И. Б. Саенко, Р. И. Захарченко, Д. В. Величко // Вопросы кибербезопасности. – 2023. – № 1(53). – С. 13–27. – DOI 10.21681/2311-3456-2023-1-13-27.*
6. *Коноваленко С. А. Методика оценивания функциональной устойчивости гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Системы управления, связи и безопасности. 2023. № 4. С. 157–195. doi: 10.24412/2410-9916-2023-4-157-195.*
7. *Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. 337 с.*
8. *Стародубцев Ю. И. Концептуальные направления решения проблемы обеспечения устойчивости Единой сети электросвязи Российской Федерации / Ю. И. Стародубцев, С. А. Иванов, П. В. Закалкин // Военная мысль. – 2021. – № 4. – С. 39–49.*
9. *Стародубцев Ю. И. Кибероружие как основное средство воздействия на критическую инфраструктуру государств / Ю. И. Стародубцев, П. В. Закалкин, С. А. Иванов // Вестник Академии военных наук. – 2022. – № 1(78). – С. 24–32.*
10. *Язов Ю. К. Составные сети Петри-Маркова со специальными условиями построения для моделирования угроз безопасности информации / Ю. К. Язов, А. П. Панфилов // Вопросы кибербезопасности. – 2024. – № 2(60). – С. 53–65. – DOI 10.21681/2311-3456-2024-2-53-65.*
11. *Язов Ю. К., Соловьев С. В. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа. – СПб.: Наукоемкие технологии. 2023. – 257 с.*
12. *Язов Ю. К. Основы теории составных сетей Петри-Маркова и их применения для моделирования процессов реализации угроз безопасности информации в информационных системах / Ю. К. Язов, А. В. Анищенко, А. С. Суховерхов. – Санкт-Петербург: Издательский дом «Сциентиа», 2024. – 194 с. – ISBN 978-5-605-21112-9. – DOI 10.32415/scientia_978-5-6052111-2-9.*
13. *Шубинский И. Б. О функциональной безопасности сложной технической системы управления с цифровыми двойниками / И. Б. Шубинский, Х. Шебе, Е. Н. Розенберг // Надежность. – 2021. – Т. 21, № 1. – С. 38–44.– DOI 10.21683/1729-2646-2021-21-1-38-44.*
14. *Shubinsky I. B. Methods for ensuring and proving functional safety of automatic train operation systems / I. B. Shubinsky, E. N. Rozenberg, H. Schabe // Reliability: Theory & Applications. – 2024. – Vol. 19, No. 1(77). – P. 360–375. – DOI 10.24412/1932-2321-2024-177-360-375.*
15. *Shubinsky, I. B. Innovative methods of ensuring the functional safety of train control systems / I. B. Shubinsky E. N. Rozenberg, H. Schabe // Reliability: Theory & Applications. – 2023. – Vol. 18, No. 4(76). – P. 909–920. – DOI 10.24412/1932-2321-2023-476-909-920.*
16. *Воеводин В. А. Модель оценки функциональной устойчивости информационной инфраструктуры для условий воздействия множества компьютерных атак // Информатика и автоматизация. 2023. № 22(3). С. 691–715. DOI 10.15622/ia.22.3.8.*
17. *Воеводин В. А. Частная полумарковская модель как инструмент снижения сложности задачи оценивания устойчивости функционирования элементов информационной инфраструктуры, подверженной воздействию угроз // Информатика и автоматизация. 2024. № 23(3). С. 611–642. doi.org/10.15622/ia.23.3.1.*
18. *Воеводин В. А., Крахотин Н. А. Методы оценивания связности неориентированного двухполюсного помеченного графа с учетом деструктивного воздействия внешних угроз на его вершины // Вестник Дагестанского государственного технического университета. Технические науки. 2024. № 51(1). С. 46–60. doi:10.21822/2073-6185-2024-51-1-46-60.*

ON THE FORMULATION OF THE TASK OF ASSESSING THE STABILITY OF THE FUNCTIONING OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Voevodin V. A.[7]

Keywords: *threats of information security violations, a system for restoring functionality, critical information infrastructure, recoverability, protection from threats, a renewable resource, a non-renewable resource.*

7 Vladislav A. Voevodin, Ph.D. in Technical Sciences, MIET, Moscow, Russia. E-mail: vva541@mail.ru. AuthorID: 1012813, ORCID 0009-0003-9431-1685.

The purpose of the study: *is to substantiate the relevance, formulate and formalize the scientific task of quantifying the stability of the functioning of a critical information infrastructure in relation to the conditions of exposure to threats of violation of its information security.*

Research methods: *system analysis, analysis of a scientific problem, formalization of scientific knowledge, methodology of scientific research.*

The results obtained: *the verbal and formal statements of the scientific problem are formulated.*

Scientific novelty: *the author's approach to assessing the dynamics of the stability of the functioning of critical information infrastructure in the face of threats, taking into account the available resource, is proposed.*

Practical significance: *The developed formulation of the scientific problem can serve as the basis for the formulation of the terms of reference for the development of methods, models and tools for quantifying the stability of the functioning of objects of critical information structure operating under the influence of threats.*

References

1. *Voevodin V. A. Genezis ponjatija strukturnoj ustojchivosti informacionnoj infrastruktury avtomatizirovannoj sistemy upravlenija proizvodstvennymi processami k vozdejstviju celenapravlennyh ugroz informacionnoj bezopasnosti. Vestnik Voronezhskogo instituta FSIN Rossii, 2023, № 2, aprel'-ijun'. – S. 30–41.*
2. *Zubkov E. A. Ocenka kiberustojchivosti setevoj infrastruktury s ispol'zovaniem raspredelennogo mehanizma analiza i monitoringa / E. A. Zubkov, V. O. Erastov, D. P. Zegzhda // Metody i tehnicheskie sredstva obespechenija bezopasnosti informacii. – 2024. – № 33. – S. 14–16.*
3. *Zegzhda D. P. Kiberbezopasnost' cifrovoj industrii. Teorija i praktika funkcional'noj ustojchivosti k kiberatakam / pod red. D. P. Zegzhdy. – M.: Gorjachaja linija – Telekom. 2022. – 560 s.*
4. *Izrailov K. E. Ocenivanie i prognozirovanie sostojanija slozhnyh ob#ektov: primenenie dlja informacionnoj bezopasnosti / K. E. Izrailov, M. V. Bujnevich, I. V. Kotenko, V. A. Desnickij // Voprosy kiberbezopasnosti. – 2022. – № 6(52). – S. 2-21. – DOI 10.21681/23113456-6-2022-2-21.*
5. *Kotenko I. V. Podsistema preduprezhdenija komp'juternyh atak na ob#ekty kriticheskoj informacionnoj infrastruktury: analiz funkcionirovanija i realizacii / I. V. Kotenko, I. B. Saenko, R. I. Zaharchenko, D. V. Velichko // Voprosy kiberbezopasnosti. – 2023. – № 1(53). – S. 13–27. – DOI 10.21681/2311-3456-2023-1-13-27.*
6. *Konovalenko S. A. Metodika ocenivanija funkcional'noj ustojchivosti geterogennoj sistemy obnaruzhenija, preduprezhdenija i likvidacii posledstvij komp'juternyh atak // Sistemy upravlenija, svjazi i bezopasnosti. 2023. № 4. S. 157-195. doi: 10.24412/2410-9916-2023-4-157-195.*
7. *Makarenko S. I. Modeli sistemy svjazi v uslovijah prednamerennyh destabilizirujushhih vozdejstvij i vedenija razvedki. Monografija. – SPb.: Naukoemkie tehnologii, 2020. 337 s.*
8. *Starodubcev Ju. I. Konceptual'nye napravlenija reshenija problemy obespechenija ustojchivosti Edinoj seti jelektrosvjazi Rossijskoj Federacii / Ju. I. Starodubcev, S. A. Ivanov, P. V. Zakalkin // Voennaja mysl'. – 2021. – № 4. – S. 39–49.*
9. *Starodubcev Ju. I. Kiberoruzhie kak osnovnoe sredstvo vozdejstvija na kriticheskuju infrastrukturu gosudarstv / Ju. I. Starodubcev, P. V. Zakalkin, S. A. Ivanov // Vestnik Akademii voennyh nauk. – 2022. – № 1(78). – S. 24–32.*
10. *Jazov Ju. K. Sostavnye seti Petri-Markova so special'nymi uslovijami postroenija dlja modelirovanija ugroz bezopasnosti informacii / Ju. K. Jazov, A. P. Panfilov // Voprosy kiberbezopasnosti. – 2024. – № 2(60). – S. 53–65. – DOI 10.21681/2311-3456-2024-2-53-65.*
11. *Jazov Ju. K., Solov'ev S. V. Metodologija ocenki jeffektivnosti zashhity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa. – SPb.: Naukoemkie tehnologii. 2023. – 257 s.*
12. *Jazov Ju. K. Osnovy teorii sostavnyh setej Petri-Markova i ih primenenija dlja modelirovanija processov realizacii ugroz bezopasnosti informacii v informacionnyh sistemah / Ju. K. Jazov, A. V. Anishhenko, A. S. Suhoverhov. – Sankt-Peterburg : Izdatel'skij dom «Scientia», 2024. – 194 s. – ISBN 978-5-605-21112-9. – DOI 10.32415/scientia_978-5-6052111-2-9.*
13. *Shubinskij I. B. O funkcional'noj bezopasnosti slozhnoj tehnicheskoj sistemy upravlenija s cifrovymi dvojnikami / I. B. Shubinskij, H. Shebe, E. N. Rozenberg // Nadezhnost'. – 2021. – T. 21, № 1. – S. 38–44. – DOI 10.21683/1729-2646-2021-21-1-38-44.*
14. *Shubinsky I. B. Methods for ensuring and proving functional safety of automatic train operation systems / I. B. Shubinsky, E. N. Rozenberg, H. Schabe // Reliability: Theory & Applications. – 2024. – Vol. 19, No. 1(77). – P. 360–375. – DOI 10.24412/1932-2321-2024-177-360-375.*
15. *Shubinsky, I. B. Innovative methods of ensuring the functional safety of train control systems / I. B. Shubinsky E. N. Rozenberg, H. Schabe // Reliability: Theory & Applications. – 2023. – Vol. 18, No. 4(76). – P. 909–920. – DOI 10.24412/1932-2321-2023-476-909-920.*
16. *Voevodin V. A. Model' ocenki funkcional'noj ustojchivosti informacionnoj infrastruktury dlja uslovij vozdejstvija mnozhestva komp'juternyh atak // Informatika i avtomatizacija. 2023. № 22(3). S. 691–715. DOI 10.15622/ia.22.3.8.*
17. *Voevodin V. A. Chastnaja polumarkovskaja model' kak instrument snizhenija slozhnosti zadachi ocenivanija ustojchivosti funkcionirovanija jelementov informacionnoj infrastruktury, podverzhennoj vozdejstviju ugroz // Informatika i avtomatizacija. 2024. № 23(3). S. 611–642. doi.org/10.15622/ia.23.3.1.*
18. *Voevodin V. A., Krahotin N. A. Metody ocenivanija svjaznosti neorientirovannogo dvuhpoljusnogo pomechennogo grafa s uchetom destruktivnogo vozdejstvija vneshnih ugroz na ego vershiny // Vestnik Dagestanskogo gosudarstvennogo tehnicheskogo universiteta. Tehnicheskie nauki. 2024. № 51(1). S. 46–60. doi:10.21822/2073-6185-2024-51-1-46-60.*

МОДЕЛЬ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ И АЛГОРИТМ ОПРЕДЕЛЕНИЯ ОПТИМАЛЬНЫХ ЗНАЧЕНИЙ КОНФИГУРИРУЕМЫХ ПАРАМЕТРОВ ВЕБ-СЛУЖБЫ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Каверин С. С.[1], Максимов Р. В.[2], Москвин А. А.[3]

DOI: 10.21681/2311-3456-2025-1-50-62

Цель исследования: *повышение защищенности веб-службы корпоративных информационных систем в условиях сетевой разведки.*

Используемые методы: *оптимизации по Парето, идеальной точки, Нелдера-Мида, роя частиц, имитации отжига.*

Результат исследования: *разработана модель функционирования веб-службы корпоративных информационных систем в условиях сетевой разведки, которая реализована в виде полумарковского случайного процесса с дискретными состояниями и непрерывным временем. Получены вероятностно-временные характеристики исследуемых процессов, которые необходимы для определения оптимального режима конфигурирования параметров веб-службы.*

Решена задача векторной оптимизации для определения оптимальных значений параметров веб-службы корпоративных информационных систем, таких как количество фрагментов HTTP-ответа, время между этими фрагментами, а также количество ложных веб-серверов, позволяющих максимизировать результативность защиты веб-службы корпоративных информационных систем и минимизировать вероятность отказа ложных веб-серверов при соответствующих ограничениях.

Научная новизна: *заключается в разработке модели и алгоритма поиска оптимальных параметров веб-службы корпоративных информационных систем в условиях сетевой разведки с применением математического аппарата полумарковских случайных процессов и скаляризацией задачи векторной оптимизации методом идеальной точки.*

Ключевые слова: *случайный процесс, вероятностно-временные характеристики, веб-ресурсы, метод идеальной точки, веб-сессия, интервально-переходные вероятности, сетевая разведка.*

Введение

В условиях активной внешнеполитической деятельности нашей страны наблюдается заметный рост числа кибератак на веб-службы. Общие тенденции в кибербезопасности показывают, что такие порталы, как «Госуслуги», «Личный кабинет ПФР», где обрабатывается большое количество персональных данных, остаются основными целями для кибератак, таких как фишинг, атаки на учетные записи и компрометация данных. Проблемы, связанные со взломом паролей, подстановкой учетных данных и использованием словарных атак, стали одними из ключевых в сфере кибербезопасности. Атаки, направленные на взлом учетных записей, представляют существенную угрозу для пользователей и организаций, часто вызывая значительные финансовые потери и ущерб репутации. Даже несмотря на применяемые средства защиты, ввиду использования импортного оборудования, а также сетей связи общего пользования и недостаточной степени доверия к открытому программному обеспечению, данные угрозы остаются актуальными [1]. Веб-службы делятся на несколько типов в зависимости от их назначения и архитектуры:

1. RESTful веб-службы. Используют протокол HTTP для обмена данными. Основаны на стандартах и предоставляют доступ через URL.
2. SOAP веб-службы. Имеют более сложную структуру, используют XML для передачи данных. Поддерживают сложные сценарии взаимодействия.
3. GraphQL веб-службы. Современные API, позволяющие клиенту запрашивать данные, определяя их структуру.
4. RPC (Remote Procedure Call). Позволяют удалённый вызов процедур.

1 Каверин Сергей Сергеевич, адъюнкт, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: sergey_kav995@mail.ru

2 Максимов Роман Викторович, доктор технических наук, профессор, Заслуженный изобретатель Российской Федерации, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: rvmaxim@yandex.ru

3 Москвин Артем Александрович, кандидат технических наук, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: tema.kg9012@gmail.com

К основным типам атак на веб-службы относятся следующие.

1. DDoS-атаки. Наблюдался рост сложности и частоты атак типа DDoS (Distributed Denial of Service), направленных на веб-приложения и API. В частности, Cloudflare[4] сообщила о 466% росте атак на отдельные страны и индустрии, такие как игры и IT-компании, что обусловлено как политическими мотивами, так и финансовыми интересами злоумышленников.
2. Атаки на API. Около 60% динамического трафика веб-приложений связано с API, что делает их привлекательной целью для атак. Исследования показывают, что многие компании не осознают масштаба своего API-трафика, и около четверти API являются «теневыми», что создает дополнительные риски.
3. Боты и автоматизация атак. Около 31% всего веб-трафика приходится на боты, из которых 93% считаются потенциально вредоносными. Они используются для различных атак, включая кражу учетных данных, инвентаризацию сайтов и проведение атак на доступность.
4. Уязвимости веб-приложений. Отчет от Edgescan[5] показал, что среднее время на устранение критических уязвимостей увеличилось, что создает длительные окна для злоумышленников. Основными уязвимостями остаются SQL-инъекции, XSS (межсайтовый скриптинг) и атаки на авторизацию.
5. Фишинг и социальная инженерия. По данным на 2024 год, 96% фишинговых атак распространяются через email, и эти атаки стали основным методом для получения доступа к веб-приложениям и учетным записям пользователей. Атаки на компании с использованием фишинга остаются основной угрозой для бизнеса.

Все эти атаки особенно опасны в условиях, когда многие пользователи продолжают использовать простые и легко угадываемые пароли. Кроме того, тенденция к повторному использованию паролей на различных веб-ресурсах делает успешную атаку на один ресурс потенциальной угрозой для всех остальных, где используются те же учетные данные.

Ключевым этапом подготовки компьютерных атак является сетевая разведка, цель которой – сбор информации о составе, структуре, алгоритмах работы, местоположении и принадлежности компонентов веб-системы, а также анализ обрабатываемых и хранимых данных. Этот процесс необходим для выявления потенциальных целей, уязвимостей и централизации усилий при осуществлении атак или других вредоносных воздействий.

Анализ публикаций [2–5] в сфере противодействия сетевой разведке показывает, что активно развиваются технологии как для защиты информационных систем от исследуемых угроз, так и для реализации сетевой разведки и компьютерных атак. Например, в контексте веб-службы защита от таких методов, как подбор паролей по словарю и подстановка учетных данных с целью обеспечения конфиденциальности и целостности данных, реализуется через использование сложных паролей, блокировки учетных записей, многофакторной аутентификации и ограничений на частоту запросов.

С другой стороны, методы атак на персональные данные со стороны злоумышленников продолжают совершенствоваться, что затрудняет обеспечение должной защиты веб-службы корпоративных информационных систем. В то же время, возможности протоколов, поддерживающих работу этой веб-службы, позволяют конфигурировать параметры с использованием сетевых «ловушек» (network tarpits) [6–8] и обманных систем (deception systems). Сетевые ловушки — это технологии или подходы, используемые для обмана, замедления или анализа действий злоумышленников, взаимодействующих с веб-службой. Эти ловушки имитируют работу системы, создавая иллюзию нормального функционирования, но при этом затрудняют или делают бесполезными попытки атак. Основная цель – защитить основные ресурсы системы, снизить эффективность атаки и собрать информацию о методах злоумышленника. В контексте защиты веб-службы использование таких технологий, как сетевые «ловушки», может быть следующим:

1. Замедление атак. Сетевая ловушка искусственно увеличивает время отклика сервера для подозрительных запросов. Это особенно эффективно против автоматизированных атак, таких как brute force или DDoS.
2. Обман злоумышленников. Создание фальшивых веб-серверов или API-методов для введения, атакующих в заблуждение. Например, злоумышленник взаимодействует с фальшивой системой, расходуя ресурсы на бесполезные действия, и вместо настоящих данных сервера получает поддельные ответы.
3. Снижение эффективности сканирования. Сетевые ловушки замедляют работу автоматизированных инструментов, таких как сканеры уязвимостей, за счёт имитации «медленных» соединений.
4. Анализ атак. Сетевые ловушки могут собирать данные о действиях злоумышленников, предоставляя администраторам информацию о потенциальных векторах атак.

4 Отчет по кибератакам на веб-приложения от Cloudflare, URL: https://newsletter.radensa.ru/wp-content/uploads/2024/10/BDES-5907_State-of-App-Security-2024.pdf

5 Отчет по уязвимостям веб-приложений от Edgescan, URL: https://info.edgescan.com/hubfs/23DOWNLOADABLE%20CONTENT/Vulnerability%20Statistics%20Reports/Edgescan_VulnerabilityStatsReport2024.pdf

5. Перенаправление атак. Сетевые ловушки могут перенаправлять избыточный трафик на фальшивые ресурсы, предотвращая перегрузку основных серверов.

Веб-система представляет собой интегрированное программное решение, включающее в себя веб-клиентов, веб-серверы, базы данных, приложения для обработки бизнес-логики, пользовательские интерфейсы и средства обеспечения безопасности. Ее архитектура основана на клиент-серверной модели, что позволяет эффективно распределять ресурсы и централизованно управлять данными. Веб-система работает в рамках стека сетевых протоколов TCP/IP. Обмен информацией между веб-клиентами и веб-серверами осуществляется через протокол прикладного уровня HTTP в модели OSI, предназначенный для передачи гипертекстовых документов по сети, в частности, через интернет. Протокол HTTP описывается в нескольких RFC (Request for Comments), в том числе:

1. RFC 2616 – «Hypertext Transfer Protocol – HTTP/1.1». Этот RFC был основным для HTTP/1.1, и в нем подробно описаны все аспекты работы протокола: методы, структура сообщений, коды состояния, заголовки, кэширование и другие.
2. RFC 7230-7235 – «Hypertext Transfer Protocol (HTTP/1.1)». В 2014 году был выпущен набор из шести документов, который обновил и уточнил спецификации, содержащиеся в RFC 2616. Эти документы описывают HTTP/1.1 и более детально регламентируют все аспекты протокола.
3. RFC 7540 – «HTTP/2». Этот RFC описывает протокол HTTP/2, который улучшает производительность за счет использования бинарных фреймов и мультиплексирования запросов.
4. RFC 9000 – «QUIC: A UDP-based Multiplexed and Secure Transport». RFC 9000 описывает HTTP/3, который использует протокол QUIC для повышения скорости и безопасности соединений.

После установления коммуникационного канала и согласования параметров веб-клиент инициирует веб-сессию, отправляя последовательность запросов к веб-серверу для получения необходимых веб-ресурсов, на которые веб-сервер, в свою очередь, отвечает.

Веб-клиент устанавливает соединение (чаще всего через веб-браузер) с веб-сервером через порт 80 для HTTP или 443 для HTTPS, он отправляет запрос, включающий метод (например, GET или POST), URL запрашиваемого ресурса, версию протокола HTTP и дополнительные заголовки, если это необходимо. Следующим шагом является обработка сервером этого запроса. Он может включать в себя обращение к базе данных, выполнение серверного скрипта или просто выборку статического файла. Далее сервер отправляет ответ клиенту, который содержит статусный код (например, 200 для успешного запроса), версию протокола HTTP, заголовки ответа и тело сообщения (например, HTML-документ). Клиент получает ответ и обрабатывает его. Если это HTML-документ, браузер анализирует HTML, CSS, JavaScript, а затем отображает страницу пользователю. Последним этапом является закрытие соединения, которое происходит после завершения передачи данных. Каждый запрос в HTTP является отдельным и независимым. После завершения передачи данных соединение между клиентом и сервером закрывается. В отличие от других протоколов, таких как FTP, HTTP не требует постоянного поддержания соединения. Однако в HTTP/1.1 и более поздних версиях может использоваться постоянное соединение для отправки нескольких запросов через одно соединение. Диалог между клиентом и сервером осуществляется поэтапно: запрос – ответ – запрос. Исходя из этого управление процессом текущей веб-сессии может осуществляться через передачу сервером HTTP-ответа, разделенного на фрагменты d_1, d_2, ..., d_n, в ответ на запрос клиента. Передача данных осуществляется с изменяемыми интервалами времени T_1, T_2, ..., T_n, [2] как показано на рисунке 1.

Для исчерпания временного ресурса средств злоумышленника за счет имитации веб-сессии низкого качества, а также введения неопределенности посредством создания в сети ложных веб-серверов, необходимо разработать модель функционирования корпоративной сети передачи данных при конфигурировании параметров веб-службы и использовании ложных сетевых информационных объектов, а также алгоритма определения оптимальных значений этих параметров [9–11].

Модель функционирования корпоративной сети передачи данных при конфигурировании параметров веб-службы

Разработанная модель включает в себя два случайных процесса с дискретными состояниями, описывающими различные этапы работы HTTP-протокола.

С одной стороны, этапы жизненного цикла веб-службы (далее – система V), представлены как случайный процесс с дискретными состояниями и непрерывным временем. В качестве дискретных состояний выступают этапы функционирования системы V, а эволюция системы происходит под воздействием случайных событий, таких как получение и отправка HTTP-запросов.

С другой стороны, процесс функционирования ложных веб-серверов в условиях ведения сетевой разведки (далее – система D) может быть представлен в виде многоканальной системы массового обслуживания с отказами, в которую поступает поток

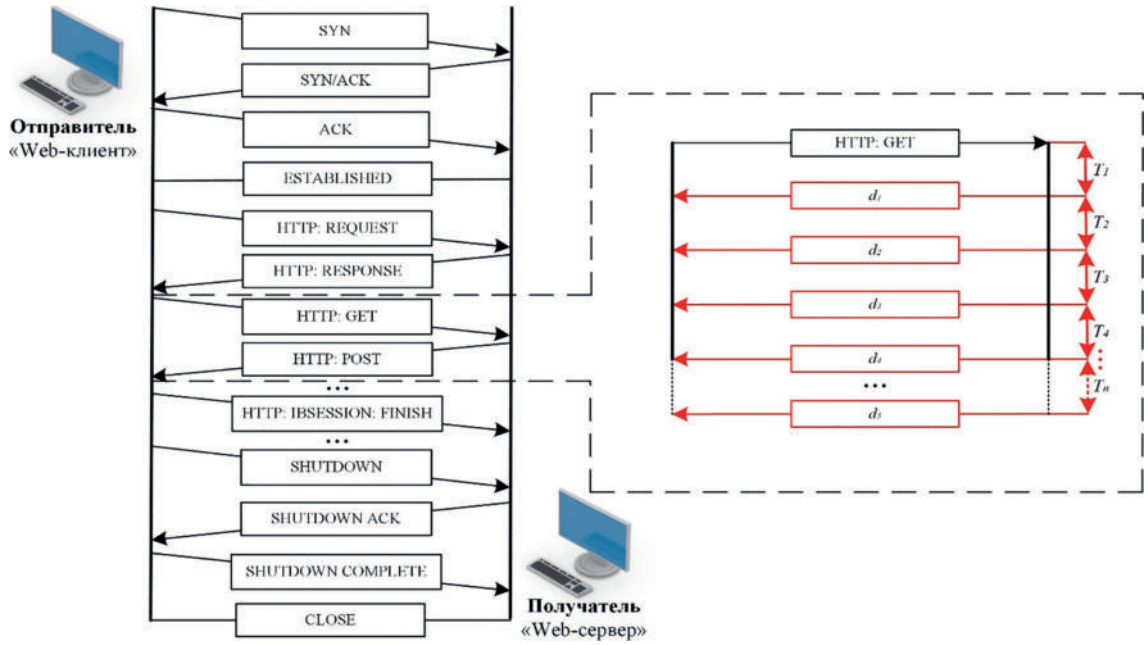


Рис. 1. Процесс установления веб-сессии HTTP и направления веб-сервером на поступивший от клиента HTTP-запрос последующего HTTP-ответа, разделенного на фрагменты d_1, d_2, ..., d_n через изменяемые интервалы времени T_1, T_2, ..., T_n

заявок на доступ к ложным веб-серверам. Число возможных состояний этого случайного процесса определяется количеством ложных веб-серверов.

Основные вероятностные характеристики полумарковского процесса включают в себя: функцию распределения времени ожидания перехода из состояния i в состояние j (далее – $F_{ij}(t)$), и вероятности этого перехода (далее – p_{ij}). На рисунке 2 представлен ориентированный граф случайного процесса для системы V, в таблице 1 описаны его дискретные состояния, а в таблице 2 содержатся вероятностные характеристики.

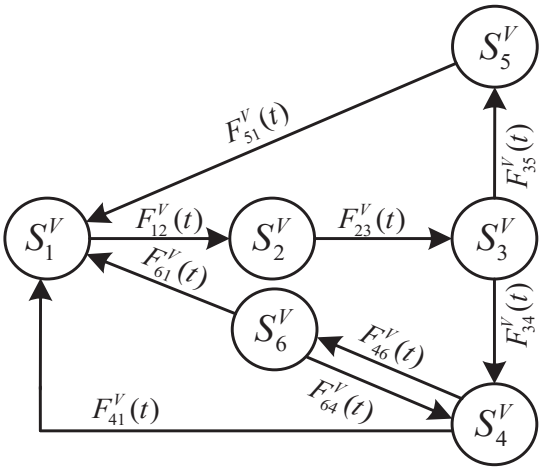


Рис. 2. Граф состояний системы V

Предположим, что вероятностные характеристики исследуемых процессов, в силу выполнения свойств простейшего потока, подчиняются экспоненциальному закону распределения [12]:

$$F_{ij}(t) = 1 - e^{-\lambda_{ij} t}, \quad (1)$$

$$p_{ij} = \int_0^\infty f_{ij}(t) \prod_{k=1,k\neq j}^{n} (1 - F_{ik}(t))\, dt, \quad (2)$$

где: λ_{ij} – интенсивности потока событий, которые переводят исследуемые системы из состояния i в состояние j, $f_{ij}(t)$ – функция плотности распределения времени ожидания перехода из состояния i в состояние j. На рисунке 3 представлен ориентированный граф случайного процесса для системы D, таблице 3 содержит описание его дискретных состояний, а в таблице 4 приведены вероятностные характеристики.

Система D содержит n ложных веб-серверов и является многоканальной системой массового обслуживания с отказами. В систему поступает один тип заявок (поток является однородным). Все ложные веб-серверы идентичны, следовательно, любая заявка может быть обработана любым ложным веб-сервером за одинаковое случайное время. Заявки, поступающие в систему D, образуют простейший поток с интенсивностью подключений сетевой разведки (network reconnaissance) λnr. Время обслуживания заявок на любом из ложных веб-серверов подчиняется экспоненциальному закону с интенсивностью:

$$\mu = \frac{n_{ch}}{d \cdot T_{res}}, \quad (3)$$

где: d – количество фрагментов, на которые разделен HTTP-ответ, T_{res} – время между фрагментами HTTP-ответа, n_{ch} – количество возможных активных

Таблица 1.

Дискретные состояния системы V

Дискретные состояния	Описание состояний
S_1^V	ожидание сервером поступления от клиента (нарушителя) на порт 80 TCP пакетов с флагом SYN на установление сетевого соединения (клиент (нарушитель) и веб-сервер находятся в состоянии простоя)
S_2^V	ожидание веб-сервером поступления от клиента (нарушителя) HTTP-запроса с методом GET на предоставление запрашиваемого веб-ресурса
S_3^V	ожидание клиентом поступления от веб-сервера HTTP-ответа об успешной авторизации с кодом состояния 200 OK и установления легитимной веб-сессии или ожидание нарушителем перенаправления его на ложный веб-сервер после 3 неудачных попыток авторизации
S_4^V	ожидание нарушителем после очередной попытки авторизации окончания поступления от ложного веб-сервера множества промежуточных откликов, разделенных на фрагменты, направляемые через изменяемые интервалы времени или окончания веб-сессии между нарушителем и ложным веб-сервером
S_5^V	ожидание окончания веб-сессии между клиентом и веб-сервером
S_6^V	ожидание очередной попытки нарушителя авторизоваться на ложном веб-сервере

Таблица 2.

Вероятностные характеристики процесса функционирования системы V

Переменная	Описание вероятностных характеристик
$F_{12}^V(t)$	функция распределения времени ожидания веб-сервером поступления от клиента (нарушителя) на порт 80 TCP пакетов с флагом SYN на установление сетевого соединения
$F_{23}^V(t)$	функция распределения времени ожидания веб-сервером поступления от клиента (нарушителя) HTTP-запроса с методом GET на аутентификацию в запрашиваемом веб-ресурсе
$F_{34}^V(t)$	функция распределения времени ожидания нарушителем перенаправления его на ложный веб-сервер после 3 неудачных попыток авторизации
$F_{35}^V(t)$	функция распределения времени ожидания клиентом поступления от сервера HTTP-ответа об успешной авторизации клиента с кодом состояния 200 OK и установления легитимной веб-сессии
$F_{41}^V(t)$	функция распределения времени ожидания окончания информационного обмена между нарушителем и веб-сервером
$F_{46}^V(t)$	функция распределения времени ожидания нарушителем окончания поступления от ложного веб-сервера множества промежуточных откликов, разделенных на фрагменты, направляемые через изменяемые интервалы времени с кодом состояния 401 UNAUTHORIZED после очередной попытки авторизации
$F_{51}^V(t)$	функция распределения времени ожидания окончания информационного обмена между клиентом и веб-сервером
$F_{61}^V(t)$	функция распределения времени ожидания окончания информационного обмена между нарушителем и ложным веб-сервером
$F_{64}^V(t)$	функция распределения времени ожидания очередной попытки нарушителя авторизоваться на ложном веб-сервере

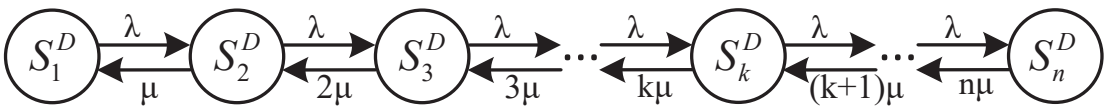


Рис.3. Граф состояний системы D

Таблица 3.

Дискретные состояния системы D

Дискретные состояния	Описание состояний
S_1^D	ожидание первым ложным веб-сервером подключения нарушителя, состояние простоя
S_2^D	ожидание вторым ложным веб-сервером подключения нарушителя, в системе находится 1 заявка, один ложный веб-сервер занят, остальные простаивают
S_3^D	ожидание третьим ложным веб-сервером подключения нарушителя, в системе находится 2 заявки, два ложных веб-сервера заняты, остальные простаивают
S_k^D	ожидание k-м ложным веб-сервером подключения нарушителя, в системе находится $k-1$ заявок, $k-1$ ложных веб-серверов заняты, остальные простаивают
S_n^D	ожидание отказа системы в обслуживании нарушителя, все веб-серверы заняты

Таблица 2.

Вероятностные характеристики процесса функционирования системы D

Переменная	Описание вероятностных характеристик
$F_{12}^D(t)$	функция распределения времени ожидания первым ложным веб-сервером подключения нарушителя
$F_{23}^D(t)$	функция распределения времени ожидания вторым ложным веб-сервером подключения нарушителя
$F_{(k-1)k}^D(t)$	функция распределения времени ожидания k-м ложным веб-сервером подключения нарушителя
$F_{(n-1)n}^D(t)$	функция распределения времени ожидания n-м ложным веб-сервером подключения нарушителя

веб-сессий на одном ложном веб-сервере, λ_{nr} – интенсивность подключений сетевой разведки.

В любой момент времени может произойти лишь одно из двух событий, которые приводят к изменению состояния системы D. Поступление заявки в систему осуществляется с интенсивностью подключений сетевой разведки λ_{nr}, k – это количество заявок. Если случайный процесс находится в состоянии S_k^D, при котором $k < n$, то происходит переход в состояние S_{k+1}^D (начало обслуживания поступившей заявки на одном из свободных ложных веб-серверов), а интенсивность перехода равна λ_{nr}. Если же случайный процесс находится в состоянии S_n^D, когда все ложные веб-серверы заняты обслуживанием заявок, то состояние S_n^D случайного процесса остается неизменным, что эквивалентно отказу в обслуживании поступившей заявки. Таким образом, переход из состояния S_k^D в состояние S_{k+1}^D, при котором $k < n$ происходит с интенсивностью λ_{nr}, а завершение обслуживания заявки на одном из ложных веб-серверов происходит с интенсивностью μ.

Математическая модель исследуемых систем может быть представлена как отображение множества входных параметров модели (множество Z) во множество выходных вероятностно-временных характеристик (множество Y):

$$Z^V \rightarrow Y^V, Z^V = \{S^V, A^V, X^V\};\ Y^V = \{P^V, G^V\}, \quad (4)$$

$$Z^D \rightarrow Y^D, Z^D = \{S^D, A^D, X^D\};\ Y^D = \{P^D, G^D\}, \quad (5)$$

где S^V, S^D – множества дискретных состояний систем S, D; A^V, A^D – множества неуправляемых факторов систем S, D; X^V, X^D – множества управляемых факторов систем S, D; $P^V = \{P_{ij}^V(t)\}$, $P^D = \{P_{ij}^D(t)\}$ – множества интервально-переходных вероятностей пребывания систем S, D в состоянии j из состояния i в момент времени t; $G^V = \{G_{ij}^V(t)\}$, $G^D = \{G_{ij}^D(t)\}$ – множества вероятностей первого достижения состояния j из состояния i к моменту времени t для систем S, D.

Неуправляемыми и управляемыми факторами для рассматриваемых систем являются:

$$A^V = \{F_{12}^V(t), F_{23}^V(t), F_{34}^V(t), F_{35}^V(t), F_{51}^V(t), F_{46}^V(t), F_{61}^V(t)\}, \quad (6)$$

$$A^D = \{\lambda_{nr}, n_{ch}\}, \quad (7)$$

$$X^V = \{F_{46}^V(t)\}, \text{ при } \lambda_{46}^V = \frac{n}{d \cdot T_{res}}, \quad (8)$$

$$X^D = \{d, T_{res}, n\}, \text{ при } \mu_1^D = \frac{n_{ch}}{d \cdot T_{res}}, \mu_2^D = \frac{2n_{ch}}{d \cdot T_{res}}, \ldots, \mu_n^D = \frac{nn_{ch}}{d \cdot T_{res}}, \quad (9)$$

где n – количество ложных веб-серверов.

Для нахождения интервально-переходных вероятностей $P_{ij}(t)$ используется решение системы интегральных уравнений вида (10):

$$P_{ij}(t) = \delta_{ij}\,\Psi_i(t) + \sum_{k=1}^{n} p_{ik} \int_0^t f_{ik}(t) P_{kj}(t - \tau)\,d\tau, \qquad (10)$$

$$\Psi_i(t) = 1 - \sum_{j=1}^{n} p_{ij}\,F_{ij}(t). \qquad (11)$$

Процесс решения таких интегральных уравнений подробно изложен в [13], и в матричной форме он будет выглядеть следующим образом:

$$P(t) = \pounds^{-1}\{[I - p \times f(s)]^{-1}\,\Psi(s)\}. \qquad (12)$$

На рисунках 4 и 5 представлены результаты расчетов вероятностно-временных характеристик веб-сессий, функционирующих в одинаковых внешних условиях, но при различных значениях параметров веб-службы, которые свидетельствуют о том, что наилучшие значения для системы S, являются наихудшими для системы D.

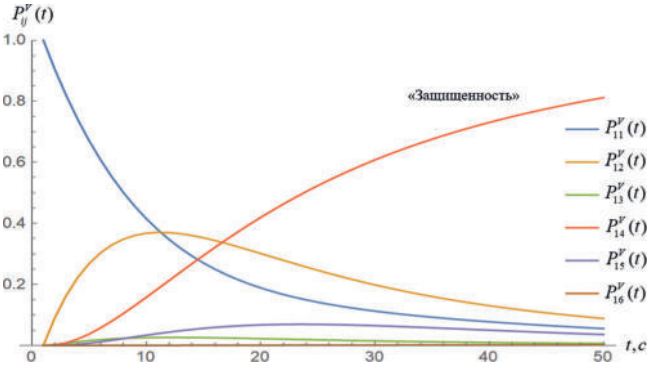


Рис. 4. Результаты расчетов интервально-переходных вероятностей нахождения системы S в состоянии j из состояния i к моменту времени t для процесса функционирования веб-службы с использованием конфигурирования параметров веб-сессии

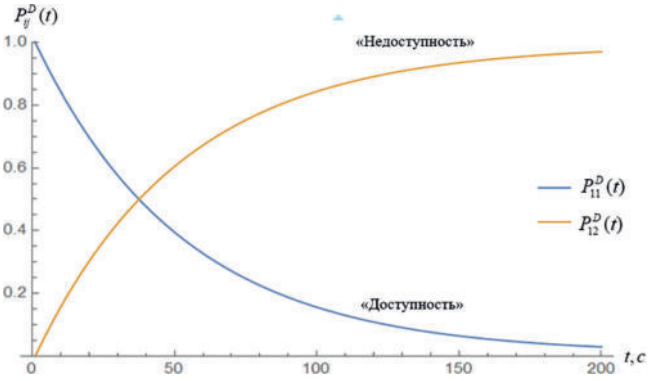


Рис. 5. Результаты расчетов интервально-переходных вероятностей нахождения системы D в состоянии j из состояния i к моменту времени t для процесса функционирования веб-службы с использованием конфигурирования параметров веб-сессии

Функции распределения Gij(t) находятся из следующего выражения:

$$G(t) = \pounds^{-1}\{s^{-1} \cdot p \cdot f(s) \cdot (I - p \cdot f(s))^{-1} \cdot \cdot [\mathrm{I} \times (I - p \cdot f(s))^{-1}]^{-1}\}. \qquad (13)$$

Функции $G_{ij}(t)$ позволяют оценить вероятности достижения соответствующих состояний впервые к конкретному моменту времени. На рисунке 6 изображен случай с обслуживанием нелегитимных клиентов, показывающий длительность первого посещения системой некоторых состояний с определенной вероятностью.

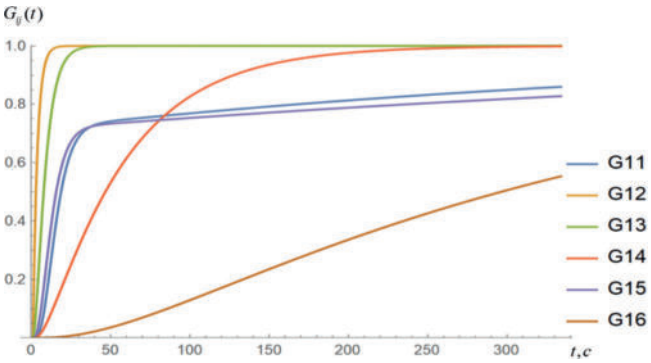


Рис. 6. Функции распределения $G_{ij}(t)$ времени первого посещения состояний процесса для процесса функционирования веб-службы с использованием конфигурирования параметров HTTP-ответа

Конфигурирование параметров веб-службы корпоративных информационных систем повышает вероятность нахождения нарушителя в состоянии удержания, однако при этих же параметрах понижается вероятность доступности ложных веб-серверов, что, в свою очередь, приводит к снижению вероятности нахождения системы в состоянии информационного обмена. Таким образом, возникает задача оптимизации конфигурируемых параметров веб-службы корпоративных информационных систем, при которой ложные веб-серверы будут функционировать наиболее эффективно с точки зрения критериев «доступности» и «защищенности».

Алгоритм определения оптимальных значений параметров конфигурирования веб-службы

Для нахождения оптимальных значений параметров веб-службы, при которых защищенность корпоративной информационной системы будет максимальной, а вероятность отказа ложных веб-серверов будет минимальной, разработан соответствующий алгоритм, который поясняется псевдокодом последовательности действий, представленном на рисунке 7.

Исходные данные для данного алгоритма указаны в таблице 5.

Рассмотрим порядок расчета оптимальных параметров веб-службы. Задача многокритериальной оптимизации включает в себя следующие компоненты:

☑ множество управляемых факторов X (которые представляют собой собственно искомые параметры конфигурирования). Элементами данного множества являются количество фрагментов откликов, средние промежутки времени между ними, а также количество ложных веб-серверов;

Algorithm 1 Алгоритм поиска оптимальных значений параметров веб-службы корпоративных информационных систем

Вход: Общее количество подключений к легитимному веб-серверу L_s, максимальное количество подключений к легитимному веб-серверу L_{smax}, общее количество подключений нарушителя к ложному веб-серверу L_k, максимальное количество подключений нарушителя к ложному веб-серверу L_{kmax}

Выход: количество фрагментов HTTP-ответа (d_i), время между отправкой этих фрагментов (T_i), количество ложных веб-серверов (n_i)

Устанавливают сетевое соединение
$(L_s) \leftarrow$ общее количество подключений всех клиентов к легитимному веб-серверу
if $(L_s > L_{smax})$ then
    (L_s) -= 1
    Выход
if $(L_s \leq L_{smax})$ then
    Принимают команду GET на запрос веб-ресурса
Выделяют идентификатор веб-сессии $(i \in N)$
Принимают команду POST от веб-сервера с предложением авторизации
Задают аутентификационные данные
(N_s) += 1
if $(N_s < 4)$ и аутентификационные данные верны then
    Авторизуют веб-клиента
    Предоставляют легитимному веб-клиенту права доступа к веб-ресурсу
if $(N_s < 4)$ и аутентификационные данные неверны then
    Пытаются авторизоваться снова
if $(N_s \geq 4)$ then
    Выделяют идентификатор веб-сессии нарушителя $(i \notin N, i \in P)$
    (L_s) -= 1
Оценивают значения функции (R), количество фрагментов HTTP-ответа (d_i), время между отправкой этих фрагментов (T_i) и количество ложных веб-серверов (n_i)
(V_s) += 1
$(L_k) = 0$
if $(V_s \geq n_i)$ then
    Завершение веб-сессии
    Выход
if $(V_s < n_i)$ then
    Перенаправляют на ложный веб-сервер
(L_k) += 1
if $(L_k > L_{kmax})$ then
    (V_s) += 1
    Переход к очередному ложному веб-серверу
if $(L_k \leq L_{kmax})$ then
    Задают аутентификационные данные
Формируют и направляют фрагменты HTTP-ответа (d_i) через время (T_i) между отправкой этих фрагментов
if разрыв соединения then
    Завершение веб-сессии
if попытка аутентификации then
    (L_k) += 1
Авторизуют легитимного веб-клиента
Предоставляют веб-клиенту права доступа к веб-ресурсу
Взаимодействуют по принципу запрос-ответ
(L_s) -= 1
Завершают веб-сессию
$(N_s) = 0$
$(V_s) = 0$
Формируют отчет

Рис. 7. Псевдокод алгоритма поиска оптимальных значений параметров веб-службы

- ☑ множество неуправляемых параметров A, характеризующих условия функционирования веб-сессии. Элементами данного множества являются функции распределения длительности ожидания наступления неуправляемых событий;
- ☑ множество целевых функций (или критериев). В качестве целевой функции, характеризующей результативность защиты корпоративных информационных систем, выступает финальная вероятность пребывания системы в состоянии удержания средства сетевой разведки.

В качестве целевой функции, характеризующей доступность ложных веб-серверов, выступает вероятность отказа данной системы, физический смысл которой заключается в невозможности обработки информации ложными веб-серверами.

Задача многокритериальной оптимизации в данном случае формулируется следующим образом: необходимо максимизировать эффективность защиты и минимизировать вероятность отказа системы при соблюдении ряда ограничений и допустимых значений.

$$\begin{cases} F_1(d, T_{res}, n) \longrightarrow \max\limits_{для\ d, T_{res}, n \in N}, \\ F_2(d, T_{res}, n) \longrightarrow \min\limits_{для\ d, T_{res}, n \in N} \end{cases} \quad (14)$$

где целевая функция F_1 характеризует «защищенность» сетевых устройств, а целевая функция F_2 характеризует доступность ложных веб-серверов.

Значения указанных функций и факторов принадлежат области допустимых значений Q:

$$\begin{cases} 0 < n \le 20, \\ 0 < d \le 30, \\ 0 < T_{res} \le 60, \\ \lambda_{12}^V \ge \lambda_{23}^V \ge \lambda_{34}^V \ge \lambda_{35}^V \ge \lambda_{41}^V \ge 0, \\ \lambda_{51}^V \ge \lambda_{61}^V \ge 0 \\ 0 \le F_1(X^V, A^V) \le 1, \\ 0 \le P_{отк} = \left(\frac{\lambda_{nr} \cdot d \cdot T_{res}}{n_{ch}}\right)^n \cdot \frac{1}{\sum_{i=0}^{n} \frac{(\lambda_{nr} \cdot d \cdot T_{res})^i}{i! n_{ch}^i}} \cdot \frac{1}{n!} \le 1 \end{cases} \quad (15)$$

Поскольку задача (14) является многокритериальной, то множество возможных значений целевых функций образует фронт Парето в достижимом критериальном пространстве.

Поиск оптимальных значений был выполнен с использованием метода идеальной точки, суть которого заключается в нахождении точки на фронте Парето, которая максимально близка к идеальной (по заданным критериям).

Таким образом, задача многокритериальной оптимизации (14) сводится к минимизации функции свертки (скалярной функции R), которая получается через частные целевые функции методом отклонения от идеальной точки [14,15] и которая имеет следующий вид:

$$\begin{cases} R(X^V, A^V, X^D, A^D) = \\ = \sqrt{k_1 \cdot \left(\frac{F_1(d, T_{res}, n)}{F_1^{\max}(d, T_{res}, n)} - 1\right)^2 + k_2 \cdot \left(\frac{F_2(d, T_{res}, n)}{F_2^{\max}(d, T_{res}, n)}\right)^2}, \\ R(X^V, A^V, X^D, A^D) \longrightarrow \min\limits_{для\ d, T_{res}, n \in N}. \end{cases} \quad (16)$$

где k_1 и k_2 – коэффициенты значимости, которые отражают предпочтения лица принимающего решения относительно величин частных критериев. Эти коэффициенты могут быть заданы экспертами или получены путем анализа данных.

Поскольку целевые функции (14) имеют различную размерность, то была осуществлена нормировка посредством деления данных целевых функций на их максимальное значение. С условиями данной нормировки, идеальная точка будет иметь координаты (1, 0).

На рисунке 8 представлена визуализация критериального пространства и фронта Парето для различных коэффициентов значимости.

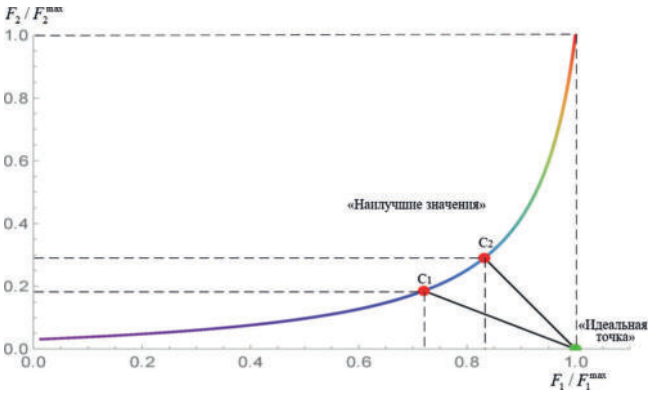


Рис. 8. Критериальное пространство, фронт Парето и два наилучших значения параметров для различных коэффициентов значимости k_1 и k_2

Минимизация скалярной функции R выполнялась с использованием алгоритма «Нелдера-Мида», поскольку благодаря меньшему числу переменных его сходимость была более быстрой (27 миллисекунд) по сравнению с алгоритмом «Имитации отжига» (202 миллисекунды) и алгоритмом «Роя частиц» (1011 миллисекунд).

При обнаружении нарушителя его удержание системой защиты в состоянии ожидания осуществляется на этапе авторизации пользователя, что приводит к снижению результативности проведения сетевой разведки. Результативность разработанного алгоритма была проверена путем его программной реализации и проведения натурного эксперимента в среде программирования Spyder Python и веб-браузере. Суть эксперимента – это оценка длительности взаимодействия веб-сервера и средства сетевой разведки на этапе авторизации при выборе оптимальных режимов конфигурирования параметров

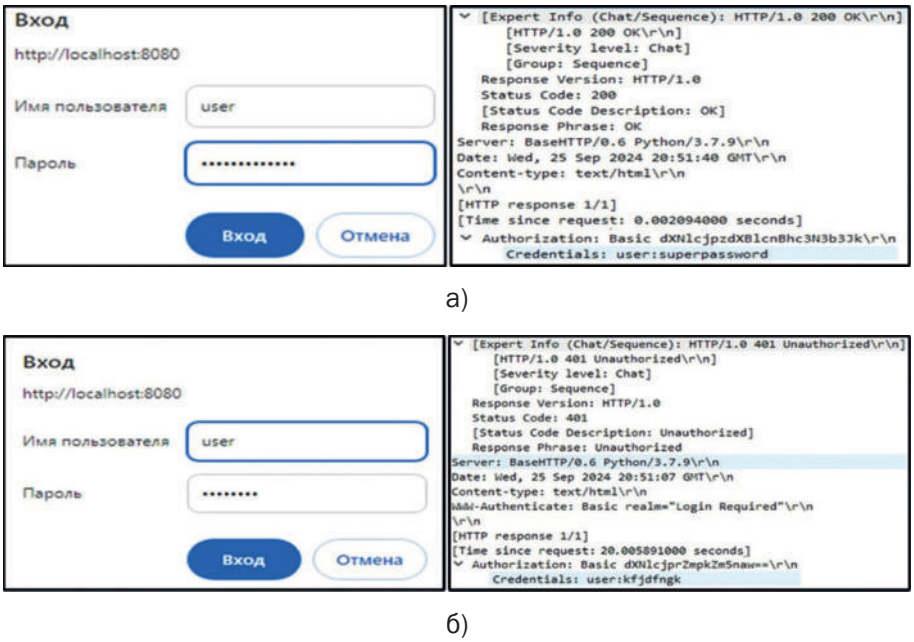


Рис. 9. Авторизация легитимного клиента (а) и попытка авторизации нарушителя (б)

веб-службы. На рисунке 9 продемонстрирована авторизация легитимного клиента (рис. 9а) при условии, что он использует верные аутентификационные данные и попытка авторизации нарушителя (рис. 9б), при условии, что он использует неверные аутентификационные данные. Конфигурирование параметров применяется только при попытке авторизации нарушителя. На рисунке 9б видно, что при конфигурировании параметров веб-службы время HTTP-ответа нарушителю существенно увеличивается.

Проведенный эксперимент показал, что конфигурирование параметров веб-службы корпоративных информационных систем, повышает время удержания средства сетевой разведки в состоянии ожидания, в отличие от ситуации, когда авторизация происходит без конфигурирования параметров. Сравнительный анализ времени авторизации при конфигурировании параметров веб-службы и без него приведен в таблице 6.

Разработанный алгоритм нахождения значений параметров веб-службы для определения оптимальных режимов конфигурирования корпоративных информационных систем позволяет повысить результативности защиты за счет снижения возможностей средств сетевой разведки по подбору имен и паролей санкционированных клиентов, и увеличении временного ресурса, расходуемого средством сетевой разведки, для идентификации средств защиты.

Таблица 6.

Сравнительный анализ времени авторизации при конфигурировании параметров веб-службы и без него

№ п/п	Протокол	Код состояния	Значение пароля	Количество фрагментов HTTP-ответа, шт	Значение времени между фрагментами HTTP-ответа, с	Количество ложных веб-серверов	Время попытки авторизации без конфигурирования параметров веб-службы, с	Время попытки авторизации с конфигурированием параметров веб-службы, с
1.	HTTP	200 OK	superpassword	–	–	–	0.002094000	–
2.	HTTP	401 UNAUTHORIZED	kfjdfngk	10	2	5	0.002137800	20.005891000
3.	HTTP	401 UNAUTHORIZED	j	7	4	7	0.003309000	28.010590500

Выводы

Разработанная модель позволяет исследовать различные этапы веб-сессии при конфигурировании параметров веб-службы корпоративной сети передачи данных в условиях сетевой разведки. Модель формализована в виде полумарковского случайного процесса с дискретными состояниями и непрерывным временем, при этом выходные характеристики (интервально-переходные вероятности, функции распределения первого достижения соответствующего состояния) определяются через основные характеристики полумарковского процесса с экспоненциальным законом распределения.

Полученные вероятностно-временные характеристики могут быть использованы как целевые функции, которые характеризуют критерии «защищенности» веб-службы и «доступности» ложных веб-серверов в условиях сетевой разведки.

Разработанный алгоритм позволяет определить оптимальный режим конфигурирования параметров веб-службы корпоративных информационных систем. Эффект достигается путем имитации веб-сессии низкого качества на этапе авторизации веб-клиента, за счет варьирования таких параметров, как количество фрагментов HTTP-ответа и время между этими фрагментами. А также за счет добавления ложных веб-серверов, что приводит к увеличению временного ресурса, расходуемого средством сетевой разведки для идентификации средств защиты.

Разработанное научно-методическое обеспечение необходимо для назначения параметров средств защиты веб-серверов при предупреждении и ликвидации компьютерных атак.

Литература

1. *Марков А. С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. 2023. № 1 (53). С. 2–12. DOI:10.21681/2311-3456-2023-1-2-12.*
2. *Соколовский С. П., Горбачев А. А. Способ проактивной защиты почтового сервера от нежелательных сообщений электронной почты // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2021. № 3-4 (153-154). С. 31–40.*
3. *Walla S., Rossow C. MALPITY: Automatic identification and Exploitation of Tarpit Vulnerabilities in Malware. 2019 IEEE European Symposium on Security and Privacy (EuroS&P). 2019. pp. 590–605. DOI: 10.1109//EuroSP.2019.00049.*
4. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Methodology for substantiating the characteristics of false network traffic to simulate information system. CEUR Workshop Proceeding. 2021. pp. 115–124.*
5. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Honeypots network traffic parameters modelling. CEUR Workshop Proceeding. 2021. pp. 229–239.*
6. *Ворончихин И. С., Иванов И. И., Максимов Р. В., Соколовский С. П. Маскирование структуры распределенных информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6(34). С. 92–101. DOI:10.21681/2311-3456-2019-6-92-101.*
7. *Патент № 2716220 Российской Федерации. Способ защиты вычислительных сетей / Р. В. Максимов, С. П. Соколовский, И. С. Ворончихин // заявитель и патентообладатель Краснодарское высшее военное училище имени генерала армии С. М. Штеменко. № 2019123718, заявл. 22.07.2019, опубл. 06.03.2020.*
8. *Патент № 2810193 Российской Федерации. Способ защиты вычислительных сетей / Р. В. Максимов, А. А. Москвин, С. П. Соколовский, В. В. Починок, И. С. Ворончихин, А. П. Теленьга, А. А. Горбачев, С. С. Каверин // заявитель и патентообладатель Краснодарское высшее военное училище имени генерала армии С.М. Штеменко. № 2023100318, заявл. 10.01.2022, опубл. 22.12.2023.*
9. *Евневич Е. Л., Фаткиева Р. Р. Моделирование информационных процессов в условиях конфликтов // Вопросы кибербезопасности. 2020. № 2. С. 42–49. DOI:10.21681/2311-3456-2020-2-42-49.*
10. *Кубарев А. В., Лапсарь А. П., Федорова Я. В. Повышение безопасности эксплуатации значимых объектов критической инфраструктуры с использованием параметрических моделей эволюции // Вопросы кибербезопасности. 2020. № 1 (35). С. 8–17. DOI:10.21681/2311-3456-2020-01-08-17.*
11. *Дроботун Е. Б. Методика снижения удобства использования автоматизированной системы при введении в ее состав системы защиты от компьютерных атак // Вопросы кибербезопасности. 2020. № 2 (36). С. 50–57. DOI:10.21681/2311-3456-2020-02-50-57.*
12. *Будников С. А., Бутрик Е. Е., Соловьев С. В. Моделирование APT-атак, эксплуатирующих уязвимость Zerologon // Вопросы кибербезопасности. 2021. № 6 (46). С. 47–61. DOI:10.21681/2311-3456-2021-6-47-61.*
13. *Горбачев А. А. Модель и параметрическая оптимизация проактивной защиты сервиса электронной почты от сетевой разведки // Вопросы кибербезопасности. 2022. № 3 (49). С. 69–81. DOI:10.21681/4311-3456-2022-3-69-81.*
14. *Шерстобитов Р. С. Модель маскирования информационного обмена в сети передачи данных ведомственного назначения // Системы управления, связи и безопасности. 2024. № 1. С. 1–25. DOI: 10.24412/2410-9916-2024-1-001-025.*
15. *Москвин А. А., Максимов Р. В., Горбачев А. А. Модель, оптимизация и оценка эффективности применения многоадресных сетевых соединений в условиях сетевой разведки // Вопросы кибербезопасности. 2023. № 3 (55). С. 13–22. DOI:10.21681/2311-3456-2023-3-13-22.*

MODEL OF THE OPERATION PROCESS AND ALGORITHM FOR DETERMINING OPTIMAL VALUES OF CONFIGURABLE PARAMETERS OF THE WEB SERVICE OF CORPORATE INFORMATION SYSTEMS

Kaverin S. S.[6], Maksimov R. V.[7], Moskvin A. A.[8]

Keywords: *random process, probabilistic-time characteristics, web resources, ideal point method, web session, interval-transition probabilities.*

The purpose of the study: *increasing the security of the web service of corporate information systems in the context of network reconnaissance.*

Methods used: *Pareto optimization, ideal point, Nelder-Mead, particle swarm, simulated annealing.*

The result of the study: *a model for the functioning of a web service of corporate information systems in network intelligence conditions has been developed, which is implemented in the form of a semi-Markov random process with discrete states and continuous time. The probabilistic-time characteristics of the processes under study were obtained, which are necessary to determine the optimal mode for configuring the parameters of the web service.*

The problem of vector optimization has been solved to determine the optimal values of the parameters of the web service of corporate information systems, such as the number of HTTP response fragments, the time between these fragments, as well as the number of false web servers, allowing to maximize the effectiveness of protecting the web service of corporate information systems and minimize the likelihood failure of false web servers under appropriate restrictions.

Scientific novelty: *consists in developing a model and algorithm for searching the optimal parameters of a web service of corporate information systems in network intelligence conditions using the mathematical apparatus of semi-Markov random processes and scalarization of the vector optimization problem by the ideal point method.*

References

1. *Markov A. S. Vazhnaja veha v bezopasnosti otkrytogo programmnogo obespechenija // Voprosy kiberbezopasnosti. 2023. № 1 (53). S. 2–12. DOI:10.21681/2311-3456-2023-1-2-12.*
2. *Sokolovskij S. P. Model' zashhity informacionnoj sistemy ot setevoj razvedki dinamicheskim upravleniem ee strukturno-funkcional'nymi harakteristikami // Voprosy oboronnoj tehniki. Serija 16 protivodejstvie terrorizmu. 2020. № 7-8. S. 62–73.*
3. *Walla S., Rossow C. MALPITY: Automatic identification and Exploitation of Tarpit Vulnerabilities in Malware. 2019 IEEE European Symposium on Security and Privacy (EuroS&P). 2019. pp. 590–605. DOI: 10.1109/EuroSP.2019.00049.*
4. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Methodology for substantiating the characteristics of false network traffic to simulate information system. CEUR Workshop Proceeding. 2021. pp. 115–124.*
5. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Honeypots network traffic parameters modelling. CEUR Workshop Proceeding. 2021. pp. 229–239.*
6. *Voronchihin I. S., Ivanov I. I., Maximov R. V., Sokolovskij S. P. Maskirovanie struktury raspredelennyh informacionnyh sistem v kiberprostranstve // Voprosy kiberbezopasnosti. 2019. № 6 (34). S. 92–101. DOI:10.21681/2311-3456-2019-6-92-101.*
7. *Patent № 2716220 Rossijskoj Federacii. Sposob zashhity vychislitel'nyh setej / R. V. Maximov, S. P. Sokolovskij, I. S. Voronchihin // zajavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishhe imeni generala armii S. M. Shtemenko. № 2019123718, zajavl. 22.07.2019, opubl. 06.03.2020.*
8. *Patent № 2810193 Rossijskoj Federacii. Sposob zashhity vychislitel'nyh setej / R. V. Maximov, S. P. Sokolovskij, I. S. Voronchihin // zajavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishhe imeni generala armii S. M. Shtemenko. № 2023100318, zajavl. 10.01.2022, opubl. 22.12.2023.*
9. *Evnevich E. L., Fatkieva R. R. Modelirovanie informacionnyh processov v uslovijah konfliktov // Voprosy kiberbezopasnosti. 2020. № 2 (36). S. 42–49. DOI:10.21681/2311-3456-2020-2-42-49.*
10. *Kubarev A. V., Lapsar' A. P., Fedorova Ja. V. Povyshenie bezopasnosti jekspluatacii znachimyh ob#ektov kriticheskoj infrastruktury s ispol'zovaniem parametricheskih modelej jevoljucii // Voprosy kiberbezopasnosti. 2020. № 1 (35). S. 8–17. DOI:10.21681/2311-3456-2020-01-08-17.*

6 Sergey S. Kaverin, post graduate student, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: sergey_kav995@mail.ru

7 Roman V. Maximov, Dr.Sc., Professor, Honored Inventor of the Russian Federation, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: rvmaxim@yandex.ru

8 Artyom A. Moskvin, Ph.D., Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: tema.kg9012@gmail.com

11. *Drobotun E. B. Metodika snizhenija udobstva ispol'zovanija avtomatizirovannoj sistemy pri vvedenii v ee sostav sistemy zashhity ot komp'juternyh atak // Voprosy kiberbezopasnosti. 2020. № 2 (36). S. 50–57. DOI:10.21681/2311-3456-2020-02-50-57.*
12. *Budnikov S. A., Butrik E. E., Solov'ev S. V. Modelirovanie APT-atak, jekspluatirujushhih ujazvimost' Zerologon // Voprosy kiberbezopasnosti. 2021. № 6 (46). S. 47–61. DOI:10.21681/2311-3456-2021-6-47-61.*
13. *Gorbachev A. A. Model' i parametricheskaja optimizacija proaktivnoj zashhity servisa jelektronnoj pochty ot setevoj razvedki // Voprosy kiberbezopasnosti. 2022. № 3 (49). S. 69–81. DOI:10.21681/4311-3456-2022-3-69-81.*
14. *Sherstobitov R. S. Model' maskirovaniya informacionnogo obmena v seti peredachi dannyh vedomstvennogo naznacheniya // Sistemy upravleniya, svyazi i bezopasnosti. 2024. № 1. S. 1–25. DOI: 10.24412/2410-9916-2024-1-001-025.*
15. *Moskvin A. A., Maximov R. V., Gorbachev A. A. Model', optimizaciya i ocenka effektivnosti primeneniya mnogoadresnyh setevyh soedinenij v usloviyah setevoj razvedki // Voprosy kiberbezopasnosti. 2023. № 3 (55). S. 13–22. DOI:10.21681/2311-3456-2023-3-13-22.*

МАСКИРОВАНИЕ ТОПОЛОГИЧЕСКИХ СВОЙСТВ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ В УСЛОВИЯХ СЕТЕВОЙ РАЗВЕДКИ. Часть 2

Горбачев А. А.[1]

DOI: 10.21681/2311-3456-2025-1-63-72

Цель исследования: *разработка системы моделей, включающей классические модели случайных графов и генеративные модели искусственного интеллекта и предназначенной для решения задачи маскирования топологических свойств вычислительных сетей при генерации ложного сетевого трафика и применении ложных сетевых информационных объектов, позволяющих, с одной стороны, обеспечить заданную степень сходства топологических свойств реальных вычислительных сетей с ложными, а с другой стороны, максимизировать показатель защищенности критических узлов реальных вычислительных сетей.*

Используемые методы*: взвешенная аддитивная линейная свертка, случайный граф Эрдеша-Реньи, Барбаши, Ваттса-Строгаца, Харари, алгоритм байесовской оптимизации, модель сверточного вариационного автокодировщика, модель графового вариационного автокодировщика.*

Результат исследования: *представленная система моделей позволяет повысить результативность защиты вычислительной сети за счет формирования у злоумышленника устойчивого ложного представления относительно топологических свойств вычислительной сети с учетом повышения защищенности критических узлов посредством смещения положения ложных критических узлов по отношению к реальным, при обеспечении заданной степени сходства ложной топологии вычислительной сети по отношению к реальной топологии. Система моделей включает в себя конвейер машинного обучения на основе моделей случайных графов Эрдеша-Реньи, Барбаши, Ваттса-Строгаца, Харари, используемых для формирования обучающего набора данных, модели графового вариационного автокодировщика, модели выборки из скрытого пространства, содержащей показатели качества генерируемой ложной структуры, эволюционного алгоритма скалярной оптимизации, осуществляющего поиск оптимальной точки синтеза ложной структуры в скрытом пространстве вариационного автокодировщика, а также генератор ложного трафика, реализующего отправку пакетов с заданными сетевыми идентификаторами. Разработанный конвейер имеет ограничения по размерности синтезируемой ложной топологии в связи с вычислительной сложностью процесса обучения генеративной модели и поиска оптимальной точки синтеза.*

Научная новизна: *заключается в применении байесовского алгоритма оптимизации для выбора оптимальной точки синтеза ложной топологии из скрытого пространства обученного графового вариационного автокодировщика, в использовании целевой функции, представленной линейной взвешенной сверткой из коэффициента Жаккара между множеством ребер ложной и реальной топологии вычислительной сети, показателей защищенности вычислительной сети: среднего кратчайшего расстояния между реальными и ложными критическими узлами, коэффициента Жаккара между множеством ложных и реальных критических узлов вычислительной сети. В применении моделей случайных графов для формирования обучающего набора данных.*

Ключевые слова: *ложные информационные объекты, вариационный автокодировщик, конвейер машинного обучения, искусственный интеллект, оптимизация, метаэвристические алгоритмы, случайные графы.*

Введение

Одним из методов снижения эффективности анализа сетевого трафика злоумышленниками является генерация ложного сетевого трафика с сетевыми параметрами ложной вычислительной сети (идентификаторами сетевого, транспортного или прикладного уровня, динамическими характеристиками, структурными атрибутами) [1–4]. Как это было показано в первой части настоящей работы синтез ложных топологий вычислительных сетей за счет решения задачи комбинаторной оптимизации матрицы смежности графа с ростом количества вершин графа становится вычислительно неэффективным, поэтому для решения задачи генерации сетей различной природы используются методы снижения размерности, вложения графа (*эмбеддинга графа, graph embedding*) в пространство меньшей размерности, параметрические модели случайных графов[2,3], а также эвристические алгоритмы[4] [5]. При синтезе сложных сетей,

1 Горбачев Александр Александрович, кандидат технических наук, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: infosec23.00@mail.ru

2 Haddadi H. Topological Characteristics of IP Networks. University College London. 2008. 114 p.

3 Liu W., Chen P., Yu F., Suzumura T., Hu G. Learning Graph Topological Features via GAN. IEEE. 2019. Vol. 7. pp. 21834–21843.

4 Батенков К. А. Анализ и синтез структур сетей связи методом перебора состояний // Вестник Санкт-Петербургского университета. Прикладная математика. Процессы управления. 2022. Т. 18. Вып. 3. С. 300–315.

Рис. 1. Классификация генеративных моделей машинного обучения

учитывающих веса и атрибуты вершин графов, используют вложения графов с использованием методов случайного блуждания, матричного разложения, алгоритмов глубокого обучения.

Представления многомерных входных данных о структуре сложных сетей осуществляется с целью кластеризации и визуализации непараметрическими методами (k-ближайших соседей, k-средних, методом главных компонент, стохастическим вложением соседей с t-распределением и др.) либо для параметризации моделей случайных графов (стохастических Кронекеровских графов, модели Ваксмана[5], экспоненциальных моделей случайных графов, безразмерных моделей случайных графов и др.), моделей глубокого обучения [6–8]. Параметрические генеративные модели используются с целью генерации графов, прогнозирования связей (ребер), классификации, кластеризации вершин, подграфов, графов [9–12]. В контексте защиты критических узлов вычислительных сетей необходимо, чтобы модель генерировала ложные структуры не только сходные с конкретной топологией (или совокупностью топологий) вычислительной сети, но и позволяла генерировать топологии в *управляемом непрерывном диапазоне* топологических характеристик со смещенным положением ложных критических узлов относительно реальных критических узлов.

С другой стороны, генерация данных произвольной природы из аппроксимированного распределения в настоящее время успешно реализуется моделями, методами и алгоритмами генеративного искусственного интеллекта (генерация текста, музыки, изображений) [13]. Генеративные модели искусственного интеллекта используют различные подходы к моделированию истинного распределения наблюдений и представлены широким классом моделей глубокого обучения, в большинстве случаев, основанных на архитектурах искусственных нейронных сетей (рис. 1).

В соответствии с теоремой «*об отсутствии бесплатных завтраков*»[6] не существует возможности априорного выбора наилучшей универсальной модели или алгоритма оптимизации для решения конкретной задачи, но полный перебор существующих моделей и алгоритмов является практически нецелесообразным, поэтому редукция многообразия методов и моделей генеративного искусственного интеллекта осуществляется на основе критериев, представленных ниже.

Использование алгоритмов машинного обучения без учителя. Функционирование вычислительных сетей связано с обработкой неструктурированных данных и постоянный анализ сетевого трафика не предполагает заблаговременного создания размеченных данных. Необходимо обеспечить возможность оперативного переобучения без проведения предварительной разметки данных.

Возможность синтеза топологии с заданными характеристиками. Модель должна позволять синтезировать структуры ложных вычислительных сетей, которые обладают заданными характеристиками качества с незначительным отклонением. В связи с чем, целесообразно использовать алгоритмы, моделирующие распределение топологических характеристик в явной форме.

Высокая вариабельность характеристик синтезируемых топологий. Генеративные модели должны обеспечивать синтез топологий как полностью идентичных исходным топологиям, так и промежуточных вариантов с заданными характеристиками. Данное требование связано с непрерывностью распределения характеристик синтезируемых топологий в скрытом пространстве моделей.

5 Waxman Bernard M. Routing of multipoint connections. IEEE journal on selected areas in communications. 1988. Vol. 6, no. 9. pp. 1617–1622.

6 Wolpert D.H., Macready W.G. No free lunch theorems for optimization. IEEE transactions on evolutionary computation. 1997. Vol №. 1. pp. 67–82.

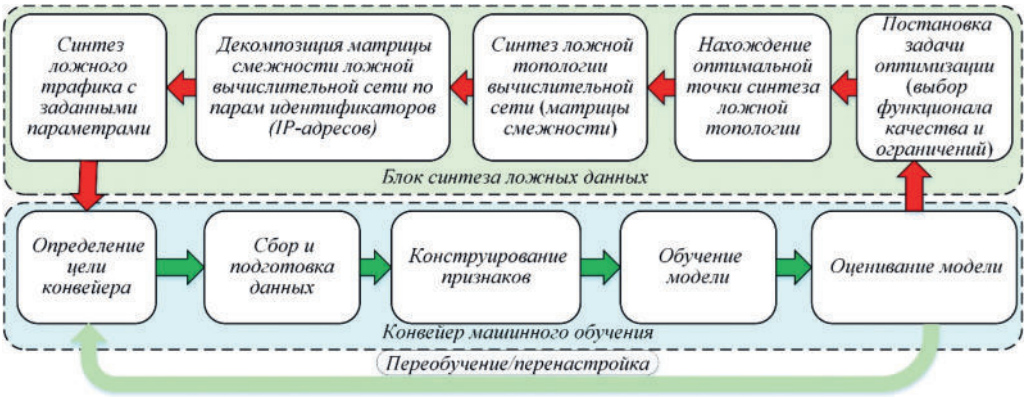


Рис. 2. Схема конвейера машинного обучения и его использование для маскирования топологических свойств вычислительных сетей

Вычислительная сложность. Особую популярность при решении широкого спектра задач получили большие языковые модели, такие как *предобученные генеративные трансформеры* (*Generative Pre-trained Transformer, GPT*). Основной трудностью их использования для маскирования топологических свойств вычислительных сетей является высокая пространственная и временная сложность моделей (количество свободных параметров от $117 \cdot 10^9$ до $500 \cdot 10^9$) [14]. Конвейеры машинного обучения на основе генеративных моделей должны разворачиваться на аппаратных платформах (устройствах, реализующих функцию генератора трафика) с относительно ограниченными возможностями для последующей оптимизации результатов синтеза с использованием численных методов. Непрерывность распределения топологических характеристик в скрытом пространстве обученных моделей ускоряет сходимость и снижает сложность алгоритмов численной оптимизации, определяющих оптимальную точку (или точки) реконструкции топологии вычислительной сети в скрытом пространстве генеративной модели.

Исходя из вышеописанных критериев, в работе используются архитектуры класса «кодировщик-декодировщик», а именно *вариационный сверточный автокодировщик* (*Variotional Autoencoder, VAE*), *вариационный графовый автокодировщик* (*Graph Variotional Autoencoder, GVAE*). Выбранные архитектуры используют разные подходы к снижению размерности и обобщению закономерностей наблюдений: в первом случае, аналогично обработке и генерации изображений, используются сверточные слои; во втором случае, ключевым является слой, который вычисляет нормированный Лапласиан от наблюдений A_i и определяет матрицу из *наименьших собственных векторов* нормированного Лапласиана заданного размера (меньшего, чем исходный размер матриц A_i), то есть основан на матричном разложении матрицы смежности.

Основная идея работы состоит в решении задачи оптимизации в пространстве низкой размерности (скрытом пространстве) генеративных моделей с использованием методов численной оптимизации вещественной скалярной либо векторной целевой функции, при этом выбор оптимальной точки реконструкции топологии осуществляется исходя из критериев, оценивающих *сходство* реальной и ложной топологии, а также смещение ложных критических узлов по отношению к реальным критическим узлам (оценка *защищенности* реальных критических узлов при синтезе ложной топологии).

Реализация маскирования топологических характеристик вычислительных сетей осуществляется на основе *конвейера машинного обучения* с генеративной моделью искусственного интеллекта и *блока синтеза ложных данных*, включающего в себя процедуры постановки задачи оптимизации ложной структуры по выбранным критериям качества, поиска оптимальной точки в скрытом пространстве генеративной модели, обученной на множестве топологических инвариантов вычислительных сетей с заданными свойствами. Далее производится генерация ложной топологии и выделение из полученной матрицы смежности сетевых идентификаторов, в соответствии с которыми осуществляется отправка пакетов ложного сетевого трафика (рис. 2) с заданных интерфейсов устройств, предназначенных для генерации ложного трафика.

Ключевое значение при создании конвейера машинного обучения имеет алгоритм формирования обучающего набора данных, включающий в себя процедуры сбора, подготовки данных и конструирования признаков. Каждое наблюдение, входящее в массив обучающих данных $\mathbf{A}_{train}$, является матрицей смежности реальной вычислительной сети A_{real} размерности N, а также некоторых преобразований $A_i = f(A_{real})$ от матрицы смежности реальной вычислительной сети. Во избежание переобучения

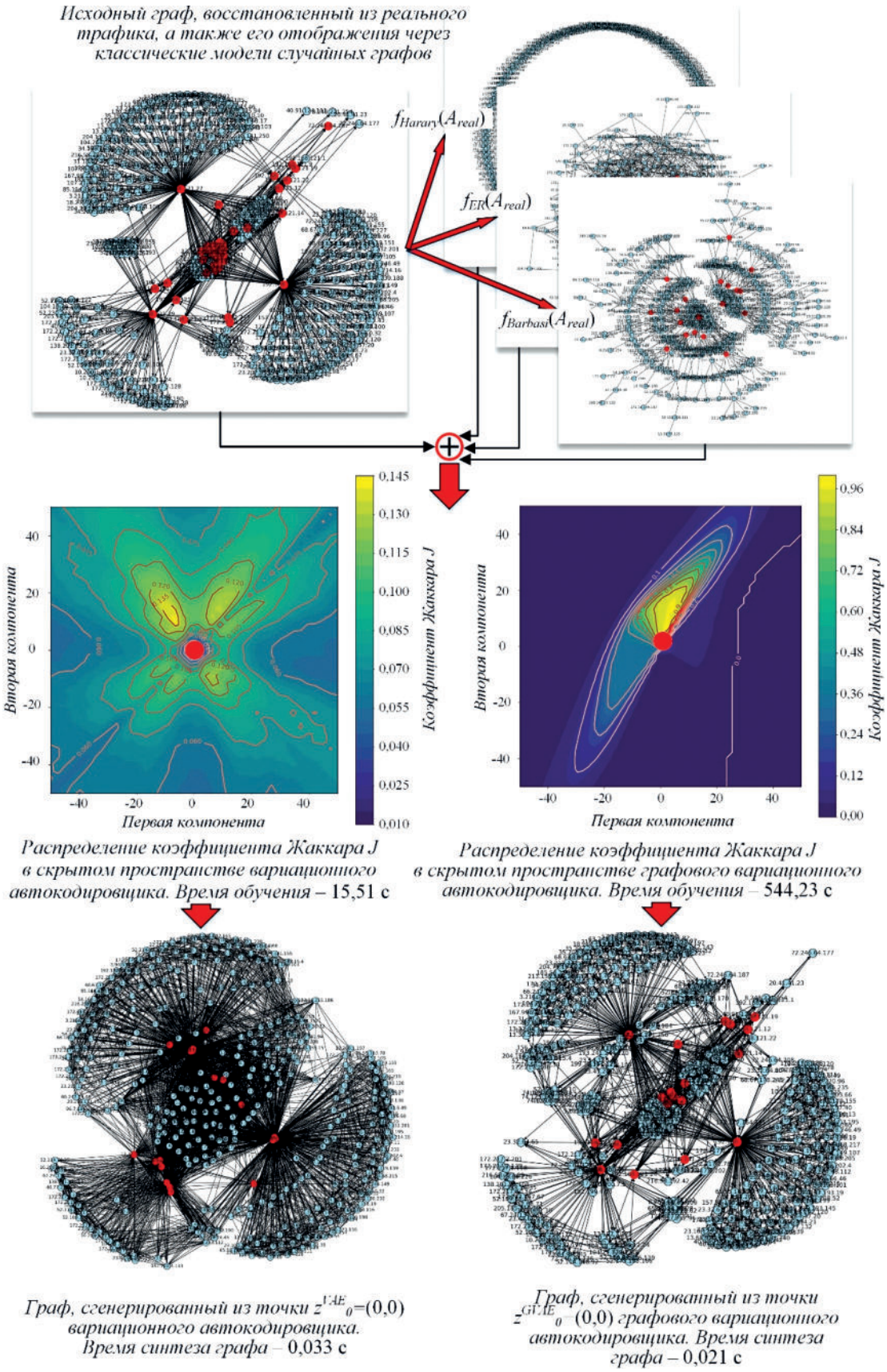


Рис. 3. Схема формирования обучающего набора данных Atrain и реконструкции топологии вычислительной сети с использованием моделей вариационных автокодировщиков

генеративных моделей и для обеспечения достаточного разнообразия ложных топологий вычислительных сетей, при формировании обучающего набора данных используются матрицы смежности A_i, полученные из моделей случайных графов (*Эрдеша-Реньи, Ватца-Строгаца, Барбаши и Харари*).

Формирование обучающего датасета $\mathbf{A}_{train}$ производится за счет конкатенации и перемешивания матриц смежности A_i, полученных из различных моделей случайных графов, а также матриц смежности A_{real} реальной вычислительной сети в равных соотношениях (рис. 3).

При этом точечные оценки параметров θ^{RG}_i указанных моделей случайных графов определяются исходя из максимизации среднего коэффициента Жаккара между множеством ребер реальной E_{real} и множествами ребер ложных вычислительных сетей E_i, полученных с помощью параметризованных оценками θ^{RG}_i моделей случайных графов.

При обучении вариационного автокодировщика решается задача оптимальной реконструкции входных данных кодировщика из выходных данных декодировщика с учетом близости распределения наблюдений в скрытом пространстве кодера к многомерному нормальному при фиксированных оптимальных значениях гиперпараметров θ^*_{gip}. Перед развертыванием конвейера машинного обучения осуществляется гиперпараметрическая оптимизация модели. Для архитектур вариационных автокодировщиков часто используют нижнюю вариационную границу (*Evidence Lower Bound*) в качестве ненормированной взвешенной линейной свертки как функционала качества обучения и гиперпараметрической оптимизации модели (выражение 1) [15]:

$$L(\theta_{gip},\theta,\varphi,\mathbf{A}_{train}) = \\ = k_1 D_{KL}(N(\mu,\sigma\|N(0,1)) + k_2 MSE \longrightarrow \min_{Q}, \quad (1)$$

$$MSE(\theta_{gip},\theta,\varphi,\mathbf{A}_{train}) = \frac{1}{n}\sum_{i=1}^{n}(A_i - \hat{A}_i(\theta_{gip},\theta,\varphi,\mathbf{A}_{train}))^2, \quad (2)$$

$$\mu = f(\theta_{gip},\theta,\varphi,\mathbf{A}_{train}),\ \sigma = f(\theta_{gip},\theta,\varphi,\mathbf{A}_{train}), \quad (3)$$

$$D_{KL}(N(\mu,\sigma\|N(0,\mathbf{I})) = \\ = \frac{1}{2N_{Lat}}\sum_{i=1}^{N_{Lat}}(1 + \log(\sigma_i^2) - \mu_i^2 - \sigma_i^2), \quad (4)$$

$$\theta^*_{gip},\theta^*,\varphi^* = \arg\min_{Q} L(\theta_{gip},\theta,\varphi,\mathbf{A}_{train}), \quad (5)$$

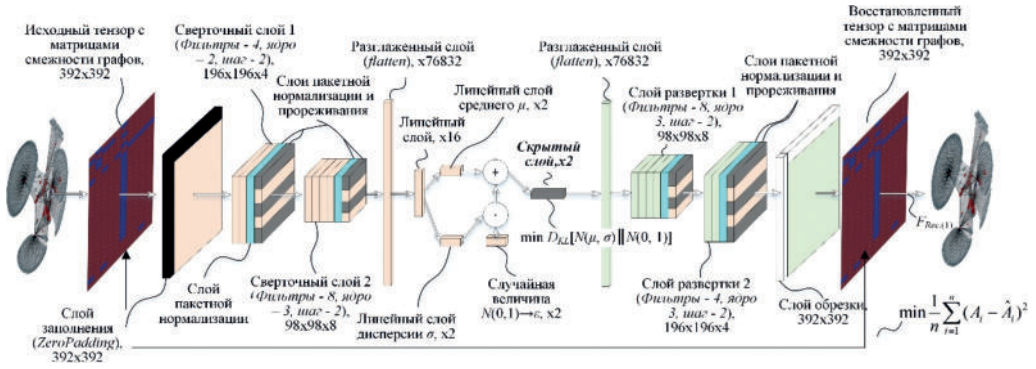
где, k_1, k_2 – коэффициенты значимости целевых функций; θ_{gip} – множество гиперпараметров генеративной модели (тип и количество нейронов, количество слоев кодера/декодера, активационная функция, количество эпох обучения, размер обучающей выборки, размер пакетов); θ, φ – свободные параметры кодировщика и декодировщика (веса и смещения нейронов); $\mathbf{A}_{train}$ – тренировочный массив данных с матрицами смежности исходных топологий вычислительных сетей; D_{KL} – дивергенция Кульбака-Лейблера между распределением представлений графов в скрытом пространстве $Z \sim N(\boldsymbol{\mu}, \boldsymbol{\sigma})$ и многомерным стандартным нормальным распределением $N(\mathbf{0}, \mathbf{I})$; MSE – среднее квадратическое отклонение между исходными матрицами смежности A_i из тензора A_{real} и реконструируемыми матрицами смежности $\hat{A}i$; Q – допустимое множество значений целевых функций и аргументов; N_{Lat} – размерность скрытого пространства Z генеративной модели; n – количество наблюдений (матриц смежности) в пакете с обучающими данными.

Архитектуры моделей, оптимальные гиперпараметры θ^*_{gip} сверточного и графового вариационных автокодировщиков, используемых для синтеза ложной топологии вычислительной сети, состоящей из 392 вершин, представлены на рис. 4.

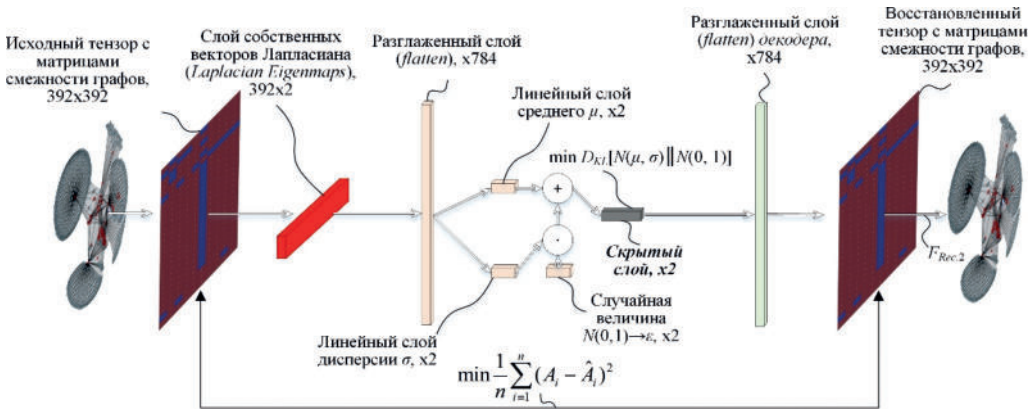
В соответствии с замыслом работы показателем защищенности реальной вычислительной сети при генерации ложной топологии вычислительной сети является *аппроксимация дистанции между множеством реальных и ложных критических узлов*. В качестве данной характеристики используется среднее кратчайшее расстояние D между критическими ложными и реальными узлами, а также коэффициент Жаккара J_{crit} между множеством критических ложных и исходных узлов. То есть, защищенность реальной вычислительной сети повышается если в среднем реальные критические узлы расположены дальше от ложных критических узлов, при этом отсутствуют пересечения между множеством ложных и реальных критических узлов. При рассмотрении только топологических характеристик, расстояние D рассчитывается в *хопах* (*скачках*), то есть в среднем минимальном количестве промежуточных узлов между множествами критических узлов.

Правдоподобие или сходство генерируемой ложной топологии вычислительной сети оценивается с помощью функционала сходства ложной и реальной топологии, в качестве которого используется коэффициент Жакарра J_{edge} между множеством ребер ложной и реальной вычислительной сети.

В соответствии с заданными критериями качества ложных топологий выбор оптимальных точек из скрытого пространства вариационного автокодировщика производится на основе решения следующей задачи многокритериальной оптимизации (выражение 6). Решение данной задачи в общем случае имеет множество Парето оптимальных решений. Использование *метаэвристических алгоритмов* получило широкое распространение при решении задач многокритериальной оптимизации, в частности, популяционные, эволюционные и смешанные



а)



б)

Рис. 4. Архитектуры вариационных автокодировщиков с оптимальными гиперпараметрами, предназначенные для синтеза матрицы смежности ложной вычислительной сети с заданными характеристиками: а) сверточный вариационный автокодировщик, б) графовый вариационный автокодировщик; где, F_{Rec1}, F_{Rec2} – функции округления выходных тензоров

алгоритмы [16–18]. Выбор конкретного алгоритма осуществляется на основе априорной информации о свойствах целевых функций, ограничений и требований к вычислительной сложности.

$$\begin{cases} J_{edge}(\theta_{hid}, A_{real}) \longrightarrow \max\limits_{Q_2}, \\ D(\theta_{hid}, A_{real}) \longrightarrow \max\limits_{Q_2}, \\ J_{crit}(\theta_{hid}, A_{real}) \longrightarrow \min\limits_{Q_2}. \end{cases} \quad (6)$$

где, $\theta_{hid}=(\theta^{hid}_1,\ldots,\theta^{hid}_m)$ – координаты скрытого пространства вариационного автокодировщика в пространстве R^{Nlat}, используемые для синтеза оптимальный топологии ложной вычислительной сети A; Q_2 – допустимое множество значений целевых функций и аргументов.

Рассмотрим упрощенный случай, в котором скрытое пространство генеративных моделей имеет всего два измерения, а решение задачи многокритериальной оптимизации осуществляется посредством сведения к скалярной функции. Поиск точки синтеза (x^*_1, x^*_2) ложной структуры в скрытом пространстве R^2 генеративной модели осуществлялся посредством минимизации функционала качества f, представленного в форме ненормированной взвешенной линейной свертки критериев (выражения 7–9):

$$f = \alpha_1 \cdot \bar{J}_{edge}(x_1,x_2) + \\ + \alpha_2 \cdot (D(x_1,x_2) + \varepsilon)^{-1} + \alpha_3 \cdot J_{crit}(x_1,x_2), \quad (7)$$

$$f \longrightarrow \min\limits_{Q_3}, (x^*_1,x^*_2) = \arg\min\limits_{Q_2} f(x_1,x_2), \quad (8)$$

$$Q_3 = \begin{cases} \alpha_1 \in [0,1],\ \alpha_2 \in [0,1],\ \alpha_3 \in [0,1], \\ \bar{J}_{edge}(x_1,x_2) \in [0,1],\ \varepsilon = 1{,}0, \\ J_{crit}(x_1,x_2) \in [0,1],\ D(x_1,x_2) \geq 0, \\ x_1,x_2 \in [-50,50]. \end{cases} \quad (9)$$

где, α_1, α_2, α_3 – коэффициенты значимости целевых функций; x_1, x_2 – координаты точки в скрытом пространстве R^2; ε – поправочный коэффициент, предотвращающий деление на 0.

В общем случае характер распределения значений целевых функций L (выражения 1–5) и f (выражения 7–9), количество локальных экстремумов, обусловленность моделей, неизвестны, несмотря на то, что распределения точек скрытого пространств в генеративных моделях близки к стандартному

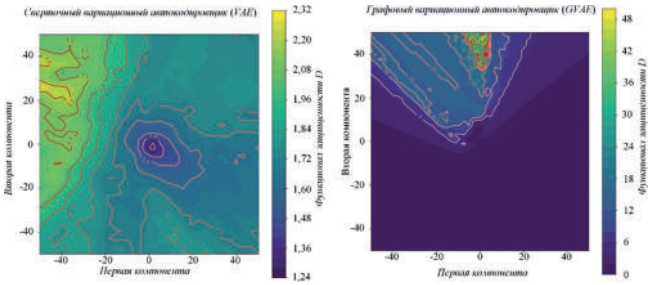


Рис. 5. Распределение среднего кратчайшего расстояния между реальными и ложными критическими узлами D в скрытых пространствах обученных генеративных моделей

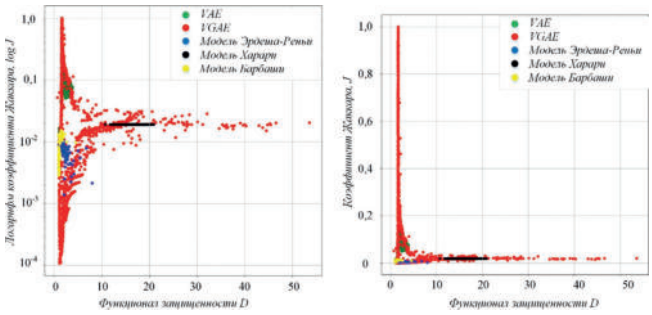


Рис. 6. Сравнение допустимого множества в критериальном пространстве показателей качества классических моделей случайных графов и вариационных автокодировщиков

нормальному. В работе решение указанных задач оптимизации осуществлялось с использованием алгоритма байесовской оптимизации, имеющего приемлемую сложность и сходимость для многопараметрических задач.

Распределения показателя защищенности D топологий ложных вычислительных сетей, синтезируемых из соответствующих точек двумерных скрытых пространств генеративных моделей, характеризуются значительными различиями как в характере распределений, так и в диапазонах значений. Так для сверточного вариационного автокодировщика среднее кратчайшее расстояние D находится в диапазоне от 1,24 до 2,32 хопов, при этом минимальные значения сгруппированы в окрестности центральной точки с координатами (0, 0), а для архитектуры графового вариационного автокодировщика наибольшие значения показателя D распределены дальше от центральной точки, при этом имеет место более широкий диапазон значений от 0 до 48 хопов (рис. 5).

Для сравнительной характеристики качества различных генеративных моделей на рис. 6 изображены допустимые множества соотношений первых двух критериев качества ложных топологий в двумерном критериальном пространстве для моделей Эрдеша-Реньи, Барбаши, Харари, сверточного и графового вариационных автокодировщиков. Стоит отметить, что при использовании моделей безразмерных графов топологические характеристики синтезируемых графов распределены в относительно узких диапазонах, однако, вычислительная сложность данных моделей является очень низкой, что позволяет их использовать для синтеза топологий с количеством вершин более 10^3.

С другой стороны, модели искусственного интеллекта показывают значительно более широкий диапазон характеристик качества структур, причем для архитектуры графового вариационного автокодировщика имеет место наибольший диапазон возможных топологических характеристик синтезируемых структур. Тем не менее с связи со сложностью матричных разложений данная архитектура является наиболее требовательной к вычислительным ресурсам.

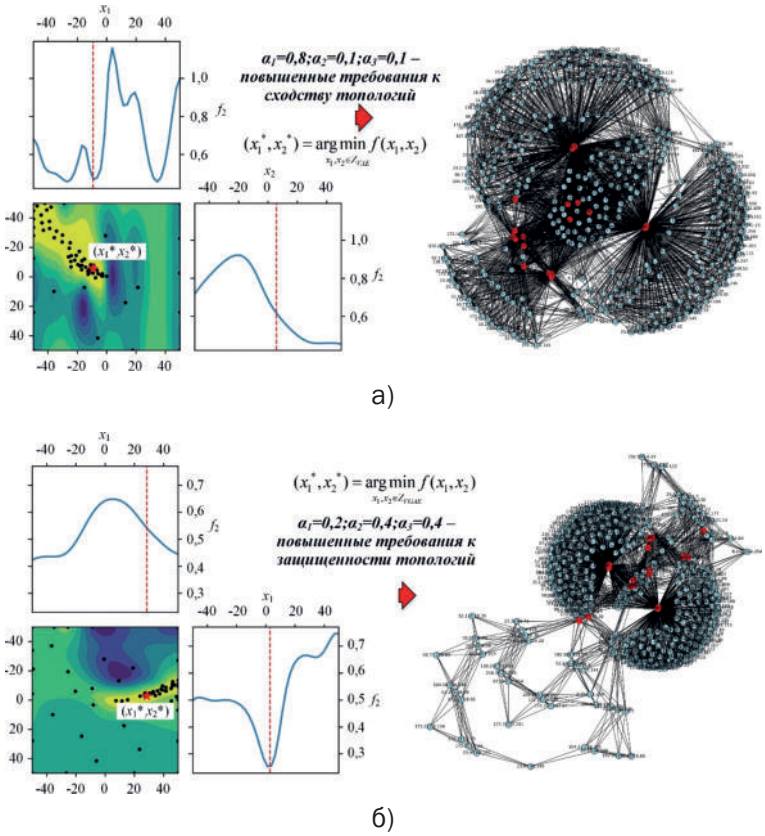


Рис. 7. Результаты решения задачи выбора оптимальной точки реконструкции ложной топологии вычислительной сети с использованием модели графового вариационного автокодировщика: а) при значениях коэффициентов значимости α_i, повышающих предпочтение к сходству ложной топологии; б) при значениях коэффициентов значимости α_i, повышающих предпочтение к защищенности критических узлов

Практическое применение. Генерация ложного сетевого трафика может быть реализована на различных устройствах, поддерживающих возможности отправки сообщений с заданными сетевыми параметрами (маршрутизаторы, межсетевые экраны, компьютеры). Ресурсы устройств, выполняющих вычислительную задачу по синтезу ложной топологии, влияют на выбор архитектуры, оптимальных значений гиперпараметров и свободных параметров генеративных моделей. Ложные сетевые информационные объекты (приманки, ловушки) в качестве источников ложного трафика могут быть развернуты на базе одного (с помощью управляемых виртуальных сетевых интерфейсов) или нескольких серверов. При ограниченных вычислительных ресурсах (генераторы на основе микрокомпьютеров и объемом оперативной памяти до 4 Гбайт) для синтеза ложной структуры целесообразно использовать модели со значительно меньшим количеством параметров (эвристические алгоритмы, модели случайных графов и ансамбли из простейших моделей случайных графов). Также модели с низкой пространственной сложностью целесообразно использовать в случаях, когда сетевой трафик содержит тысячи узлов и десятки тысяч ребер, так как обучающие тензоры $\mathbf{A}_{train}$ будут требовать значительных объемов оперативной памяти, в связи с тем, что асимптотические оценки сложности рассмотренных генеративных моделей, при фиксированных параметрах сверточных слоев и размера матрицы собственных векторов Лапласиана, составляют $O(N^2)$.

Вывод

Для маскирования топологических характеристик вычислительных сетей относительно большой размерности (при $10^2 < N < 10^3$) целесообразно использовать модели и методы генеративного искусственного интеллекта на вычислительных устройствах, способных обеспечить работоспособность конвейеров машинного обучения:

- архитектуры графового и сверточного вариационных автокодировщиков позволяют обрабатывать немаркированные данные из сетевого трафика, обладают относительно невысокой пространственной и временной сложностью при рассмотренных ограничениях на размерность составной сети, имеют возможность синтезировать ложные топологии вычислительных сетей в широких диапазонах показателей качества;
- модель выборки, задающая характеристики ложной топологии, может включать коэффициент Жаккара между множеством ребер реальной и ложной топологии в качестве показателя сходства, коэффициент Жаккара между множеством ложных и реальных критических узлов, а также среднее кратчайшее расстояние между реальными и ложными критическими узлами в качестве показателей защищенности;
- для поиска оптимальных точек синтеза ложной топологии в скрытом пространстве генеративных моделей целесообразно использовать метаэвристические алгоритмы скалярной и многокритериальной оптимизации, в частности, алгоритм байесовской оптимизации;
- модели случайных графов целесообразно использовать на этапе формирования набора данных для обучения генеративных моделей либо в качестве генераторов ложных топологий с количеством вершин $N > 10^3$.

Литература

1. *Горбачев А. А., Максимов Р. В. Проблема маскирования и применения технологий машинного обучения в киберпространстве // Вопросы кибербезопасности. 2023. № 5 (57). С. 37–49. DOI: 10.21681/4311-3456-2023-5-37-49.*
2. *Москвин А. А., Максимов Р. В., Горбачев А. А. Модель, оптимизация и оценка эффективности применения многоадресных сетевых соединений в условиях сетевой разведки // Вопросы кибербезопасности. 2023. № 3 (55). С. 13-22. DOI: 10.21681/2311-3456-2023-3-13-22.*
3. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Methodology for sustaniating the characteristics of false network traffic to simulate information systems // Selected Papers of the XI International Scientific and Technical Conference on Secure Information Technologies (BIT-2021). 2021. p. 115–124.*
4. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Honeypots network traffic parameters modelling // Selected Papers of the XI International Scientific and Technical Conference on Secure Information Technologies (BIT-2021). 2021. p. 229–239.*
5. *Кузьмин В. Н., Шуваев Ф. Л., Розганов М. В. Сравнительный анализ моделей случайных графов // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2022. №. 58. С. 23–34.*
6. *Лыгин В. С., Сирота А. А., Головинский П. А. Регуляризация процесса обучения графовых нейронных сетей методом распространение меток // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2024. №. 3. С. 92–101. DOI: 10.17308/sait/1995-5499/2024/3/92-101.*
7. *Schweinberger M., Krivitsky P. N., Butts C. T., Stewart J. R. Exponential-Family Models of Random Graphs: Inference in Finite, Super and Infinite Population Scenarios. Statistical Science. 2020. Vol. 35. No. 4. pp. 627–662. DOI: 10.1214/19-STS743.*
8. *Fanourakis N., Efthymiou V., Kotzinos D., Christophides V. Knowledge graph embedding methods for entity alignment: experimental review. Data Mining and Knowledge Discovery. 2023. Vol. 37. pp. 2070–2137. DOI: 10.1007/s10618-023-00941-9.*
9. *Said A., Shabbir M., Hassan S., Hassan Z. R., Ahmed A., Koutsoukos X. On augmenting topological graph representations for attributed graphs. Applied Soft Computing. 2023. Vol. 136. 110104. DOI: 10.1016/j.asoc.2023.110104.*
10. *Van Der Hofstad R. Random graphs and complex networks. Cambridge university press. 2024. Volume 2. 492 p.*

11. *Xu M. Understanding Graph Embedding Methods and Their Applications. Society for Industrial and Applied Mathematics. 2021. Vol. 63. No 4. pp. 825–853. DOI: 10.1137/20M1386062.*
12. *Li J., Fu X., Sun Q., Ji C., Tan J., Wu J., Peng H. Curvature graph generative adversarial networks. In Proceedings of the ACM web conference 2022. 2022. pp. 1528–1537. DOI: 10.1145/3485447.3512199.*
13. *Naveed H. et al. A comprehensive overview of large language models // ArXiv. 2023. pp. 1–35.*
14. *Коробцов В.И., Овсянников И.В., Сачков Д.И. Автоматическая генерация надежного программного кода с помощью генеративных предобученных трансформеров (GPT) // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. 2024. №1. С.52–59.*
15. *Mrabah N., Bouguessa M., Ksantini R. Beyond The Evidence Lower Bound: Dual Variational Graph Auto-Encoders For Node Clustering. In Proceedings of the 2023 SIAM International Conference on Data Mining (SDM). 2023. pp. 100–108.*
16. *Sharma S., Kumar V. A comprehensive review on multi-objective optimization techniques: Past, present and future. Archives of Computational Methods in Engineering. 2022. Vol. 29(7). pp. 5605–5633. DOI: 10.1007/s11831-022-09778-9.*
17. *Asfar B., Miettinen K., Ruiz F. Assessing the performance of interactive multiobjective optimization methods: A survey. ACM Computing Surveys (CSUR). 2021. Vol. 54(4). pp. 1–27. DOI: 10.1145/3448301.*
18. *Liu S., Lin Q., Wong K. C., Li Q., Tan K. C. Evolutionary large-scale multiobjective optimization: Benchmarks and algorithms. IEEE Transactions on Evolutionary Computation. 2021. Vol. 27(3). pp. 401–415. DOI: 10.1109/TEVC.2021.3099487.*

MASKING THE TOPOLOGICAL PROPERTIES OF COMPUTER NETWORKS IN THE CONDITIONS OF NETWORK RECONNAISSANCE. Part 2

Gorbachev A. A.[7]

Keywords: *false information objects, variational autoencoder, machine learning pipeline, artificial intelligence, optimization, metaheuristic algorithms, random graphs.*

The purpose of the study: *to develop a model system including classical random graph models and generative artificial intelligence models designed to solve the problem of masking the topological properties of computer networks when generating false network traffic and using false network information objects, allowing on the one hand to ensure a given degree of similarity of the topological properties of real computer networks with false ones, and on the other hand to maximize an indicator of the security of critical nodes of real computer networks.*

Methods used: *Erdos-Renyi random graph, Barbashi, Watts-Strogatz, Harari, Bayesian optimization algorithm, convolutional variational autoencoder model, graph variational autoencoder model, weighted additive linear convolution.*

The result of the study: *the presented system of models makes it possible to increase the effectiveness of protecting a computer network by forming a stable false idea in an attacker about the topological properties of a computer network, taking into account the increased security of critical nodes by shifting the position of false critical nodes relative to real ones, while ensuring a given degree of similarity of the false topology of a computer network in relation to the real topology. The model system includes a machine learning pipeline based on random graph models of Erdos-Renyi, Barbashi, Watts-Strogatz, Harari, used to form a training dataset, a graph variational autoencoder model, a hidden space sampling model containing quality indicators of the generated false structure, an evolutionary scalar optimization algorithm that searches for the optimal synthesis point a false structure in the hidden space of a variational auto-encoder, as well as a false traffic generator, which implements sending packets with the specified network identifiers. The developed pipeline has limitations in the dimension of the synthesized false topology due to the computational complexity of the generative model learning process and the search for the optimal synthesis point.*

Scientific novelty: *it consists in the application of a Bayesian optimization algorithm to select the optimal point for the synthesis of a false topology from the hidden space of a trained graph variational autoencoder, in using the objective function represented by a linear weighted convolution from the Jacquard coefficient between the set of edges of the false and real topology of the computer network, indicators of the security of the computer network: the average shortest distance between real and false critical nodes, the Jacquard coefficient between the set of false and real critical nodes of a computer network. In the application of random graph models to form a training dataset.*

References

1. *Gorbachev A.A., Maksimov R.V. Problema maskirovaniya i primeneniya texnologij mashinnogo obucheniya v kiberprostranstve // Voprosy` kiberbezopasnosti. 2023. № 5 (57). S. 37–49. DOI:10.21681/4311-3456-2023-5-37-49.*

7 Gorbachev Alexander, candidate of technical sciences. Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: infosec23.00@mail.ru

2. *Moskvin A.A., Maksimov R.V., Gorbachev A.A. Model', optimizaciya i ocenka e'ffektivnosti primeneniya mnogoadresny'x setevy'x soedinenij v usloviyax setevoj razvedki // Voprosy` kiberbezopasnosti. 2023. № 3 (55). S. 13-22. DOI: 10.21681/2311-3456-2023-3-13-22.*
3. *Maximov R.V., Sokolovsky S.P., Telenga A.P. Methodology for sustaniating the characteristics of false network traffic to simulate information systems // Selected Papers of the XI International Scientific and Technical Conference on Secure Information Technologies (BIT-2021). 2021. p. 115–124.*
4. *Maximov R.V., Sokolovsky S.P., Telenga A.P. Honeypots network traffic parameters modelling // Selected Papers of the XI International Scientific and Technical Conference on Secure Information Technologies (BIT-2021). 2021. p. 229–239.*
5. *Kuz'min V.N., Shuvaev F.L., Rozganov M.V. Sravnitel'ny'j analiz modelej sluchajny'x grafov // Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie, vy`chislitel`naya texnika i informatika. 2022. №. 58. S. 23–34.*
6. *Ly'gin V.S., Sirota A.A., Golovinskij P.A. Regulyarizaciya processa obucheniya grafovy`x nejronny`x setej metodom rasprostranenie metok // Vestnik VGU. Seriya: Sistemny`j analiz i informacionny`e texnologii. 2024. №. 3. S. 92–101. DOI: 10.17308/sait/1995-5499/2024/3/92-101.*
7. *Schweinberger M., Krivitsky P.N., Butts C.T., Stewart J.R. Exponential-Family Models of Random Graphs: Inference in Finite, Super and Infinite Population Scenarios. Statistical Science. 2020. Vol. 35. No. 4. pp. 627–662. DOI: 10.1214/19-STS743.*
8. *Fanourakis N., Efthymiou V., Kotzinos D., Christophides V. Knowledge graph embedding methods for entity alignment: experimental review. Data Mining and Knowledge Discovery. 2023. Vol. 37. pp. 2070–2137. DOI: 10.1007/s10618-023-00941-9.*
9. *Said A., Shabbir M., Hassan S., Hassan Z.R., Ahmed A., Koutsoukos X. On augmenting topological graph representations for attributed graphs. Applied Soft Computing. 2023. Vol. 136. 110104. DOI: 10.1016/j.asoc.2023.110104.*
10. *Van Der Hofstad R. Random graphs and complex networks. Cambridge university press. 2024. Volume 2. 492 p. DOI: 10.1137/20M1386062.*
11. *Xu M. Understanding Graph Embedding Methods and Their Applications. Society for Industrial and Applied Mathematics. 2021. Vol. 63. No 4. pp. 825–853. DOI: 10.1145/3485447.3512199.*
12. *Li J., Fu X., Sun Q., Ji C., Tan J., Wu J., Peng H. Curvature graph generative adversarial networks. In Proceedings of the ACM web conference 2022. 2022. pp. 1528–1537.*
13. *Naveed H. et al. A comprehensive overview of large language models // ArXiv. 2023. pp. 1–35.*
14. *Korobczov V.I., Ovsyannikov I.V., Sachkov D.I. Avtomaticheskaya generaciya nadezhnogo programmnogo koda s pomoshh'yu generativny'x predobuchenny'x transformerov (GPT) // «Informacionny'e texnologii i matematicheskoe modelirovanie v upravlenii slozhny'mi sistemami»: e'lektron. nauch. zhurn. 2024. №1. S. 52–59.*
15. *Mrabah N., Bouguessa M., Ksantini R. Beyond The Evidence Lower Bound: Dual Variational Graph Auto-Encoders For Node Clustering. In Proceedings of the 2023 SIAM International Conference on Data Mining (SDM). 2023. pp. 100–108.*
16. *Sharma S., Kumar V. A comprehensive review on multi-objective optimization techniques: Past, present and future. Archives of Computational Methods in Engineering. 2022. Vol. 29(7). pp. 5605–5633. DOI: 10.1007/s11831-022-09778-9.*
17. *Asfar B., Miettinen K., Ruiz F. Assessing the performance of interactive multiobjective optimization methods: A survey. ACM Computing Surveys (CSUR). 2021. Vol. 54(4). pp. 1–27. DOI: 10.1145/3448301*
18. *Liu S., Lin Q., Wong K.C., Li Q., Tan K.C. Evolutionary large-scale multiobjective optimization: Benchmarks and algorithms. IEEE Transactions on Evolutionary Computation. 2021. Vol. 27(3). pp. 401–415. DOI: 10.1109/TEVC.2021.3099487.*

УПРАВЛЕНИЕ АКТИВАМИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ КАК ОБЯЗАТЕЛЬНЫЙ ЭТАП УПРАВЛЕНИЯ ИХ УЯЗВИМОСТЯМИ

Милославская Н. Г.[1], Толстой А. И.[2]

DOI: 10.21681/2311-3456-2025-1-73-85

Цель работы: *систематизация подходов к управлению активами (УА) информационно-телекоммуникационных сетей (ИТКС) организаций как обязательному этапу управления их уязвимостями для последующего исключения возможности эксплуатации (использования) обнаруженных уязвимостей в рамках управления сетевой безопасностью ИТКС и разработки краткой инструкции по реализации процесса УА ИТКС.*

Методы исследования: *анализ релевантных нормативных документов и научных публикаций, концептуальное моделирование, экспертная оценка, синтез комплексного подхода к управлению активами в рамках управления сетевой безопасностью.*

Полученные результаты: *в статье вводится понятийная база УА ИТКС и на основе специально подобранной нормативной базы систематизируются подходы к УА ИТКС организаций как обязательному этапу управления их уязвимостями с целью последующего устранения этих уязвимостей. Выделяются мероприятия, реализуемые в ходе процесса УА ИТКС, особенно при идентификации активов ИТКС, и обсуждается состав системы УА (СУА) ИТКС, ориентированный на минимизацию возможности осуществления компьютерных атак на ИТКС организации. Кратко рассматриваются основные документы СУА ИТКС – стратегический план УА ИТКС, планы УА нижнего уровня и политика УА ИТКС, предназначенные для достижения целей УА ИТКС. На основе проведенного исследования с соблюдением принципа разумной достаточности разработана краткая пошаговая инструкция по реализации процесса УА ИТКС.*

Практическая значимость *заключается в разработке краткой инструкции по реализации процесса УА ИТКС, особенно процесса идентификации активов ИТКС, в рамках управления сетевой безопасностью ИТКС при решении задач устранения найденных для активов ИТКС уязвимостей, что, в свою очередь, приведет к минимизации возможностей реализации компьютерных атак на ИТКС организаций.*

Ключевые слова: *информационно-телекоммуникационная сеть, управление активами, процесс управления активами, система управления активами, управление уязвимостями активов, управление сетевой безопасностью.*

Введение

Деятельность современных организаций в различных сферах человеческой деятельности невозможно представить без использования информационных технологий (ИТ) и построенных на их основе ***информационно-телекоммуникационных сетей (ИТКС)***. В Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ИТКС определена как технологическая система (ТС), предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (СВТ)[3]. В свою очередь ТС представляет собой совокупность технических и программных средств, обеспечивающая передачу информации на значительные расстояния с использованием коммутируемых и выделенных линий или специальных каналов связи[4], а СВТ — это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем[5].

Используя ИТКС организации, ее сотрудники работают на постоянной или временной основе, выполняя свои функциональные обязанности и пользуясь всем спектром предоставляемых услуг [1]. Но в то же время по единодушным оценкам различных аналитиков каждый день фиксируется огромное

1 Милославская Наталья Георгиевна, доктор технических наук, Ph.D. in Cybersecurity, доцент, НИЯУ МИФИ, Москва, Россия. E-mail: NGMiloslavskaya@mephi.ru, https://orcid.org/0000-0002-1231-1805

2 Толстой Александр Иванович, кандидат технических наук, доцент, НИЯУ МИФИ, Москва, Россия. E-mail: aitolstoj@mephi.ru, https://orcid.org/0000-0001-9265-1510

3 Об информации, информационных технологиях и о защите информации / Федеральный закон от 27 июля 2006 г. № 149-ФЗ, статья 2: принят Гос. Думой 8 июля 2006 г.; одобрен Советом Федерации 14 июля 2006 г. – 2006. – 88 с.

4 Руководство по организации эксплуатации информационно-телекоммуникационной системы Банка России: в 2 томах. [Электронный ресурс]. М.: АС «Сфинкс», 2008. № НМД-4. 1 электрон, опт. диск (CD-ROM).

5 ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. – Введен 1996-01-01. – М., Госстандарт РФ, 1995. – 8 с.

количество компьютерных атак (КА), направленных на получение любой ценной информации – коммерческой, служебной, технической, персональных данных (ПДн), сведений об учетных записях пользователей, почтовых сообщений, конфигурационных файлов, журналов регистрации событий и т.п. [2–4]. А далее для реализации новых КА (поиска уязвимых ресурсов, получения первичного доступа к ИТКС, кражи данных и т.д.) используются полученные в результате предыдущих КА данные, находящиеся в открытом доступе (англ. *Open Source Intelligence – OSINT*) [5].

На SOC-форуме[6], состоявшемся в Москве 6–8 ноября 2024 г., сотрудники ПАО «Сбербанк» подчеркнули, что ПДн 90 % населения есть в интернете[7]. В начале года фиксировалось около 20 млн попыток дозвона мошенников до граждан в сутки, но благодаря новым разработкам эта цифра снизилась к концу года до 6–8 млн. На межотраслевой конференции «Безопасность клиента на первом месте» (19 ноября 2024 г.) было уточнено, что 50 % этих звонков осуществляется с мессенджеров с применением технологий SIM-box (устройства, поддерживающего несколько SIM-карт, подключенных к одному шлюзу) и виртуальных автоматических телефонных станций (АТС).

Представители ФСТЭК России в своих выступлениях 2023–2024 гг. неоднократно отмечали КА через критические уязвимости на периметре и цепочки поставок (англ. *supply chains*) [7], а также неистребимый фишинг, основанный на доверии людей [8]. Среди главных целей атакующих – нарушение функционирования ИТ-инфраструктур компаний или даже их разрушение и уничтожение, стирание информации, чтобы информационные системы (ИС) больше не могли работать [9], а также ее шифрование с целью выкупа [10].

Компьютерные преступления могут приобретать и еще более изощренные формы, особенно в период нестабильной политической ситуации. Отключения провайдеров от крупных магистральных каналов, атаки на СМИ для создания инфоповодов и вызова общественного резонанса, появление вредоносного кода в обновлениях программного обеспечения (ПО) – вот лишь некоторые из них.

Новые технологии, такие как беспроводной доступ (*Wi-Fi*), виртуализация, интернет вещей (англ. *Internet of Things – IoT*), системы искусственного интеллекта (англ. *Artificial Intelligence*), изначально разрабатываемые без учета требований по обеспечению информационной безопасности (ИБ, ОИБ), также предоставляют злоумышленникам возможности для КА.

По данным МВД[8], 45 % компьютерных преступлений в 2024 г. связано с ИТКС, что в 2025 г. уже приблизится к 50 %.

Эксперты считают, что многие проблемы возникают из-за пренебрежения элементарными мерами ОИБ (например, неправильно сконфигурированные системы и оборудование), недостатка или даже отсутствия самых необходимых средств защиты информации (СЗИ) типа антивирусов из-за низкой приоритетности вопросов ОИБ при распределении ресурсов, недостаточно защищенных точек удаленного доступа к ИТКС, отсутствия разработанных и внедренных процессов реагирования на инциденты ИБ и выяснения причин произошедших нарушений ИБ, человеческого фактора, включая неправильное распределение обязанностей работников во избежание ситуаций, когда все зависит от одного человека, и недостаточного внимания, уделяемого непрерывному обучению специалистов по ИБ и повышению информированности остальных работников, и много другого.

Таким образом, можно сказать, что главный вопрос сегодня – не случится ли КА на организацию или отдельного индивидуума, а когда это произойдет, что во многом зависит от причин и условий реализации КА. Следовательно, как никогда ранее необходимо уделять должное внимание вопросам, связанным с управлением уязвимостями активов ИТКС. Поэтому целью данной статьи является систематизация подходов к управлению активами (УА) ИТКС организаций как обязательному этапу управления их уязвимостями для последующего исключения возможности эксплуатации (использования) обнаруженных уязвимостей в рамках управления сетевой безопасностью ИТКС и разработка краткой инструкции по реализации процесса УА (ПУА) ИТКС.

1. Нормативная база управления активами

Российская нормативная база УА представлена следующими стандартами:

1) группа ГОСТ Р 55.0.0Х «Управление активами» в составе:
   - ГОСТ Р 55.0.00-2014[9], основополагающего в данной группе и устанавливающего общие положения и структуру национальной системы стандартов в области управления физическими и нематериальными активами;

6 SOC Forum 2024: подводя итоги. 12 ноября 2024 г. [Электронный ресурс]. – Режим доступа: https://ib-bank.ru/bisjournal/post/2333 (дата обращения: 30.12.2024).

7 Кошкин В. Топ-менеджер Сбербанка: Данные 90 % взрослых россиян есть в открытом доступе. 6 ноября 2024. // Российская газета [Электронный ресурс]. – Режим доступа: https://rg.ru/2024/11/06/top-menedzher-sberbanka-dannye-90-vzroslyh-rossiianest-v-otkrytom-dostupe.html (дата обращения: 30.12.2024).

8 МВД оценило ущерб от преступлений в бюджетной сфере в 2024 г. в 112 млрд рублей. 16 декабря 2024 г. [Электронный ресурс]. – Режим доступа: https://smotrim.ru/article/4269430 (дата обращения: 30.12.2024).

9 ГОСТ Р 55.0.00-2014 Управление активами. Национальная система стандартов. Основные положения. – Введ. 2015-04-01. – М., Стандартинформ, 2015. – 12 с.

- ГОСТ Р 55.0.01-2014/ИСО 55000:2014[10], дающего общее представление об УА и системе УА (СУА) и содержащего принципы УА и соответствующую терминологию, а также демонстрирующего ожидаемые выгоды от осуществления УА в большей степени для использования при управлении физическими активами;
- ГОСТ Р 55.0.02-2014/ИСО 55001:2014[11], устанавливающего требования к разработке, внедрению, поддержанию в рабочем состоянии и улучшению СУА в большей степени при управлении физическими активами с учетом внешнего и внутреннего контекста организации, что может повлиять на способность организации достичь намеченных результатов ее СУА;
- ГОСТ Р 55.0.03-2021[12], содержащего рекомендации по применению СУА в соответствии с требованиями ГОСТ Р 55.0.02 и дающего пояснения к указанным в ГОСТ Р 55.0.02 требованиям с примерами, демонстрирующими выполнение этих требований;
- ГОСТ Р 55.0.05-2016[13], устанавливающего требования к порядку выбора метода УА на этапе эксплуатации для принятия оптимального решения по повышению безопасности и надежности активов, основанного на оценке рисков и обеспечивающего выполнение активами своих функций;
- ГОСТ Р 55.0.06-2021[14], содействующего организациям в обеспечении согласованности финансовой и нефинансовой деятельности всех подразделений при УА как «по вертикали», так и «по горизонтали» с целью улучшить внутренний контроль при управлении организацией;

2) два стандарта по УА при управлении непрерывностью бизнеса:

   - ГОСТ Р 55235.1-2012[15], устанавливающий требования к СУА, направленные на обеспечение оптимального управления производственными активами и системами активов (информационных, нематериальных, финансовых и человеческих) на всех этапах их жизненного цикла;
   - ГОСТ Р 55235.2-2012[16], формулирующий основные принципы применения требований ГОСТ Р 55235.1 к оптимальному управлению производственными активами и содержащий руководство по созданию, внедрению, поддержке и улучшению системы управления производственными активами и ее взаимодействия с другими системами менеджмента организации;

3) ГОСТ Р ИСО/МЭК 27005-2010[17], описывающий весь процесс управления рисками ИБ, включая установление контекста (выходные данные процесса – спецификация основных критериев, область применения и границы, организационная структура для процесса управления рисками ИБ), идентификации рисков ИБ (выходные данные процесса – перечень активов, подлежащих управлению рисками, и перечень бизнес-процессов, связанных с активами, а также их ценность, выявление уязвимостей (выходные данные процесса – перечень уязвимостей, связанных с активами, угрозами и мерами ОИБ, и перечень уязвимостей, не связанных с выявленной угрозой, подлежащей рассмотрению), общая оценка и обработки рисков ИБ, а также принятие, обмен информацией (коммуникация), мониторинг и переоценка рисков ИБ.

Международная нормативная база УА опирается на стандарты ISO и ISO/IEC, указанные выше для идентичных им стандартов РФ, и их новые редакции, например, ISO 55000:2024, ISO 55001:2024, ISO/TS 55010:2024, ISO/IEC 27005:2022.

Отдельно разработана группа стандартов ISO/IEC 19770-X для управления ИТ-активами, первый из которых наиболее интересен в рамках тематики исследования, поскольку в нем изложены дополнительные или более подробные требования к управлению ИТ-активами. В РФ существует ГОСТ Р ИСО/МЭК 19770-1-2021[18], идентичный стандарту ISO/IEC 19770-1. Основным его отличием от стандартов ГОСТ Р 55.0.02-2014 и ИСО 55001:2014 является обоснование необходимости управления программными активами с их особыми характеристиками.

10 ГОСТ Р 55.0.01-2014/ИСО 55000:2014 Управление активами. Национальная система стандартов. Общее представление, принципы и терминология. – Введ. 2015-04-01. – М., Стандартинформ, 2015. – 24 с.

11 ГОСТ Р 55.0.02-2014/ИСО 55001:2014 Управление активами. Национальная система стандартов. Система менеджмента. – Введ. 2015-04-01. – М., Стандартинформ, 2015. – 16 с.

12 ГОСТ Р 55.0.03-2021 Управление активами. Система менеджмента. Руководство по применению ИСО 55001. – Введ. 2021-09-01. – М., Стандартинформ, 2021. – 58 с.

13 ГОСТ Р 55.0.05-2016 Управление активами. Повышение безопасности и надежности активов. Требования. – Введ. 2016-10-01. – М., Стандартинформ, 2018. – 15 с.

14 ГОСТ Р 55.0.06-2021 Управление активами. Руководство по обеспечению согласованности финансовой и нефинансовой деятельности при управлении активами. – Введ. 2016-09-01. – М., Стандартинформ, 2021. – 21 с.

15 ГОСТ Р 55235.1-2012 Практические аспекты менеджмента непрерывности бизнеса. Менеджмент активов. Требования к оптимальному управлению производственными активами. – Введ. 2013-12-01. – М., Стандартинформ, 2020. – 30 с.

16 ГОСТ Р 55235.2-2012 Практические аспекты менеджмента непрерывности бизнеса. Менеджмент активов. Руководство по применению требований к оптимальному управлению производственными активами. – Введ. 2013-12-01. – М., Стандартинформ, 2020. – 62 с.

17 ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Введ. 2011-12-01. – М., Стандартинформ, 2011. – 47 с.

18 ГОСТ Р ИСО/МЭК 19770-1-2021 Информационные технологии. Управление ИТ-активами. Часть 1. Системы управления ИТ-активами. Требования. – Введ. 2013-12-01. – М., Российский институт стандартизации, 2021. – 36 с.

Также заслуживает отдельного внимания опубликованный в США (2018 г.) документ NIST SP 1800-5[19] «IT Asset Management» в трех частях (NIST SP 1800-5A «Executive Summary», NIST SP 1800-5B «Approach, Architecture, and Security Characteristics» и NIST SP 1800-5C «How-To Guides»), который является подробным практическим руководством, демонстрирующим конкретные технологии и средства, подлежащие внедрению для отслеживания местоположения и конфигурации сетевых устройств и ПО в организации, включая традиционное отслеживание физических активов, информацию об ИТ-активах, физическую безопасность, а также информацию об уязвимостях и соответствии требованиям.

Представленные далее результаты работы базируются на данной нормативной базе.

2. Активы ИТКС

Как следует из названия, ИТКС представляет собой симбиоз двух видов сетей — информационной и телекоммуникационной. Эти сети территориально распределены по месту размещения, объединяют большое количество разнообразных технических средств обработки, передачи и хранения информации, различаются по масштабу, решаемым задачам и типам обрабатываемых данных.

Чаще всего ИТКС рассматривают как часть организации, реализующей определенные бизнес-процессы. При этом можно считать, что ИТКС оказывает организации внутренние ИТ-услуги (англ. *IT services*) на основе реализации совокупности процессов, связанных со сложными режимами автоматизированной обработки данных и совмещением выполнения информационных запросов различных категорий пользователей — потребителей информации и ИТ-услуг. При этом все составляющие ИТКС должны функционировать непрерывно и устойчиво в условиях высокой интенсивности информационных потоков [11] и существования угроз нанесения ущерба информации и ущерба функциональной устойчивости (ФУ) ИТКС (англ. *resilience*).

С учетом этого можно определить цели, которые необходимо достичь при использовании ИТКС в конкретной организации – это выполнение требований по реализации определенного набора процессов ИТКС для предоставления ИТ-услуг (функционал ИТКС), ОИБ ИТКС и обеспечению ФУ (ОФУ) ИТКС.

При ОИБ и ОФУ ИТКС как некоторого объекта прежде всего обращают внимание на ту его часть, которая признается наиболее ценной для его владельца и которую принято[20] называть активом объекта. В данной работе принимаются следующие термины [12] и их определения.

Актив (англ. *asset*) ***объекта*** (ИТКС) — наиболее ценная для владельца часть объекта (ИТКС).

Владелец актива – субъект, осуществляющий владение и пользование активом и реализующий полномочия распоряжения им в пределах, установленных законом.

Ценность актива объекта (ИТКС) будет определяться исходя из влияния актива на реализацию процессов самого объекта. При этом возможны принципиально отличающиеся два варианта: ИТКС как уникальный объект, реализующий определенные процессы, и ИТКС как часть организации, реализующая вспомогательные (обеспечивающие) процессы для ее бизнес-процессов.

При реализации соответствующих угроз ИБ (например, КА) на ИТКС их целью прежде всего являются активы ИТКС. Поэтому актуальным будет выполнение следующей совокупности необходимых действий для определения и описания активов ИТКС: формирование перечня активов с учетом их ценности, определение их свойств, классификация активов с учетом их видов и определение уязвимостей активов. Совокупность этих действий будем называть ***идентификацией активов объекта*** (ИТКС). При их выполнении необходимо учитывать следующие факторы.

В перечень активов ИТКС должны быть включены только те активы, которые непосредственно влияют на результативность процессов, реализуемых ИТКС, а также бизнес-процессов организации, если ИТКС рассматривается как объект этой организации. Причем ценность активов будет определяться с учетом уровня влияния активов на вышеуказанные процессы.

Поскольку активы ИТКС рассматриваются в контексте ОИБ и ОФУ ИТКС, то основными свойствами активов будут свойства ИБ (конфиденциальность, целостность, доступность[20]) и свойства ФУ (доступность и целостность процессов, реализуемых ИТКС, и свойства, определяющие готовность ИТКС к обеспечению непрерывности бизнеса[21]).

Активы ИТКС целесообразно классифицировать, разделив их на виды и группы[16]. При дальнейших рассуждениях возьмем за основу два вида активов ИТКС: основные и вспомогательные, которые разделяются на две группы: основные активы (информационные активы и процессы ИТКС) и вспомогательные активы (аппаратное обеспечение (АО), ПО, телекоммуникационное и сетевое оборудование (ТСО), бизнес-приложения, персонал, сама ИТКС (и, возможно, сама организация), место функционирования ИТКС и организации).

19 Stone M., Irrechukwu C., Perper H., Wynne D., Kauffman L. IT Asset Management. NIST SP 1800-5. September 2018. 237 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf. (дата обращения: 10.01.2025).

20 ГОСТ Р ИСО/МЭК 27000-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

21 ГОСТ Р ИСО 27031-2012 «Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».

Иногда в отдельный класс выделяют ***ИТ–актив*** (англ. *IT asset*) – это любая принадлежащая организации информация, система или оборудование, используемые в ее деятельности с применением ИТ. Из анализа приведенных выше примеров активов ИТКС можно сделать вывод, что ИТ-активы являются подмножеством как основных (информационные активы), так и вспомогательных (АО, ПО, ТСО) активов.

Для уточнения понятия «информационный актив» воспользуемся определениями понятия «информация», данные в Федеральном законе № 149-ФЗ[3] и в стандарте ГОСТ Р 50922-2006[22]. ***Информационный актив*** (ИА) (англ. *information asset*) – это информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для организации, находящаяся в распоряжении этой организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме[23]. При выделении ИА необходимо учитывать категории информации (общедоступная или ограниченного доступа) и возможные разновидности свойств ИБ, присущих отдельным ИА.

Именно вспомогательным активам присущи уязвимости, которые могут быть использованы угрозами ИБ, нацеленными на нанесение ущерба активам ИТКС.

Теперь определим важное понятие исследования – «***уязвимость (актива объекта)***» (англ. *vulnerability*). Это любая характеристика или свойство актива объекта, которое может быть использовано для реализации или способствовать реализации угрозы ИБ [11].

Если уязвимость соответствует угрозе, то существует риск нарушения свойств активов ИТКС. Уязвимости, например, активов ИС, могут использоваться для компрометации (взлома) объекта, в данном случае ИТКС. Деятельность по анализу и исключению возможностей их использования (эксплуатации) выявленных уязвимостей активов ИТКС обобщенно называют ***управлением уязвимостями***. Согласно методическому документу ФСТЭК России[24], этот процесс включает в себя пять основных этапов: мониторинг уязвимостей и оценка их применимости, оценка уязвимостей, определение методов и приоритетов исключения возможностей их использования (эксплуатации) уязвимостей угрозами нарушения безопасности информации (угрозами ИБ) в ИТКС или угрозами нарушения ФУ ИТКС, собственно реализация этих методов и контроль исключения возможностей использования (эксплуатации) уязвимостями. Очевидно, что перед началом осуществления процесса управления уязвимостями, необходимо идентифицировать все активы ИТКС, в которых эти уязвимости могут быть обнаружены. Такие действия выполняются в рамках реализации процессов идентификации и процессов управления активами ИТКС.

Имеется еще один аспект, относящийся к идентификации активов объектов (ИТКС). Результатом управления уязвимостями активов объекта может быть использование на объекте (в ИТКС) определенных мер ОИБ (средств и систем ОИБ и ОФУ объекта (ИТКС). Эти средства и системы имеют свои активы, возможно, обладающие уязвимостями, требующими реализации своих процессов идентификации активов и управления этими уязвимостями. В противном случае добавление в ИТКС средств и систем ОИБ может привести не к улучшению, а к ухудшению ситуации, связанной с ОИБ и ОФУ ИТКС.

Источником информации для формирования перечня активов ИТКС в аспекте необходимости ОИБ и ОФУ ИТКС является спецификация ИТКС, дополненная перечнем информации, обрабатываемой в ИТКС. Спецификация создается на этапе разработки (планирования) ИТКС с учетом требований к функционалу ИТКС на основе выполнения следующих действий (процессов): определение и описание основного процесса (бизнес-процесса) организации; определение и описание процессов, которые должны быть реализованы ИТКС в рамках оказания внутренних ИТ-услуг (вспомогательные процессы); разработка архитектуры ИТКС; обоснование и выбор информационных технологий и средств, которые будут использованы в ИТКС; разработка набора схем ИТКС (структурная, функциональная и принципиальная схемы).

Полную совокупность элементов спецификации можно назвать перечнем активов ИТКС. По сути, формируется три перечня активов ИТКС: полный перечень активов в контексте обеспечения реализации функционала, перечень активов в контексте ОИБ и перечень активов в контексте ОФУ ИТКС.

Эти перечни активов имеют следующие различия:

1) максимальное количество активов ИТКС имеет первый перечень;
2) разные подходы к определению ценностей активов;
3) активы из второго и третьего перечней являются обоснованной выборкой активов из первого перечня. Их количество не может превышать количество активов первого перечня. Второй и третий перечень могут включать разные активы;
4) выделение в качестве главных разных активов: все активы (первый перечень), ИА (второй перечень), процессы, реализуемые в рамках ИТ-услуг (третий перечень);
5) при идентификации активов их уязвимости не определяются для активов первого перечня;
6) уязвимости активов второго и третьего перечня могут быть разными.

22 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
23 Милославская Н. Г., Толстой А. И. Управление информационной безопасностью. Конспект лекций: учебное пособие. М., НИЯУ МИФИ, 2020. 534 с.
24 Федеральная служба по техническому и экспортному контролю. Методический документ. Руководство по организации процесса управления уязвимостями в органе (организации) (утв. ФСТЭК России 17 мая 2023 г.)

При идентификации активов рекомендуется определенный порядок действий: сначала идентификация активов первой, затем второй и далее третьей групп.

3. Процессы идентификации активов ИТКС

При идентификации активов ИТКС будем использовать процессный подход, который базируется на понятии «процесс». Опираясь на определения Большого толкового словаря русского языка [14] и ГОСТ Р ИСО 9000–2015, введем следующее «интегрирующее» определение: процесс – это совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующая входы (входные данные) в выходы (выходные данные) и требующая для этого определенных ресурсов и управляющих воздействий (управления) [15]. Входами для процесса обычно являются выходы других процессов, а выходы процессов – входами для других процессов. Выходные данные являются результатом процесса, в той или иной степени удовлетворяющие сформулированным заранее требованиям. Два или более взаимосвязанных и взаимодействующих процессов совместно могут также рассматриваться как процесс.

Действия, связанные с идентификацией активов объекта (ИТКС), можно рассмотреть как совокупность связанных процессов идентификации активов. В табл. 1 представлено описание этих процессов в части определения входных данных (К1i) и выходных данных (К2i) для каждого i-ого процесса, где $i = 1, \ldots, N$, N – количество процессов ($N = 4$).

Следует отметить, перечень процессов, представленных в табл. 1, относится к активам всех трех перечней, за исключением отсутствия процесса 4 для активов первого перечня.

Анализ данных из табл. 1 показывает, что все выделенные процессы связаны друг с другом. Причем во входные данные, начиная со второго процесса, входят выходные данные одного или нескольких предыдущих процессов. Входные данные первого процесса содержат данные описания процессов объекта (ИТКС) и бизнес-процессов организации, если объект является частью организации, выполненных в виде процессных моделей организации и объекта, а также данные функциональной схемы объекта (ИТКС) и его спецификации.

При описании процессов идентификации активов объекта (ИТКС) важным является определение целей реализации таких процессов. В данном случае цель реализации конкретного процесса идентификации совпадает с выходом этого процесса (табл. 1).

Необходимо отметить дополнительные различия в описании процессов идентификации активов объекта (ИТКС), относящихся к различным перечням активов.

1. Идентификация активов в контексте ОИБ ИТКС и ОФУ ИТКС осуществляется на стадии планирования (проектирования) системы ОИБ (СОИБ) и системы ОФУ (СОФУ) ИТКС соответственно.
2. Идентификация активов в контексте обеспечения функционала ИТКС должна проводится в отношении процессов различных стадий жизненного цикла

Таблица 1.

Описание процессов идентификации активов объекта (ИТКС)

№ п/п	Процессы идентификации активов объекта	Входные данные К1i	Выходные данные К2i
1	Формирование перечня активов с учетом их ценности	К11: Процессная модель объекта и организации, функциональная схема и спецификация объекта	К12: Перечень активов с определением их связей с процессами объекта и организации и определением их ценности
2	Определение свойств активов	К21 = К12 Перечень активов с определением их связей с процессами объекта и организации и определением их ценности	К22: Перечень активов с определением их свойств и указанием приоритетов по сохранению этих свойств
3	Проведение классификации активов	К31 = К11 + К21 + К22	К32: Результаты классификации активов с учетом их видов, типов и категорий
4	Определение уязвимостей активов	К41 = К32	К42: Перечень и описание уязвимостей активов объекта

активов ИТКС. К таким процессам, например, можно отнести процессы, связанные с приобретением, учетом (инвентаризацией), эксплуатацией, обслуживанием, модернизацией и выводом из эксплуатации (утилизацией) активов ИТКС.

3. Возможны разные варианты регламента идентификации активов с учетом необходимости формирования разных перечней активов ИТКС:
   - первый (наиболее простой) основан на последовательной раздельной разработке ИТКС, СОИБ ИТКС и СОФУ ИТКС. Такой подход предусматривает сначала формирование первого перечня активов с учетом только требований к функционалу ИТКС. Далее этот перечень фиксируется и остается неизменным при формировании второго и третьего перечней активов;
   - второй (итерационный, более сложный) предусматривает итерацию следующих действий: разработка ИТКС, СОИБ и СОФУ, анализ выполнимости требований по ОИБ и/или ОФУ ИТКС с этим набором ИТ и/или реализующих их средств, определение необходимости их замены, выбор новых ИТ и/или реализующих их средств, возврат к разработке ИТКС, СОИБ и СОФУ с корректированными перечнями активов. Этот итерационный процесс необходимо продолжать до удовлетворения всех требований по обеспечению функционала, ОИБ и ОФУ ИТКС.

4. Процессы управления активами ИТКС

Процессный подход предполагает, что достижение определенной цели реализации конкретного процесса возможно только при результативном управлении этим процессом. С учетом этого, взяв за основу стандарт ГОСТ Р 55235.1, можно сформулировать определение следующего понятия: ***управление активами объекта (УА)*** (англ. *asset management*) – это постоянная и скоординированная деятельность по реализации ценности от активов объекта для стабильного достижения основных целей деятельности организации [16]. Все действия (бизнес-практики) по управлению активами необходимо выполнять и поддерживать на разных уровнях управления организацией.

Учитывая положения группы стандартов ГОСТ Р 55.0.0Х, можно определить следующие принципы, на которых должно базироваться УА ИТКС:

- ценность, предоставляемая активами ИТКС, которая может быть материальной или не материальной, финансовой или не финансовой, непосредственно связана с удовлетворением требований заинтересованных сторон;
- согласованность целей УА ИТКС (т.е. результаты, которые должны быть достигнуты при УА ИТКС) с целями организации;
- лидерство и приверженность на всех уровнях управления, которые необходимы для успешного создания, функционирования и улучшения УА ИТКС в организации;
- предоставление гарантий того, что активы ИТКС будут выполнять требуемые от них функции.

Согласно ГОСТ Р 55235.Х, основными принципами УА ИТКС с несколько иной точки зрения являются целостность, систематичность, системность, обоснованность с точки зрения риска, оптимальность, жизнеспособность, интегрированность.

Принципиально важным является определение целей УА ИТКС. Цели УА ИТКС определяют направления деятельности организации для обеспечения того, чтобы активы ИТКС могли выполнить предъявляемые к ним требования, следуют из целей организации и должны учитывать требования соответствующих заинтересованных сторон, а также другие финансовые, технические, нормативные, законодательные и организационные требования. Согласно ГОСТ Р 55.0.00, эти цели могут быть определены как количественно (например, готовность производственных мощностей или количественные критерии приемлемости риска), так и качественно (например, ощущение социальной ответственности, репутация или нравственные ценности) и должны регулярно пересматриваться.

Для двух разных групп процессов, относящихся к активам ИТКС (процессы идентификации активов, относящиеся к базовым процессам управления их уязвимостями, и процессы, относящиеся к этапам жизненного цикла активов), то цели УА ИТКС будут отличаться:

- цель УА ИТКС в отношении процессов идентификации активов ИТКС: обеспечение необходимого качества реализации этих процессов в контексте достижения требуемого уровня ОИБ и ОФУ ИТКС в условиях воздействия КА;
- цель УА ИТКС в отношении процессов этапов жизненного цикла активов ИТКС: обеспечение необходимого качества реализации этих процессов в контексте достижения требуемого функционала ИТКС.

Указанные цели достигаются путем реализации ***процессов управления активами*** (ПУА) ИТКС, которые представляют собой совокупность согласованных действий, направленных на процессы идентификации активов ИТКС, или на процессы этапов жизненного цикла активов ИТКС на стадиях планирования, реализации, контроля и совершенствования этих процессов.

Общей методологической базой формирования и реализации ПУА ИТКС является процессный подход и использование циклической модели PDCA[25].

Примером может быть формулировка типового ПУА ИТКС: организационное и документационное сопровождение планирования, реализации, контроля и совершенствования конкретного процесса идентификации (или процесса, этапа жизненного цикла) актива ИТКС.

Согласно ГОСТ Р 55.0.00, ПУА ИТКС включает в себя следующие действия:

- согласование целей УА ИТКС и стратегического плана УА (СПУА) ИТКС с целями и стратегическим планом организации;
- определение необходимых активов ИТКС (формирование портфеля активов ИТКС), их функций и производительности для достижения целей;
- выбор методов, критериев и подходов для эффективного УА ИТКС с последующей разработкой процессов;
- идентификация и оценка рисков, связанных с активами ИТКС (только при формировании первого перечня активов);
- выработка и принятие оптимальных инвестиционных решений на этапах жизненного цикла активов ИТКС;
- планирование деятельности на всех этапах жизненного цикла активов ИТКС;
- мониторинг, измерение, анализ и оценка достигнутых результатов;
- выработка решений по улучшениям.

На основе анализа многочисленных зарубежных публикаций на тему управления ИТ-активами (например, [17, 18]) обобщенно определим два ключевых процесса, отличающихся от представленных в рассмотренных стандартах и конкретизирующих те из них, которые связаны с ОИБ:

1) ***управление учетностью активов*** (англ. *accountability management*), что включает в себя, например, следующие подпроцессы:
   - обнаружение (англ. *discovery*) активов вручную или автоматизировано (с использованием агентов, установленных на подключенных к ИТКС устройствах, или без использования агентов посредством сканирования диапазона IP-адресов, чему может помешать МЭ или политика безопасности);
   - периодически проводимая на систематической основе инвентаризация (англ. *inventory operations*) с фиксацией названия актива, серийного номера, модели, локации и т.п.;
   - осуществление порядка поставок активов (англ. *supply discipline*), их размещения в необходимых локациях и определение ответственных за них;
   - управление поставщиками (англ. *vendor management*), что важно, например, при замене или ремонте части активов;
   - аудит БД активов (англ. *asset database audit*), содержащей записи обо всех активах в области применения управления ИТ-активами, на регулярной основе;
2) ***управление операциями с активами*** (англ. *asset operations management*), что включает в себя следующие подпроцессы:
   - управление ИТ-операциями (англ. *IT operations management*) с активами на протяжении их жизненного цикла;
   - управление лицензиями на ПО (англ. *software license management*);
   - управление на основе «службы поддержки» (англ. *service desk*);
   - техническое управление (англ. *technical management*) для диагностики и решения технических проблем за пределами полномочий «службы поддержки».

5. Система управления активами ИТКС

Для руководства, координации и контроля всей деятельности организации по управлению всеми ее активами предназначена соответствующая ***система управления активами*** (СУА) (англ. *asset management system*). Определим СУА ИТКС как совокупность взаимосвязанных и взаимодействующих элементов организации для разработки политики УА (ПолУА) ИТКС и целей УА ИТКС и процессов, необходимых для достижения этих целей. СУА ИТКС обеспечивает структурированный подход к разработке, координации и управлению всей деятельностью по УА ИТКС на всех этапах жизненного цикла активов ИТКС, а также для согласования этой деятельности с основной деятельностью организации. Такая система призвана способствовать долгосрочному и устойчивому подходу к принятию решений в области обеспечение функционала ИТКС, ОИБ и ОФУ ИТКС организации. СУА ИТКС может способствовать более полному пониманию активов, их производительности, рисков, связанных с УА ИТКС, требуемых инвестиций и ценности активов ИТКС, что важно в качестве исходных данных для принятия решений и стратегического планирования организации.

Для результативного и эффективного функционирования СУА ИТКС организации необходимо решить следующие задачи:

25 Циклическая модель улучшения процессов Шухарта-Деминга, или цикл, PDCA: от англ. Plan-Do-Check-Act – «планируй – выполняй – проверяй –действуй».

- определить, документально оформить и поддерживать в актуальном состоянии организационную структуру и состав ее элементов, отразив подчиненность руководства СУА ИТКС и их основные функции;
- определить состав процессов СУА ИТКС и документально оформить схему их взаимодействия;
- определить состав и разработать процедуры, включая документированные, с учетом требований, применяемых организацией стандартов на системы управления и потребностей самой организации.

Согласно ГОСТ Р 55.0.0Х и ГОСТ Р 55235.Х, помимо соответствующей деятельности СУА, включает в себя все необходимые политики, планы, процессы, средства и ресурсы, которые интегрируются для обеспечения гарантии, что деятельность по УА будет осуществлена. Структура и состав элементов СУА ИТКС определяются ее предназначением и целями УА ИТКС, организационной структурой, используемыми ресурсами и процессами, которые реализуются при УА ИТКС для достижения основных бизнес-целей организации.

СУА ИТКС должна быть обязательно интегрирована в структуру общего управления и управления рисками, включая управление рисками ИБ, организации (рис. 1).

Рис. 1. Взаимоотношение между управлением организацией и УА, СУА и портфелем активов ИТКС

Область применения (действия) СУА ИТКС предполагает определение ее границы (рамки) и объема использования и должна быть задокументирована. Такая область следует из СПУА ИТКС и ПолУА ИТКС и согласована с этими документами. Область применения СУА ИТКС необходимо определять для того, чтобы все значимые с точки зрения ОИБ активы ИТКС были приняты в расчет, а исключения некоторых активов из этой области должным образом обоснованы.

При определении области применения СУА ИТКС организация должна учитывать следующее:

- внешние и внутренние обстоятельства (контекст организации), включая, например, масштабы, компоновку и функциональные связи активов, участвующих в предоставлении сервиса клиентам или другим заинтересованным сторонам, а также структурные части организации, местоположение активов ИТКС и договорные условия;
- требования заинтересованных сторон в отношении УА ИТКС;
- взаимодействие с другими системами управления (при их использовании);
- портфель активов ИТКС (англ. *asset portfolio*) – активы ИТКС, включенные в область применения СУА ИТКС. СУА ИТКС может охватывать множество портфелей активов ИТКС. Портфели для физических активов могут быть отнесены к различным категориям (например, завод, оборудование, инструменты). Портфели ПО могут определяться по разработчику или по платформе (например, персональный компьютер, сервер, мэйнфрейм).

Схема планирования и внедрения элементов СУА ИТКС представлена на рис. 2, на котором показано важное значение этих двух процессов, обеспечивающих взаимодействие верхних и нижних уровней СУА ИТКС.

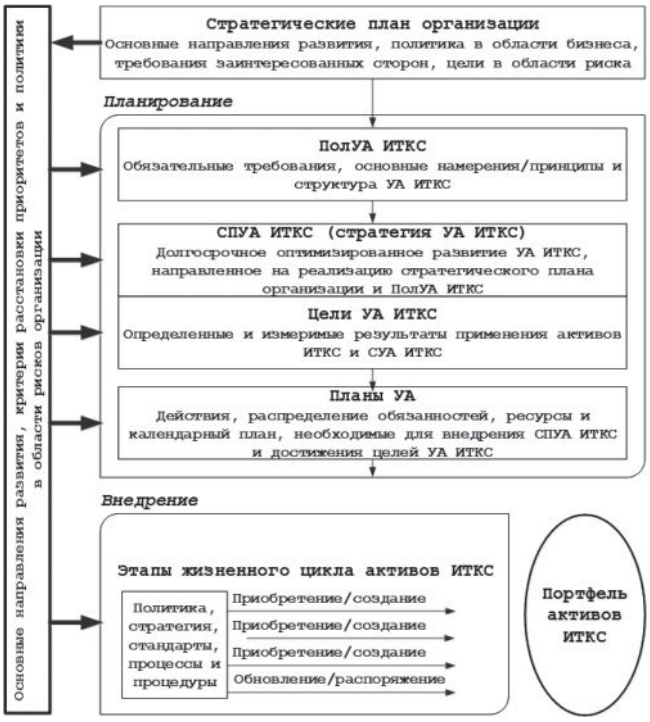


Рис. 2. Схема планирования и внедрения элементов СУА ИТКС

Долгосрочный оптимизированный ***стратегический план УА (СПУА) ИТКС организации***, иначе стратегия УА ИТКС, детализирует цели УА ИТКС, объясняет

их связь с целями организации и концептуальной моделью, необходимой для достижения целей УА ИТКС. Оптимизация распространяется на три составляющие: требуемые вмешательства (затраты, доходы, риск, план-график действий с активами), жизненный цикл актива ИТКС (затраты, производительность, риск, устойчивое развитие) с индивидуальными для отдельных активов планами по полному жизненному циклу и для интеграции систем активов с устойчивым повышением производительности и эффективности, а также программы действий (затраты, доходы, риск, план-график).

Стратегический план организации и СПУА ИТКС, используемые для долгосрочного планирования, должны быть связаны и согласованы, и созданы в рамках итеративного процесса. Цели организации разрабатываются согласно деятельности организации по УА ИТКС, а исходными данными для установления реалистичных и достижимых целей организации могут быть свойства активов ИТКС (например, их мощность и производительность) и результаты деятельности по УА ИТКС (например, планы УА).

СПУА ИТКС на верхнем уровне управления делает следующее:

- преобразует цели организации в цели УА ИТКС;
- идентифицирует и определяет процессы, которые организация использует для установления критериев принятия решений, связанных с активами ИТКС;
- предоставляет руководящие указания для разработки планов УА, в которых указываются действия на уровне активов ИТКС.

Планы УА ИТКС организации формулируют задачи, обеспечивающие выполнение каждой цели УА ИТКС, и содержат обоснование предполагаемых мероприятий по УА ИТКС, включая сами мероприятия, и описание целей, для достижения которых они предназначены, планы эксплуатации, технического обслуживания, капитальных инвестиций (капитальный ремонт, реконструкция, замена, модернизация и списание), а также финансовый и ресурсный планы.

Помимо прочего, СПУА ИТКС должен включать в себя принятую стратегию внедрения ПолУА ИТКС.

Политика УА (ПолУА) ИТКС – это краткое заявление с изложением принципов, с помощью которых организация намерена применять УА ИТКС для достижения своих целей. ПолУА ИТКС выражает общие намерения высшего руководства в отношении активов ИТКС, СУА ИТКС и всей деятельности по УА ИТКС и не относится к конкретным экземплярам активов. ПолУА ИТКС соответствует предназначению организации, согласована с ее целями, разрабатывается на основе стратегического плана организации, действует на высшем уровне и соответствует другим политикам организации, таким как корпоративная политика, политика управления безопасностью труда и охраной здоровья, политика управления качеством, политика управления рисками и политика финансового управления и отчетности. Эта политика устанавливается и утверждается высшим руководством для демонстрирования его заинтересованности и ответственного отношения к УА ИТКС в поддержку достижения целей организации. Кроме этого, ПолУА ИТКС должна включать положение о соответствии законодательным, обязательным и иным требованиям, предъявляемым к организации и принимаемым ею.

ПолУА ИТКС разрабатывается с учетом классификации активов ИТКС. Она содержит обязательства организации и ее ожидания в отношении постоянного улучшения активов ИТКС, УА ИТКС и СУА ИТКС.

Необходимо отметить, что результаты идентификации активов в контексте ОИБ должны быть отражены в Политике ОИБ ИТКС, а результаты идентификации активов в контексте ОФУ – в Стратегии готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса организации, в состав которой входит ИТКС.

6. Краткая инструкция по реализации процесса управления активами ИТКС

Обобщим вышеизложенное применительно к ПУА ИТКС организации в виде следующей краткой пошаговой инструкции, включающей в себя двадцать ключевых мероприятий.

1. Составьте перечень всех активов ИТКС (название, серийный номер, модель, локация...) вручную и автоматизировано.
2. Распределите активы ИТКС по категориям в зависимости от типа (компьютеры/серверы/сетевое оборудование/хранилище/ПО...) и местоположения (офис1/офис2/центр обработки данных...).
3. Определите подразделения, ответственные за каждый актив ИТКС, и их владельцев.
4. Проанализируйте жизненный цикл каждого актива ИТКС (история использования, производительности, технического обслуживания и ожидаемый срок службы).
5. Выполните оценку рисков ИБ для каждого актива ИТКС (уязвимость, угрозы ИБ, потенциальные последствия отказа активов, соответствие нормативным требованиям, выбор подходящих мер ОИБ и обеспечение функциональной устойчивости).
6. Подготовьте финансовый анализ активов ИТКС (стоимость приобретения, амортизация (износ), затраты на техническое обслуживание и т.п, в итоге получив общую стоимость каждого актива).

7. Создайте ПолУА ИТКС с руководящими принципами, ограничениями и ответственностью (должное использование, злоупотребления, НСД и т.п.).
8. Утвердите ПолУА ИТКС.
9. Отслеживайте и записывайте изменения в активах ИТКС (история состояний, изменений и техобслуживания, включая модернизацию, ремонт или перемещение).
10. Регулярно проводите аудит активов ИТКС (с предварительной самооценкой), чтобы идентифицировать любые пропавшие, поврежденные или несанкционированные активы и предпринять необходимые действия для устранения выявленных несоответствий.
11. Регулярно готовьте отчеты по активам ИТКС для обобщения ключевых показателей и информации по активам, включая их состояние, финансовый анализ, статистику использования и результаты оценки рисков ИБ.
12. Выработайте рекомендации по оптимизации активов ИТКС для максимизации их ценности и обеспечения их соответствия целям организации (за счет повышения эффективности и общей окупаемости инвестиций в активы и сокращения времени их простоя).
13. Утвердите рекомендации по оптимизации активов ИТКС.
14. Внедрите утвержденные стратегии оптимизации активов ИТКС и проводите мониторинг их внедрения.
15. Выведите из эксплуатации, замените или модернизируйте устаревшие активы ИТКС.
16. Удалите (сотрите, уничтожьте, переработайте) вышедшие из эксплуатации активы ИТКС защищенным образом.
17. Регулярно пересматривайте и обновляйте ПолУА ИТКС, чтобы соответствовать развивающимся и возникающим технологиям, мерам ОИБ и потребностям организации.
18. Утвердите обновленную ПолУА ИТКС.
19. Обучайте политикам, руководящим принципам и передовой практике УА ИТКС сотрудников организации, что снизит риски и повысит соответствие требованиям и общую эффективность УА ИТКС.
20. Создайте систему, позволяющую сотрудникам немедленно сообщать о проблемах с активами ИТКС (по электронной почте или иным образом).

Выводы

На основе специально подобранной нормативной базы в статье вводится понятийная база УА ИТКС и систематизируются подходы к УА ИТКС организаций как обязательному этапу управления их уязвимостями с целью последующего исключения возможности эксплуатации (использования) обнаруженных уязвимостей. Выделяются мероприятия, реализуемые в ходе процесса УА ИТКС, и обсуждается состав СУА ИТКС, ориентированный на минимизацию возможности осуществления КА на ИТКС организация. Кратко рассматриваются важные составляющие СУА ИТКС, а именно ее основные документы – СПУА ИТКС, планы УА нижнего уровня и ПолУА ИТКС, предназначенные для достижения целей УА ИТКС.

На основе проведенного исследования с соблюдением принципа разумной достаточности разработаны рекомендации по реализации процесса УА ИТКС организации, в виде краткой пошаговой инструкции, состоящей из двадцати основных мероприятий. Эта инструкция имеет непосредственную практическую значимость для управления сетевой безопасностью ИТКС при решении задач устранения найденных для активов ИТКС уязвимостей, что, в свою очередь, приведет к минимизации возможностей реализации КА на ИТКС организаций, использующих конкретные уязвимости активов.

В заключении можно сделать вывод, что чем более качественно разработаны и спланированы все подпроцессы в рамках УА ИТКС организации и чем более своевременно и грамотно они внедрены и пересматриваются с целью совершенствования в течение жизненного цикла всех активов ИТКС, тем более высок уровень зрелости организации и ее готовность к эффективному управлению сетевой безопасностью ИТКС, включающему в себя такие процессы, как управление рисками ИБ, управление инцидентами ИБ, управление уязвимостями, изменениями, управление конфигурациями, управление непрерывностью бизнеса и киберустойчивостью ИТКС [19-20], поддерживающей его.

Литература

1. *Чичков С. Н. Безопасность информационно-телекоммуникационных сетей // Сборник научных статей 7-й Международной молодежной научной конференции. 2019. Т. 4. С. 279–282.*
2. *Савченко М. Ю. Способы совершения преступлений в сфере компьютерной информации и меры их профилактики // Вестник Краснодарского университета МВД России. 2024. № 2 (62). С. 24–27.*
3. *Григорян Д. К., Кондратенко Е. Н. Характерные особенности современных информационных войн политической направленности // Государственное и муниципальное управление. Ученые записки. 2024. № 2,. С.178–183. DOI: 10.22394/2079-1690-2024-1-2-178-183.*
4. *Беседина В. Актуальные киберугрозы: III квартал 2024 года. 5 ноября 2024 г. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/ (дата обращения: 30.12.2024).*

5. *Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. 2022. № 2 (38). С. 131–135.*
6. *Башарин А. Атаки на цепочки поставок: какие существуют риски и как от них защититься. 18 сентября 2023. [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/Supply-Chain-Attack (дата обращения: 30.12.2024).*
7. *Шерстяных А. С. Фишинг как инструмент социальной инженерии // Материалы XXV международной научно-практической конференции «Актуальные проблемы борьбы с преступность: вопросы теории и практики». В 2-х частях. Часть 2. Красноярск, 2022. С. 299–301. DOI: 10.51980/978-5-7889-0334-7_2022_5_2_299*
8. *Баянов Э. И. Новые модификации программ-шифровальщиков // Материалы XVIII Всероссийской студенческой научно-практической конференции «Первые шаги в науку третьего тысячелетия». Уфа, 2022 С. 98–100.*
9. *Таков А. З. Проблемы обеспечения кибербезопасности в современных цифровых системах // Пробелы в российском законодательстве. Т. 16, № 5, 2023. С. 232–236.*
10. *Милославская Н. Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. М.: Горячая линия – Телеком, 2021. – 432 с.*
11. *Серова Т. С., Филимонцев Д. А. Терминология в выражении структуры и функций дефиниций ключевых понятий в подъязыке сферы информационной безопасности // Вестник ПНИПУ. Проблемы языкознания и педагогики. № 3, 2021. С. 8–23. DOI: 10.15593/2224-9389/2021.3.1*
12. *Ушаков Д. Н. Большой толковый словарь русского языка. М., Стандарт, 2021. 816 с.*
13. *Толстой А. И. Системотехника обеспечения безопасности объектов и информационной сфере // Вопросы кибербезопасности. 2024. № 5 (63). С. 47–57. DOI: 10.21681/2311-3456-2024-5-47-57.*
14. *Пушкин С. Как определить ценность использования актива // МСФО на практике. № 6, 2014. [Электронный ресурс]. – Режим доступа: https://msfo-practice.ru/341197 (дата обращения: 30.12.2024).*
15. *Alkhard A. Leveraging Digital Asset Management and Meta-Data Integration for Enhanced Asset Management // Construction Economics and Building, Vol. 24, No. 3 July 2024. Pp. 76–94. DOI: 10.5130/ajceb.v24i3.8741*
16. *Rijadi S. C. R., Suakanto S. Development of an Information System for Asset Management // JURNAL INOVTEK POLBENG – SERI INFORMATIKA, VOL. 9, No. 2, 2024. Pp. 940–952.*
17. *Будзко В. И., Мельников Д. А., Фомичёв В. М. Основы организации обеспечения информационной безопасности и киберустойчивости в централизованных информационно-телекоммуникационных системах высокой доступности // Радиотехника. 2023. Т. 87, № 2. С. 157–162. DOI: 10.18127/j20729472-201901-08*
18. *Канзюба Е. Д. Обеспечение информационной безопасности и киберустойчивости телекоммуникационных сетей, автоматизированных систем управления // Материалы VI Международной молодежной научно-практической конференции в рамках Десятилетия науки и технологий в Российской Федерации «ЭНЕРГОСТАРТ». Кемерово, 2023. С.405-1 – 405-4.*

INFORMATION AND TELECOMMUNICATION NETWORK ASSET MANAGEMENT AS A MANDATORY STAGE OF THEIR VULNERABILITIES MANAGEMENT

Miloslavskaya N. G.[26], Tolstoy A. I.[27]

Keywords: *information and telecommunication network, asset management, asset management process, asset management system, asset vulnerability management, network security management.*

Purpose of work: *systematization of approaches to organizations' information and telecommunication networks (ITCN) asset management (AM) as a mandatory stage of managing their vulnerabilities for the subsequent elimination of the possibility of exploitation (usage) of identified vulnerabilities within the framework of ITCN network security management and development of brief instructions for the implementation of the ITCN AM process.*

Research methods: *analysis of relevant regulatory documents and scientific publications, conceptual modeling, expert assessment, synthesis of an integrated approach to asset management within the framework of network security management.*

Results obtained: *the article introduces the conceptual framework of the ITCN management system and, based on a specially selected regulatory framework, systematizes approaches to the organization's ITCN AM as a mandatory stage of managing their vulnerabilities with the aim of subsequently eliminating these vulnerabilities. The activities implemented during the ITCN AM process, especially when identifying ITCN assets, are highlighted and the composition of the ITCN AM system (AMS) is discussed, aimed at minimizing the possibility of computer attacks against the organization's ITCN. The main documents of the ITCN AMS are briefly considered, namely the strategic plan of the ITCN AMS, lower-level AM plans and the ITCN AM policy, designed to achieve the goals of the ITCN AM. Based on the research conducted, in compliance*

26 Natalia G. Miloslavskaya, Dr.Sc., Ph.D in Cybersecurity, Associate Professor, Professor of Dep. of Information Security of Banking Systems of National Research Nuclear University MEPhI, Moscow, Russia. E-mail: NGMiloslavskaya@mephi.ru
27 Alexander I. Tolstoy, Ph.D, Associate Professor, Head of Dep. of Information Security of Banking Systems of National Research Nuclear University MEPhI, Moscow, Russia. E-mail: AITolstoj@mephi.ru

with the principle of reasonable sufficiency, a brief step-by-step instruction for implementing the ITCN AM process has been developed.

Practical significance *consists in developing brief instructions for implementing the ITCN AM process, especially the process of identifying ITCN assets, within the framework of ITCN network security management when solving the problems of eliminating vulnerabilities found for ITCN assets, which, in turn, will lead to minimizing the possibilities of implementing computer attacks against the organizations' ITCN.*

References

1. *Chichkov S. N. Bezopasnost' informatsionno-telekommunikatsionnykh setey // Sbornik nauchnykh statey 7-y Mezhdunarodnoy molodezhnoy nauchnoy konferentsii. T. 4, 2019. S. 279–282.*
2. *Savchenko M. YU. Sposoby sovershenstva prestupleniy v sfere komp'yuternoy informatsii i mery ikh profilaktiki // Vestnik Krasnodarskogo universiteta MVD Rossii. № 2(62), 2024. S. 24–27.*
3. *Grigoryan D. K., Kondratenko Ye. N. Kharakternyye osobennosti sovremennykh informatsionnykh voyn politicheskoy napravlennosti // Gosudarstvennoye i munitsipal'noye upravleniye. Uchenyye zapiski. № 2, 2024. S178-183. DOI: 10.22394/2079-1690-2024-1-2-178-183*
4. *Besedina V. Aktual'nyye kiberugrozy: III kvartal 2024 goda. 5 noyabrya 2024 g. [Elektronnyy resurs]. – Rezhim dostupa: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/ (data obrashcheniya: 30.12.2024).*
5. *Yangayeva M. O., Pavlenko N. O. OSINT. Polucheniye kriminalisticheski znachimoy informatsii iz seti Internet // Altayskiy yuridicheskiy vestnik. № 2(3), 2022. S. 131–135.*
6. *Basharin A. Ataki na tsepochki postavok: kakiye sushchestvuyut riski i kak ot nikh zashchitit'sya. 18 sentyabrya 2023. [Elektronnyy resurs]. – Rezhim dostupa: https://www.anti-malware.ru/analytics/Threats_Analysis/Supply-Chain-Attack (data obrashcheniya: 30.12.2024).*
7. *Sherstyanykh A. S. Fishing kak instrument sotsial'noy inzhenerii // Materialy XKHV mezhdunarodnoy nauchno-prakticheskoy konferentsii «Aktual'nyye problemy bor'by s prestupnost': voprosy teorii i praktiki». V 2-kh chastyakh. Chast' 2. Krasnoyarsk, 2022. S. 299–301. DOI: 10.51980/978-5-7889-0334-7_2022_5_2_299*
8. *Bayanov E. I. Novyye modifikatsii programm-shifroval'shchikov // Materialy XVIII Vserossiyskoy studencheskoy nauchno-prakticheskoy konferentsii «Pervyye shagi v nauku tret'yego tysyacheletiya». Ufa, 2022 S. 98–100.*
9. *Takov A. Z. Problemy obespecheniya kiberbezopasnosti v sovremennykh tsifrovykh sistemakh // Probely v rossiyskom zakonodatel'stve. T. 16, № 5, 2023. S. 232–236.*
10. *Miloslavskaya N. G. Nauchnyye osnovy postroyeniya tsentrov upravleniya setevoy bezopasnost'yu v informatsionno-telekommunikatsionnykh setyakh. M.: Goryachaya liniya – Telekom, 2021. – 432 s.*
11. *Serova T. S., Filimontsev D. A. Terminologiya v vyrazhenii struktury i funktsiy definitsiy klyuchevykh ponyatiy v pod"yazyke sfery informatsionnoy bezopasnosti // Vestnik PNIPU. Problemy yazykoznaniya i pedagogiki. № 3, 2021. S. 8-23. DOI: 10.15593/2224-9389/2021.3.1*
12. *Ushakov D. N. Bol'shoy tolkovyy slovar' russkogo yazyka. M., Standart, 2021. 816 s.*
13. *Tolstoy A. I. Sistemotekhnika obespecheniya bezopasnosti ob"yektov i informatsionnoy sfere // Voprosy kiberbezopasnosti. № 5(63), 2024. S. 47–57. DOI: 10.21681/2311-3456-2024-5-47-57.*
14. *Pushkin S. Kak opredelit' tsennost' ispol'zovaniya aktiva // MSFO na praktike. № 6, 2014. [Elektronnyy resurs]. – Rezhim dostupa: https://msfo-practice.ru/341197 (data obrashcheniya: 30.12.2024).*
15. *Alkhard A. Leveraging Digital Asset Management and Meta-Data Integration for Enhanced Asset Management // Construction Economics and Building, Vol. 24, No. 3 July 2024. Pp. 76-94.*
16. *Rijadi S.C.R., Suakanto S. Development of an Information System for Asset Management // JURNAL INOVTEK POLBENG – SERI INFORMATIKA, VOL. 9, No. 2, 2024. Pp. 940–952.*
17. *Budzko V. I., Mel'nikov D. A., Fomichov V. M. Osnovy organizatsii obespecheniya informatsionnoy bezopasnosti i kiberustoychivosti v tsentralizovannykh informatsionno-telekommunikatsionnykh sistemakh vysokoy dostupnosti // Radiotekhnika. 2023. T. 87, № 2. S. 157–162. DOI: 10.18127/j20729472-201901-08*
18. *Kanzyuba Ye. D. Obespecheniye informatsionnoy bezopasnosti i kiberustoychivosti telekommunikatsionnykh setey, avtomatizirovannykh sistem upravleniya // Materialy VI Mezhdunarodnoy molodezhnoy nauchno-prakticheskoy konferentsii v ramkakh Desyatiletiya nauki i tekhnologiy v Rossiyskoy Federatsii «ENERGOSTART». Kemerovo, 2023. S. 405-1 – 405-4.*

МОДЕЛЬ СЛОЖНОГО ИНФОРМАЦИОННОГО КОНФЛИКТА ДЛЯ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

Головской В. А.[1]

DOI: 10.21681/2311-3456-2025-1-86-95

Цель работы: *формализация модели сложного информационного конфликта и конструктивное доказательство повышения информативности модели такого конфликта, усовершенствованной путем включения в нее индифферентного информационного взаимодействия.*

Методы исследования: *общенаучные методы – абстрагирование, обобщение, анализ и методы теории алгоритмов и теории информации.*

Результат исследования: *формализована известная модель сложного информационного конфликта информационно-технических систем, осуществлено её качественное усовершенствование для условий функционирования робототехнических комплексов. Предложено измерять информативность формализованных моделей непосредственно, а не косвенно – через моделирование влияния используемых моделей на качество функционирования системы. С привлечением абстракций отождествления и потенциальной осуществимости, традиционных для теоретико-алгоритмических построений, обоснован подход к использованию колмогоровской сложности для количественного оценивания качественного усовершенствования рассматриваемой модели сложного информационного конфликта. Получены аналитические выражения, позволяющие, оценивать информативность предложенных моделей.*

Практическая ценность: *представленные результаты обеспечивают возможность решения задач оценивания достаточности средств защиты информации и выбора конфликтно-устойчивого состояния радиосистемы, а также расширяют спектр методов, используемых при исследованиях информационных конфликтов.*

Ключевые слова: *антагонистический конфликт, информационное взаимодействие, количество информации, радиоэлектронный конфликт, колмогоровская сложность.*

Введение

В работе исследуется информационный конфликт как условие функционирования радиосистемы робототехнического комплекса, рассматриваемого экспертами[2] как средство повышения эффективности вооруженного противоборства, становящегося все более сложным и динамичным [1, 2].

Под РТК далее понимается информационно-техническая система (ИТС), включающая в себя [3] группу робототехнических средств (РТС), радиосистему передачи данных (РС), сопряженную с подсистемой защиты информации (ЗИ) РТК, а также пункт управления.

РТС обладают рядом ограничений [3, 4], наследуемых их подсистемами. Такими ограничениями являются массогабаритные характеристики и емкость источников питания, что накладывает, в свою очередь, ограничения на время автономной работы, вычислительные возможности подсистем и т.д. Одной из подсистем РТК, наиболее зависимой от ограничений и в то же время функционирующей в условиях конфликта со средой, является его РС. Полагаем, что РС РТК обеспечивает [3] передачу по радиоканалам разнородных данных как между РТС и пунктом управления, так и между РТК и коалиционными системами, т.е. объединенными в условную «коалицию» согласованностью своих целей функционирования с целями надсистемы [3].

Развитие теории и практики информационного противоборства [1, 5, 6] обуславливает как ужесточение требований к конфликтной устойчивости РС РТК [3, 6] и защищенности циркулирующей в радиоканалах этих РС информации, так и актуальность исследований по обеспечению указанных требований в условиях информационного конфликта (ИК).

Для обеспечения защищенности передаваемой по радиоканалам РС информации могут применяться криптографические или некриптографические средства, обладающие специфическими особенностями [7]. В работе [8] сформулирована актуальная проблема оценивания достаточности средств ЗИ и показана необходимость использования формальной модели ИК для разрешения соответствующей алгоритмической проблемы. Однако подходящая для этой цели модель ИК в настоящее время отсутствует [8].

Одним из способов обеспечения конфликтной устойчивости РС в условиях реализуемой антагонистической стороной ИК активной электромагнитной

1 Головской Василий Андреевич, кандидат технических наук, доцент, Краснодарское высшее военное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: golovskoy_va@mail.ru

2 Science & Technology Trends 2023-2043. NATO Science & Technology Organization. Volume 1: Overview. https://cesmar.it/wp-content/uploads/2023/04/stt23-vol1.pdf

деятельности при наличии ряда критичных ограничений, характерных для РТК, является повышение информированности подсистемы управления ресурсами [9] об условиях среды функционирования. Исследователями рассматриваются два основных направления повышения информированности: экстенсивное, характеризующееся всеобъемлющей интеграцией коалиционных ИТС [5], и интенсивное, заключающееся в повышении информативности моделей и эффективности их использующих алгоритмов управления ресурсами [4, 5, 9], например, когнитивного управления [5]. В русле второго направления совершенствование моделей осуществляется за счет введения в них новых сущностей или связей [3, 10]. Такое совершенствование призвано обеспечить более полное описание явлений объективной реальности, что объясняет увеличение количества информации, содержащейся в модели. При предложенной выше дихотомии сделано естественное предположение, что увеличение количества информации, поступающей на вход ИТС, улучшает качество функционирования указанной системы, понимаемое в широком смысле и далее в работе подлежащее пояснению. Однако в доступных автору источниках отсутствуют подходы к количественному оцениванию информативности моделей ИК.

Предлагаемая статья, являясь развитием работ [3, 11], посвящена построению формальной модели ИК, которая при наполнении ее конкретными данными будет являться непосредственно входом для соответствующих алгоритмов, и оцениванию информативности различных описаний ИК.

1. Постановка задачи

Рассмотрим в качестве условий функционирования РС РТК содержание информационного и радиоэлектронного конфликтов. Известна [10, 12] вложенность последнего в ИК, под которым понимается [13] «процесс столкновения ИТС на этапе сбора и обработки данных о состоянии, намерениях и действиях противостоящей стороны, каждая из которых стремится упреждающему принятию управленческих решений по отношению к противостоящей стороне и предпринимает определенные действия по снижению возможностей противостоящих средств сбора и обработки данных». Вследствие указанной вложенности понятий «информационное взаимодействие» (ИВ) является более широким [3, 14], чем используемый термин «радиоэлектронное взаимодействие». Далее для построения формальной модели ИК при описании взаимодействий ИТС будет использоваться термин ИВ, учитывающий вложенность в него «радиоэлектронного взаимодействия».

По типам возникающих между сторонами конфликта ИВ выделяют [15] коалиционный и антагонистический ИК. Антагонистический ИК определяют [6, 11] как «процесс ИВ сторон ИК, имеющих противоположные цели и стремящихся достигнуть несовместимых состояний». Указанные цели ИТС раскрываются при информационном анализе радиоэлектронной борьбы [16], осуществляемой с целью «обеспечения доступа к электромагнитному спектру своим пользователям и осложнения/запрещения доступа пользователям противоположной стороны ИК» [16]. Коалиционный ИК объясняется нарушением электромагнитной совместимости[3] РС с системами, отнесенными к коалиции.

Исследования ИК ИТС – предмет множества работ, в которых ИК рассматривается, как правило, с позиций антагонистического ИК [1, 2], либо с позиций коалиционного [18], и как исключение рассматриваются оба типа ИВ [15]. Анализу подходов к исследованию ИК посвящен подробный обзор[4], а формализации их моделей – работы [17, 19], в которых, как и в подавляющем большинстве рассмотренных работ, акцент делается на антагонистическом ИК.

В монографии[5] предложена описательная модель сложного ИК (СИК), отличающаяся одновременным учетом антагонистического и коалиционного типов конфликтных ИВ ИТС с объектом взаимодействия, однако данная модель не была формализована. В работе [3] предложено расширение указанной модели СИК, заключающееся во введении в рассмотрение еще одного типа ИВ, в дополнение к антагонистическому и коалиционному, существенного для исследуемой проблемы обеспечения конфликтной устойчивости РС РТК, – индифферентного ИВ. Указанное расширение при этом обосновывалось индуктивно, и конструктивного доказательства его достоинств дано не было. В монографии [17] индифферентный тип ИВ выведен из рассмотрения ввиду декларируемой практической возможности его устранения. В докладе [11] показана согласованность расширения [3] известной модели СИК с графовой моделью [9] когнитивной РС (КРС) и с методологией обучения с подкреплением, рассматриваемой в качестве приоритетной при создании КРС [9], а также представлены предложения по использованию алгоритмического подхода к количественному оцениванию эффективности указанного качественного

3 Козирацкий Ю. Л., Иванцов А. В., Мамаджанян Е. А. Метод оперативной оценки радиоэлектронной обстановки в интересах обеспечения скрытности и электромагнитной совместимости радиоэлектронных средств // Журнал Сибирского федерального университета. Серия: Техника и технологии. 2018. № 3. С. 256–262.

4 Макаренко С. И., Михайлов Р. Л. Информационные конфликты – анализ работ и методологии исследования // Системы управления, связи и безопасности. 2016. № 3. С. 95–178.

5 Астапенко Ю. А. и др. Конфликтно-устойчивые радиоэлектронные системы. Методы анализа и синтеза / Под ред. С. В. Ягольникова. – М.: Радиотехника, 2015. 312 с.

усовершенствования модели СИК. Однако в [11] не представлен способ описания ИК, а формализация ограничена только описанием рассматриваемых типов ИВ.

Необходимо отметить, что формализация необходима не только для устранения известной семантической неполноты вербальных моделей. Формализованная модель, при наполнении её конкретными данными, способна служить источником информации непосредственно для подсистем управления [9], а также – для разработчиков как конфликтно-устойчивых ИТС в целом [15], так и их подсистем ЗИ [8]. Так, например, система обучения с подкреплением способна сформировать модель среды, однако неверные посылки, получаемые от подсистемы логического вывода, могут привести к неточной модели или к более трудному нахождению оптимального решения. В работе [9] была предложена модель подсистемы управления КРС, использующая логический вывод для получения знаний о среде, необходимых для обеспечения конфликтной устойчивости КРС. Также предлагалось [9] формировать знания на основе информации, заложенной в подсистему и поступающей при функционировании управляемой системы, при этом были показаны [9] подходы к использованию информации о ИК для формирования решения о выборе конфликтно-устойчивого состояния. Однако в работах [3, 9] было приведено достаточно общее содержание требуемых данных о среде и ИК, что было частично устранено при попытке построения формальной модели ИК [11] и использовании ее в качестве входа для алгоритма прогнозирования.

С учетом приведенных аргументов повышение качества, указанное в сформулированном выше предположении, может быть интерпретировано как повышение эффективности расходования ресурсов при вычислении решения задачи, или же – повышение точности этого решения. Примером описываемого явления может служить различающаяся эффективность алгоритма на разных входах, что наблюдается у алгоритмов поиска элемента массива на несортированных и сортированных входных данных.

2. Основная часть

Несмотря на декларируемую экспертами [6] невозможность построения законченной теории ИК, практика, обусловленная развитием средств информационного противоборства, требует как уточнения моделей, так и расширения условий их применимости. Следует отметить, что указанное требование совершенствования моделей характерно для всех сфер деятельности, использующих моделирование [20]. При совершенствовании модели необходимо соблюдение баланса между требуемыми от нее низкой сложностью и высокой адекватностью [11]. Тогда цель совершенствования модели может быть сформулирована как увеличение количества информации, получаемой субъектом моделирования в результате применения модели [11], либо как нахождение более короткой записи модели при той же её информативности для пользователя[6]. Необходимым является определение условий и правил использования модели, от которых будет зависеть выделение из среды объекта исследования, которым в настоящей работе является функционирование РС РТК в условиях ИК. Предмет исследования – информационные взаимодействия, возникающие при ИК с участием РС РТК.

Рассмотрим содержание ИК и место в нем РС РТК. Разделяемым ресурсом является радиочастотный спектр в рассматриваемой области пространства, с использованием которого осуществляется ИВ между сторонами ИК [3, 5]. Информация о состоянии спектра необходима для формирования модели среды и прогнозирования ИК, обеспечивающих решение задачи выбора конфликтно-устойчивого состояния КРС [9], а также – для выбора средств ЗИ в радиоканалах [8]. С учетом этих аргументов модель ИК с участием РС РТК формализована с использованием методологической схемы, описываемой кортежем[7]

$$M = \langle ES, SM, T, IM, L \rangle, \quad (1)$$

где: ES – радиочастотный диапазон электромагнитного спектра в области функционирования РС, представляющий собой объект-оригинал; SM – субъект моделирования, которым в зависимости от дальнейшего предназначения модели может быть подсистема управления ресурсами РС РТК или же система поддержки принятия решений конструктора системы ЗИ; T – цель моделирования, которая с учетом изложенного выше может быть сформулирована как обеспечение информацией субъекта моделирования; IM – инфраструктура моделирования, предоставляемая мастер-системой, выделенной на структурном уровне [9] из КРС РТК или указанной выше системой поддержки принятия решений; L – язык описания отношения объект-модель, обеспечивающий отображение ES в его конечное описание

$$L{:}ES \longrightarrow code(ES),$$

который и является определяющим информативность модели ИК элементом.

Очевидным примером L для получения описания $code(ES)$ являются алгоритмы, реализуемые в современных средствах спектрального анализа. Описание ES на их выходе будет конечным, однако

6 Верещагин Н. К., Успенский В. А., Шень А. Колмогоровская сложность и алгоритмическая случайность. – М.: МЦНМО, 2013. 576 с.

7 Волкова В. Н., Козлов В. Н., Магер В. Е., Черненькая Л. В. Классификация методов и моделей в системном анализе // Сборник докладов XX Международной конференции по мягким вычислениям и измерениям. – СПб.: СПбГЭТУ(ЛЭТИ). 2017. – С. 223–226.

не обеспечит достижение цели T, т.к. отражает текущее состояние ES, однако не обладает достаточной для прогнозирования ИК информативностью о природе конфликтных ИВ [20].

При моделировании ИК и оценивании характеристик его сторон используются различные подходы [9], отличающиеся, в том числе, требуемыми наборами исходных данных о его сторонах и, соответственно, принятыми уровнями абстракции. Однако участие в ИК перспективных ИТС, в том числе интеллектуальных [1], ограничивает возможность применения многих из указанных подходов ввиду отсутствия достаточно полных описаний предполагаемых конструктивных решений и методов управления ресурсами. В этой ситуации представляется адекватным применение теоретико-алгоритмического подхода, зарекомендовавшего себя эффективным при исследованиях гипотетических систем [9, 21], представленных описаниями нетривиальных семантических свойств их реализующих алгоритмов. С учетом привлеченных абстракций и известной алгоритмической природы составляющих антагонистического ИК [1, 12] представляется целесообразным использовать традиционные для теории алгоритмов обозначения: $code(X) \in \sum^*$ – слово определенной структуры конечной длины в алфавите $\sum$, кодирующее объект X; $A_D^C(x,y) = z$ – алгоритм, выполняющий задачу D в интересах стороны ИК C, останавливается на входе с результатом z.

Опишем условия, отличающие СИК от традиционно рассматриваемых дуэльных ситуаций и проблемы электромагнитной совместимости. При моделировании СИК предложено [15] рассматривать одновременно два типа конфликтных ИВ: антагонистическое и коалиционное (рис. 1). Известно [12], что реализация активного антагонистического ИВ одной стороной ИК в отношении элемента другой может быть осуществлена только на основании результатов успешно проведенных радиомониторинга и идентификации последнего, что согласуется и с известными моделями кибератак [22]. Будем далее в качестве допущения рассматривать только такой подход к организации ИВ антагонистической стороной ИК.

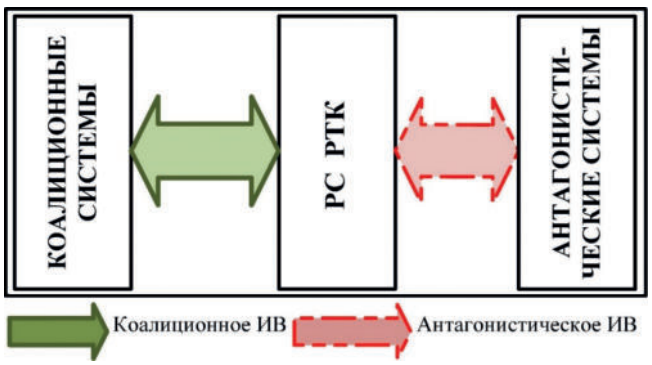


Рис. 1. Информационные взаимодействия при ИК

С учетом современных взглядов на информационное противоборство [5, 12, 16], принятых абстракций и допущений реализация антагонистического ИВ может быть представлена последовательностью событий, которым поставлены в соответствие следующие высказывания:

$$S_{RM}^A \Leftrightarrow \exists\, A_{RM}^A : A_{RM}^A(code(ES)) = D_{RM}; \quad (2)$$

где S_{RM}^A – обнаружение антагонистической стороной ИК факта функционирования РС РТК, описываемого набором данных D_{RM} о РС, в результате радиомониторинга, реализуемого соответствующим алгоритмом A_{RM}^A

$$S_{Id}^A \Leftrightarrow \exists\, A_{Id}^A : A_{Id}^A(D_{Apr}^A, D_{RM}) = D_{Id}, \quad (3)$$

где S_{Id}^A – успешная идентификация антагонистической стороной ИК режима работы РС, реализуемая алгоритмом A_{Id}^A; D_{Apr}^A – априорные данные, позволяющие антагонистической стороне вычислить идентификационные данные D_{Id} РС;

$$S_D^A \Leftrightarrow \exists\, A_D^A : A_D^A(D_{Apr}^A, D_{Id}) = ES_d^A, \quad (4)$$

где S_D^A – реализация целевого активного ИВ алгоритмом A_D^A в отношении выявленных в результате идентификации ресурсов РС; ES_d – состояние ES, при котором к нему осложнен/запрещен доступ пользователям противоположной стороны ИК. Далее для состояний ES будут использоваться записи ES_d^A или ES_d^C, обозначающие, что ES перешел в них результате антагонистического ИВ или коалиционного ИВ соответственно.

Для формализации антагонистического ИВ с учетом теории и практики информационного противоборства [5, 12, 16] сформируем высказывание

$$\mathrm{K}_A \Leftrightarrow S_D^A \vee S_{Id}^A, \quad (5)$$

т.е. считаем, что антагонистическое ИВ имеет место (K_A), только если антагонистическая сторона осуществила радиомониторинг и/или радиоподавление КРС. Тогда последовательность событий (2)–(4) может быть адекватно описана композицией формирующих эти события алгоритмов

$$A_D^A(A_{Id}^A(A_{RM}^A(code(ES)))) = ES_d^A.$$

При построении условия (5) умышленно не было учтено ИВ, обусловленное влиянием работы телекоммуникационных систем антагонистической стороны ИК, что будет сделано и пояснено ниже.

Коалиционные ИВ с учетом трех основных типов задач, решаемых коалицией, могут быть описаны при помощи трех высказываний. Влияние коалиционных ИВ на ES ввиду функционирования телекоммуникационных систем, управляемых алгоритмом A_{TM}^C, формализуемо следующим высказыванием:

$$S_{TM}^C \Leftrightarrow \exists\, A_{TM}^C : A_{TM}^C(D_{Apr}^C, code(ES)) = ES_d^C. \quad (6)$$

Получение данных о состоянии ES и о носителях средств радиомониторинга (D_I) алгоритмом $A_I^C(D_{Apr}^C, code(ES))$, а также реализация алгоритмом A_D^C активного ИВ описываются соответствующими высказываниями

$$S_I^C \Longleftrightarrow \exists\, A_I^C : A_I^C\,(D_{Apr}^C, code(ES)) = D_I, D_{RM},$$
$$S_D^C \Longleftrightarrow \exists\, A_D^C : A_D^C\,(D_{Apr}^C, code(ES)) = ES_d^C.$$

Высказывание о существовании коалиционного ИВ (K_C) может быть формализовано следующим условием, поскольку для рассматриваемого ИК играют роль только события, соответствующие высказываниям S_{TM}^C и S_D^C:

$$\mathrm{K}_C \Longleftrightarrow S_{TM}^C \vee S_D^C. \qquad (7)$$

Далее предполагается, что $S_d^C \neq S_d^A$ и $code(ES_d^C) \neq code(ES_d^A)$, однако $A_D^C\,(D_{Apr}^C, code(ES_d^A)) = ES_d^{C,A}$, $A_D^A\,(D_{Apr}^A, code(ES_d^C)) = ES_d^{A,C}$ и $ES_d^{A,C} \approx ES_d^{C,A}$, но $code(ES_d^{A,C}) = code(ES_d^{C,A})$. С учетом этого предположения и принятых абстракций сформулируем критерий отнесения ИК к сложному согласно [15]

$$\Omega_{\mathrm{K}} \Longleftrightarrow \mathrm{K}_C \wedge \mathrm{K}_A. \qquad (8)$$

Рассмотрим содержание усовершенствования модели СИК, реализованного путем введения в рассмотрение индифферентного ИВ [3]. Данный тип ИВ обуславливает ИК, заключающийся в нарушении электромагнитной совместимости РС РТК с техническими системами, не относящимися ни к коалиционным, ни к антагонистическим [3]. Предложено [3] называть такой конфликт индифферентным, а технические системы, участвующие в индифферентном ИК с системами РС РТК, – индифферентными. Такими индифферентными системами могут быть работающие в активном режиме [3, 11] радиорелейные и радиолокационные станции, средства подвижной радиосвязи, земных станций спутниковой связи, радиовещательных станций, а также телекоммуникационные системы антагонистической стороны ИК, если они не осуществляют целевого воздействия на РС РТК.

С учетом рассмотренных условий функционирования РТК предложено [3] выделить следующие объекты ИВ с РС РТК (рис. 2):

- антагонистические системы (информационного противоборства);
- коалиционные системы;
- индифферентные системы и часть среды функционирования РТК, оказывающая влияние на распространение радиоволн.

Выделение лишь части среды в качестве объекта ИВ объясняется влиянием условий распространения радиоволн на характеристики ИК [9] и соответствует известным положениям онтологии проектирования[8].

8 Боргест Н. М. Научный базис онтологии проектирования // Онтология проектирования. 2013. № 1(7). С. 7–25.

При этом актуализируется [11] вопрос о целесообразности введения новой сущности в модель (8), т.е. о нахождении баланса между её сложностью и адекватностью с учетом того, что индифферентное ИВ вносит наименьший вклад в формируемый ИК по сравнению с другими ИВ. Отметим, что необходимость выделения индифферентного ИВ обусловлена тем, что оно может быть самостоятельно описано после соответствующего наблюдения и выявления регламента работы индифферентных систем или получения их технического описания, в то время как антагонистическое ИВ является достаточно непредсказуемым и может изменяться как по причине следования тактике и её развития, так и по причине наращивания интеллектуальных способностей систем информационного противоборства [1, 5].

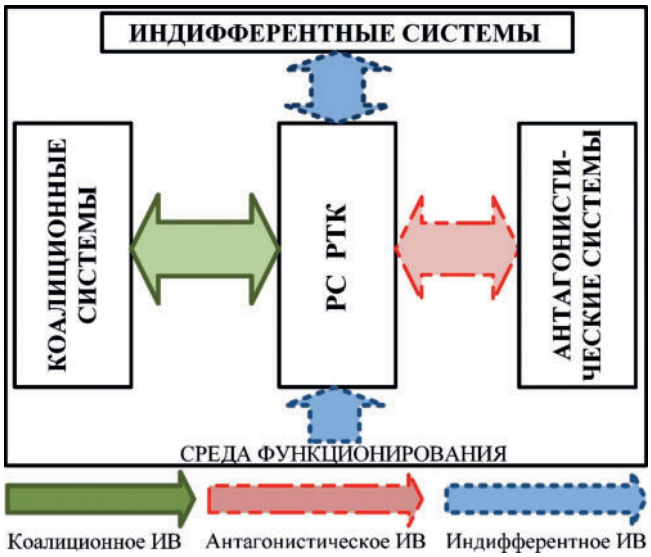


Рис. 2. Информационные взаимодействия при сложном ИК

С учетом приведенного обоснования природы индифферентного ИВ его влияние может быть описано по аналогии с (2)-(4) при помощи высказывания

$$S_{TM}^I \Longleftrightarrow \exists\, A_{TM}^I : A_{TM}^I\,(code(ES)) = ES_d^I.$$

Высказывание о существовании индифферентного ИК (K_I) формализуем условием

$$\mathrm{K}_I \Longleftrightarrow S_{TM}^I. \qquad (9)$$

С учетом введенного индифферентного ИВ по аналогии с (8) сформулируем высказывание об условиях отнесения ИК к сложному

$$\Omega_{\mathrm{K}+} \Longleftrightarrow \mathrm{K}_C \wedge \mathrm{K}_A \wedge \mathrm{K}_I, \qquad (10)$$

приняв допущения, что $ES_d^I \neq ES_d^C \neq ES_d^A$ и $code(ES_d^I) \neq code(ES_d^C) \neq code(ES_d^A)$, однако $A_{TM}^I(D_{Apr}^C, code(ES_d^{C,A})) = ES_d^{I,C,A}$, $A_D^I(D_{Apr}^A, code(ES_d^{A,C})) = ES_d^{I,A,C}$ и $ES_d^{I,A,C} \approx ES_d^{I,C,A} \approx \ldots \approx ES_d^{C,A,I}$, но $code(ES_d^{I,A,C}) = code(ES_d^{I,C,A}) = code(ES_d^{C,A,I})$.

Иллюстрация формирования ИК с учетом принятых допущений осуществлена с использованием аппарата теории графов (рис. 3), выбранного по причине обеспечения наглядности, а также адекватности для моделирования ИК [10] и изучения причинно-следственных связей [23], необходимых для описания процесса.

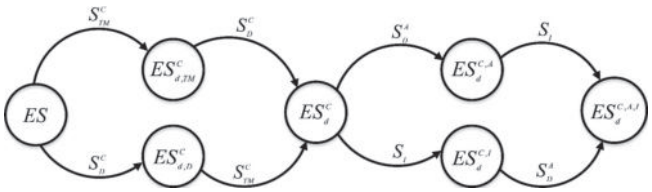


Рис. 3. Модель возникновения ИК

Разделяемый ресурс (ES) в результате воздействия одной из составляющих коалиционного ИК (7) может перейти из бесконфликтного состояния ES в одно из состояний $ES^C_{d,TM}$ или $ES^C_{d,D}$, обусловленных соответствующими ИВ S^C_{TM} или S^C_D, что иллюстрируют помеченные дуги. Дальнейший переход в новое состояние ES^C_d, описываемое условием (7), из состояний $ES^C_{d,TM}$ или $ES^C_{d,D}$ может быть инициирован рассмотренными уже ИВ S^C_D или ES^C_{TM}, соответственно. Формирование СИК согласно модели (8) отражает переход между состояниями ES^C_d и $ES^{C,A}_d$ по причине антагонистического ИВ S^A_D, а индифферентное ИВ S_I обуславливает формирование СИК согласно (10) из $ES^{C,A}_d$. Также состояние $ES^{C,A,I}_d$ может быть получено из ES^C_d по причинам ИВ S^A_D и S_I, обусловившего состояние $ES^{C,I}_d$.

Далее необходимо построить конструктивные объекты из рассмотренных выше описательных моделей ИК, которые могут быть непосредственно использованы IM в вычислениях для достижения T.

Известную описательную модель СИК (рис. 1), сущность которой отражает сформированное условие (8), предлагается формализовать с помощью отображения

$$L_{\text{K}} : ES \longrightarrow code(ES^{A,C}_d), \qquad (11)$$

где $code(ES^{A,C}_d)$ – описание СИК через состояние ES_d, обусловленное влиянием учитываемых типов ИВ. Т.к. $code(ES^{A,C}_d)$ будет использоваться согласно T, представляется целесообразным потребовать раздельного описания различных составляющих СИК, т.е.

$$code(ES^{A,C}_d) = W_A, W_C, \qquad (12)$$

где W_A и W_C – слова, кодирующие данные об антагонистическом (5) и коалиционном (7) ИК, соответственно.

Выделение из общего описания ES двух слов, кодирующих каждый соответствующий тип конфликтного ИВ, обосновано целью моделирования T. Содержание и структура слов W_A и W_C определяются характеристиками потребителя информации – SM из (1). Например, для подсистемы управления ресурсами КРС, использующей логический вывод [9], словом целесообразно кодировать совокупность термов, каждый из которых есть высказывание об эмиссии, потенциальной или реализуемой одной из сторон ИК. При описании антагонистического ИВ для построения W_A с учетом (2) и (5) используются также термы – высказывания о рецепторах, способных своими алгоритмами реализовывать этапы (2) и (3) ИК. Такое содержание слов обеспечит подсистему управления ресурсами КРС информацией о природе существующих конфликтных ИВ, что позволит ей прогнозировать ИК [9]. При использовании же модели (12) для решения задачи о достаточности средств ЗИ, обеспечивающих конфиденциальность передаваемой по радиоканалу информации [8], слово W_A должно содержать термы, кодирующие данные о возможностях средств радиомониторинга и анализа его результатов. Далее для сохранения общности изложения абстрагируемся от конкретного содержания слов, кодирующих типы ИВ, и методов их получения.

С учетом введенного понятия индифферентного ИВ и (11) предлагается СИК описывать с помощью отображения

$$L_{\text{K+}} : ES \longrightarrow code(ES^{A,C,I}_d),$$
$$code(ES^{A,C,I}_d) = W_A, W_C, W_I, \qquad (13)$$

где W_I – слово, кодирующее данные об индифферентном ИВ.

Оценим информативность двух формализованных выше моделей СИК с привлечением методов теории информации. Для оценивания информативности описаний систем применяют алгоритмический, комбинаторный или вероятностный подходы [11]. С учетом цели работы и отсутствия вероятностного описания ИК, необходимого для вычисления энтропии Шеннона [16], оценивание информативности представляется адекватным только с алгоритмических позиций Колмогорова [11, 24].

В докладе [11] предложен подход к оцениванию информативности моделей ИК с использованием колмогоровской сложности как меры содержащейся в них информации. Колмогоровская сложность является эффективным инструментом для оценивания информативности описаний [24], т.к. является числовой характеристикой сложности описываемого объекта.

Алгоритмический подход ставит в соответствие количеству информации в слове x конечной длины простую колмогоровскую сложность (KS) этого слова [24], определяемую как длина самого короткого описания y слова x

$$KS^{\Gamma}(x) = \min\{l(y) | \Gamma(y) = x\},$$

где Γ – способ получения описания y слова x, представленный вычислимой функцией $\Gamma(y)$, определенной на множестве слов $\{0,1\}^+$; $l(y)$ – длина слова y при фиксированном Γ. В качестве x обычно рассматривается конечный объект, вследствие чего область значений функции $\Gamma(y)$ определена природой описываемого объекта. Задание $\Gamma(y) = x$ традиционно [24] предполагает наличие вычислимого кодирования.

Примем стандартное [24] допущение, что значения $\Gamma(y)$ вычисляются соответствующим алгоритмом A_Γ, останавливающимся на заданном входе.

После пояснений содержания описаний $code(ES_d^{A,C})$ и $code(ES_d^{A,C,I})$ предлагается оценить ожидаемое повышение информативности модели СИК после введения в рассмотрение индифферентного ИВ.

Известны следующие соотношения, описывающие сложность описания отдельных слов и их наборов [11]:

$$KS(x_1,x_2) \le KS(x_1) + KS(x_2) + O(log_2 N),$$
$$KS(x_1,x_2,x_3) \le KS(x_1) + KS(x_2) + KS(x_3) + O(log_2 N),$$

где x_i, $i = \overline{1,3}$ – слова длины не больше N; $O(log_2 N)$ – сложность выбранного способа описания Γ. Тогда при использовании модели (12) сложности описаний ES_d, использующих единое, цельное описание радиоэлектронной обстановки и раздельное её описание через учитываемые типы ИВ, оцениваются выражением

$$KS(W_K) \le KS(W_A) + KS(W_C) + O(log_2 N), \qquad (14)$$

а для модели СИК (13)

$$KS(W_{K+}) \le KS(W_A) + KS(W_C) + KS(W_I) + O(log_2 N), \qquad (15)$$

где $W_K = code(ES_d^{A,C})$ и $W_{K+} = code(ES_d^{A,C,I})$ – описания СИК согласно принятым моделям при допущении, что слова W_A, W_C, и W_I имеют длину не больше N.

С учетом содержания (14), (15) и того, что $code(ES_d^{A,C})$ и $code(ES_d^{A,C,I})$ являются разными описаниями объекта ES_d, справедливо

$$KS(W_A) + KS(W_C) + O(log_2 N) <$$
$$< KS(W_A) + KS(W_C) + KS(W_I) + O(log_2 N), \qquad (16)$$

откуда следует, что разница в информативности моделей имеет значение

$$\Delta = KS(W_{K+}) - KS(W_K) = KS(W_I),$$

т.е. введение в рассмотрение еще одного типа ИВ обеспечивает повышение информативности на $KS(W_I)$ битов при переходе от модели (12) к модели (13) .

Вычисление колмогоровской сложности до этого осуществлялось при допущении независимости составляющих ИК между собой, т.е.

$$I(W_A{:}W_C) \approx I(W_C{:}W_I) \approx 0,$$

где $I(W_A{:}W_C)$ – количество информации в слове W_A о слове W_C, вычисляемое как

$$I(W_A{:}W_C) = KS(W_C) - KS(W_C/W_A), \qquad (17)$$

где $KS(W_C/W_A)$ – условная сложность описания W_C при известном описании W_A, равная длине кратчайшего описания W_C.

При учете взаимных зависимостей K_A и K_C, что соответствует современным взглядам на ИК [16] с участием технологически развитых противников, получим по аналогии с (17) следующие соотношения:

$$I(W_C{:}W_A) = KS(W_A) - KS(W_A/W_C),$$
$$I(W_C{:}W_I) = KS(W_I) - KS(W_I/W_C),$$
$$I(W_A{:}W_I) = KS(W_I) - KS(W_I/W_A).$$

Последние выражения призваны описать взаимное влияние ИВ разных типов. Например, запись $I(W_C{:}W_A)$ обозначает, что ИТС коалиции учитывают при формировании коалиционного ИВ особенности антагонистического ИВ и имеют одну из целей – адекватно реагировать на антагонистическое ИВ, которое, в свою очередь, обусловлено задачей эффективно действовать против коалиционного ИВ, что описывает величина $I(W_A{:}W_C)$. Величины же $I(W_C{:}W_I)$ и $I(W_A{:}W_I)$ характеризуют реакции коалиции и антагонистической стороны на индифферентное ИВ соответственно.

Тогда от выражений (14) и (15) перейдем к соответствующим формулам

$$KS(W_K) = I(W_C{:}W_A) + I(W_A{:}W_C),$$
$$KS(W_{K+}) = I(W_C{:}W_A) + I(W_A{:}W_C) +$$
$$+ I(W_C{:}W_I) + I(W_A{:}W_I).$$

Из последних выражений по аналогии с (16) получим разницу в информативности моделей

$$\Delta = KS(W_{K+}) - KS(W_K) = I(W_C{:}W_I) + I(W_A{:}W_I).$$

Выражения для вычисления Δ при различных допущениях о взаимном влиянии типов ИВ позволяют оценить повышение информативности описаний СИК при введении индифферентного ИВ в модель. Повышение информативности модели за счет введения в рассмотрение нового типа ИВ может быть объяснено такой аналогией, как увеличение количества информации об объекте анализа при увеличении числа сторон его рассмотрения, позволяющем учесть большее количество причинно-следственных связей.

Конкретное содержание алгоритма кодирования для получения слов W_A, W_C и W_I определяется архитектурой системы-потребителя информации, целями и правилами её функционирования, и выходит за рамки рассмотрения настоящей статьи.

Необходимо отметить, что для системы поддержки принятия решений по оцениванию достаточности средств ЗИ достаточно будет модели, в то время как для более эффективного управления ресурсами КРС

необходима конечная модель $W_К = code(ES_d^{A,C})$, которая ввиду необходимости учета взаимного влияния ИВ разных типов не может быть построена в реальном времени.

Выводы

Представленные результаты имеют как практическую значимость для исследования вопросов выбора средств ЗИ и построения конфликтно-устойчивых КРС РТК, так и теоретическую – могут быть полезны при исследовании ИК. Представленная модель СИК изначально предназначена для использования в продукционных системах [9], но может применяться и для других ИТС, функционирующих в условиях ИК. Усовершенствованная модель СИК обладает такими важными качествами, как адекватность, простота, проблемная ориентация, гибкость. Предложенный подход к оцениванию потенциальной информативной емкости моделей расширяет сферы применения теоретико-информационных методов. Развитие исследований будет посвящено доказательству необходимости и достаточности содержания модели ИК для выбора средств ЗИ в радиоканале РС РТК.

Литература

1. *Sharma P., Sarma K. K., Mastorakis N. E. Artificial Intelligence Aided Electronic Warfare Systems – Recent Trends and Evolving Applications // IEEE Access. 2020. vol. 8, pp. 224761–224780. DOI: 10.1109/ACCESS.2020.3044453.*
2. *Стародубцев Ю. И., Липатников В. А., Парфиров В. А. Проблема повышения разведывательной защищенности элементов военной системы связи // Военная мысль. 2023. № 7. С. 88–99.*
3. *Головской В. А., Чернуха Ю. В., Семенюк Д. Б. Формализация задачи построения системы передачи данных робототехнического комплекса, функционирующего в условиях антагонистической киберэлектромагнитной деятельности // Вопросы кибербезопасности. 2019. № 6(34). С. 113–122. DOI: 10.21681/2311-3456-2019-6-113-122.*
4. *Куракин А. С. Оценка эффективности функционирования группы беспилотных летательных аппаратов при выполнении задач аэрофотосъемки // Проблемы информационной безопасности. Компьютерные системы. 2024. № 1(58). С. 62–69. DOI: 10.48612/jisp/fpf1-59d2-x8t1.*
5. *Борисов В. И., Вилков С. В. Технологическая платформа развития систем управления, связи и радиоэлектронной борьбы // Теория и техника радиосвязи. 2023. № 1. С. 5–11.*
6. *Ельцов О. Н., Крутских П. П., Радзиевский В. Г. Конфликтная устойчивость роботизированных систем. – М.: Радиотехника, 2023. 350 с.*
7. *Махов Д. С. Анализ некриптографических методов защиты информации в радиоканалах информационных систем // Вопросы кибербезопасности. 2024. № 1(59). С. 82–88. DOI: 10.21681/2311-3456-2024-1-82-88.*
8. *Буторин Н. А., Головской В. А. Массовая проблема оценивания достаточности мер защиты информации // Прикладная математика: современные проблемы математики, информатики и моделирования: Материалы VI Всероссийской научно-практической конференции, Краснодар, 2024. – С. 169–173.*
9. *Головской В. А. Операционная модель когнитивной радиосистемы робототехнического комплекса // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18. № 5. С. 12–20. DOI: 10.36724/2072-8735-2024-18-5-12-20.*
10. *Козлитин С. Н., Козирацкий Ю. Л., Будников С. А. Моделирование совместного применения средств радиоэлектронной борьбы и огневого поражения в интересах повышения эффективности борьбы за превосходство в управлении // Системы управления, связи и безопасности. 2020. № 1. С. 49–73. DOI: 10.24411/2410-9916-2020-00001.*
11. *Головской В. А. Расширение модели сложного радиоэлектронного конфликта // Радиолокация, навигация, связь: сборник трудов XXX Международной научно-технической конференции (г. Воронеж, 16–18 апреля 2024 г.), т. 5. С. 63–68.*
12. *Сахнин А. А. Комплексная оценка радиоэлектронной защищенности военных систем связи. – М.: Радиотехника. 2022. 309 с.*
13. *Михайлов Р. Л. Динамическая модель информационного конфликта информационно-телекоммуникационных систем специального назначения // Системы управления, связи и безопасности. 2020. № 3. С. 238–251. DOI: 10.24411/2410-9916-2020-10309.*
14. *Андреев Г. И., Замарин М. Е., Созинов П. А., Тихомиров В. А. Концептуальная модель информационного взаимодействия радиоэлектронных средств // Радиотехника. 2021. Т. 85. № 12. С. 31–41. DOI: 10.18127/j00338486-202112-02.*
15. *Власов В. В., Шевчук В. И., Шевчук Д. В., Ягольников С. В. Метод синтеза космической системы дистанционного зондирования Земли в условиях сложного информационного конфликта // Нейрокомпьютеры: разработка, применение. 2022. Т. 24. № 2. С. 30–34.*
16. *Созинов П. А., Андреев Г. И., Тихомиров В. А., Замарин М. Е. Совместность производства энтропии с мерой оценки эффективности систем информационного обеспечения в радиоэлектронной борьбе // Радиотехника. 2023. Т. 87. № 5. С. 9–23. DOI: 10.18127/j00338486-202305-02.*
17. *Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. – СПб.: Наукоемкие технологии, 2020. 337 с.*
18. *Антипин Б. М., Виноградов Е. М. Характеристики и параметры РЭС СПС, необходимые для анализа ЭМС в полосах совместного использования: аналитический обзор // Труды учебных заведений связи. 2020. Т. 6. № 2. С. 6–18. DOI: 10.31854/1813-324X-2020-6-2-6-18.*
19. *Михайлов Р. Л., Данилов Д. Ю., Потапов А. А., Гречко П. В. Динамическая координация подсистем наблюдения и воздействия: метод прогнозирования взаимодействий // Системы управления, связи и безопасности. 2024. № 3. С. 49–77. DOI: 10.24412/2410-9916-2024-3-049-077*
20. *Антипова С. А., Воробьев А.А. Целенаправленная трансформация математических моделей на основе стратегической рефлексии // Компьютерные исследования и моделирование. 2019. Т. 11. № 5. С. 815–831. DOI: 10.20537/2076-7633-2019-11-5-815-831.*
21. *Alfonseca M., Cebrian M., Anta A. F., Coviello L., Abeliuk A., Rahwan I. Superintelligence cannot be contained: lessons from computability theory // Journal of Artificial Intelligence Research. 2021. No 70. pp. 65–76. DOI: 10.1613/jair.1.12202.*

22. Котенко И. В., Хмыров С. С. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак // Вопросы кибербезопасности. 2022. № 4(50). 52–79. DOI: 10.21681/2311-3456-2022-4-52-79.
23. Грушо А. А., Грушо Н. А., Забежайло М.И., Тимонина Е. Е., Шоргин С. Я. Сложные причинно-следственные связи // Информатика и ее применения. 2023. Т. 17. № 2. С. 84–89. DOI: 10.14357/19922264230212.
24. Верещагин Н. К., Семёнов А. Л., Шень А. Х. Последнее открытие Колмогорова? (Колмогоров и алгоритмическая статистика) // Теория вероятностей и ее применения. 2023. Т. 68. № 4. С. 719–750. DOI: 10.4213/tvp5650.

A MODEL OF COMPLEX INFORMATION CONFLICT FOR ROBOTIC SYSTEMS

Golovskoy V. A.[9]

Keywords: *algorithm, information conflict, information interaction, model, electronic conflict, Kolmogorov complexity, robotic complex.*

The purpose of the work *is to formalize the model of a complex information conflict and to constructively prove the increase in the informativeness of the model of such a conflict, improved by including indifferent information interaction in it.*

Research methods: *general scientific methods – abstraction, generalization, analysis, and methods of the theory of algorithms and information theory.*

The result of the study: *a well-known model of a complex information conflict of information technology systems has been formalized, its qualitative improvement has been carried out for the operating conditions of robotic complexes. It is proposed to measure the informativeness of formalized models directly, rather than indirectly, through modeling the influence of the models used on the quality of the system functioning. Using the abstractions of identification and potential feasibility, which are traditional for theoretical and algorithmic constructions, the approach to using Kolmogorov complexity for quantitative assessment of qualitative improvement of the considered model of complex information conflict is substantiated. Analytical expressions are obtained that allow evaluating the informativeness of the proposed models.*

Practical value: *the presented results provide an opportunity to solve the problems of assessing the sufficiency of information security tools and choosing a conflict-resistant state of the radio system, as well as expand the range of methods used in the study of information conflicts.*

References

1. Sharma P., Sarma K. K., Mastorakis N. E. Artificial Intelligence Aided Electronic Warfare Systems – Recent Trends and Evolving Applications // IEEE Access, 2020. vol. 8, pp. 224761–224780. DOI: 10.1109/ACCESS.2020.3044453.
2. Starodubcev Yu. I., Lipatnikov V. A., Parfirov V. A. Problema povysheniya razvedyvatel'noj zashchishchennosti elementov voennoj sistemy svyazi // Voennaya mysl', 2023. No 7. pp. 88–99.
3. Golovskoy V. A., Chernuha Yu. V., Semenyuk D. B. Formalizaciya zadachi postroeniya sistemy peredachi dannyh robototekhnicheskogo kompleksa, funkcioniruyushchego v usloviyah antagonisticheskoj kiberelektromagnitnoj deyatel'nosti // Voprosy kiberbezopasnosti [Cybersecurity issues], 2019, No 6 (34), pp. 113–122. DOI: 10.21681/2311-3456-2019-6-113-122.
4. Kurakin A. S. Ocenka effektivnosti funkcionirovaniya gruppy bespilotnyh letatel'nyh apparatov pri vypolnenii zadach aerofotos"emki // Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy [Problems of information security. Computer systems], 2024, No 1(58). pp. 62–69. DOI: 10.48612/jisp/fpf1-59d2-x8t1.
5. Borisov V. I., Vilkov S. V. Tekhnologicheskaya platforma razvitiya sistem upravleniya, svyazi i radioelektronnoj bor'by // Teoriya i tekhnika radiosvyazi, 2023, No 1. pp. 5–11.
6. El'cov O. N., Krutskih P. P., Radzievskij V. G. Konfliktnaya ustojchivost' robotizirovannyh sistem. Moscow: Radiotehnika, 2023. 350 p.
7. Makhov D. S. Analiz nekriptograficheskih metodov zashchity informacii v radiokanalah informacionnyh sistem // Voprosy kiberbezopasnosti [Cybersecurity issues], 2024. No 1(59). pp. 82–88. DOI: 10.21681/2311-3456-2024-1-82-88.
8. Butorin N. A., Golovskoy V. A. Massovaya problema ocenivaniya dostatochnosti mer zashchity informacii // Prikladnaya matematika: sovremennye problemy matematiki, informatiki i modelirovaniya: Materialy VI Vserossijskoj nauchno-prakticheskoj konferencii, Krasnodar, 2024. – pp. 169–173.
9. Golovskoy V. A. Operacionnaya model' kognitivnoj radiosistemy robototekhnicheskogo kompleksa // T-Comm: telekommunikacii i transport [T-Comm], 2024. vol. 18. No 5. pp. 12–20. DOI: 10.36724/2072-8735-2024-18-5-12-20.
10. Kozlitin S. N., Kozirackij Yu. L., Budnikov S. A. Modelirovanie sovmestnogo primeneniya sredstv radioelektronnoj bor'by i ognevogo porazheniya v interesah povysheniya effektivnosti bor'by za prevoskhodstvo v upravlenii // Sistemy upravleniya, svyazi i bezopasnosti [Systems of Control, Communication and Security], 2020. No 1. pp. 49–73. DOI: 10.24411/2410-9916-2020-00001.
11. Golovskoy V. A. Rasshirenie modeli slozhnogo radioelektronnogo konflikta // Radiolokaciya, navigaciya, svyaz': sbornik trudov XXX Mezhdunarodnoj nauchno-tekhnicheskoj konferencii. Voronezh, vol. 5. pp. 63–68.
12. Sakhnin A. A. Kompleksnaya ocenka radioelektronnoj zashchishchennosti voennyh sistem svyazi. – Moscow, Radiotehnika. 2022. 309 p.

9 Vasiliy A. Golovskoy, Ph.D. (in Engineering sciences), Associate Professor, Krasnodar Higher Military School named after army general S. M. Shtemenko, Krasnodar, Russia. E-mail: golovskoy_va@mail.ru

13. *Mikhailov R. L. Dinamicheskaya model' informacionnogo konflikta informacionno-telekommunikacionnyh sistem special'nogo naznacheniya // Sistemy upravleniya, svyazi i bezopasnosti [Systems of Control, Communication and Security], 2020. No 3. pp. 238–251. DOI: 10.24411/2410-9916-2020-10309.*
14. *Andreev G. I., Zamarin M. E., Sozinov P. A., Tikhomirov V. A. Konceptual'naya model' informacionnogo vzaimodejstviya radioelektronnyh sredstv // Radiotehnika [Radioengineering], 2021. vol. 85. No 12. pp. 31–41 DOI: 10.18127/j00338486-202112-02.*
15. *Vlasov V. V., Shevchuk V. I., Shevchuk D. V., Yagol'nikov S. V. Metod sinteza kosmicheskoj sistemy distancionnogo zondirovaniya Zemli v usloviyah slozhnogo informacionnogo konflikta // Nejrokomp'yutery: razrabotka, primenenie [Neurocomputers], 2022. vol. 24. No 2. pp. 30–34.*
16. *Sozinov P. A., Andreev G. I., Tikhomirov V. A., Zamarin M. E. Sovmestnost' proizvodstva entropii s meroj ocenki effektivnosti sistem informacionnogo obespecheniya v radioelektronnoj bor'be // Radiotehnika [Radioengineering], 2023. vol. 87. No 5. pp. 9–23. DOI: 10.18127/j00338486-202305-02.*
17. *Makarenko S. I. Modeli sistemy svyazi v usloviyah prednamerennyh destabiliziruyushchih vozdejstvij i vedeniya razvedki. – SPb.: High Tech Publishing House, 2020, 337 p.*
18. *Antipin B. M, Vinogradov E. M. Harakteristiki i parametry RES SPS, neobhodimye dlya analiza EMS v polosah sovmestnogo ispol'zovaniya: analiticheskij obzor // Trudy uchebnyh zavedenij svyazi [Proceedings of telecommunication universities], 2020. vol. 6. No 2. pp. 6–18. DOI: 10.31854/1813-324X-2020-6-2-6-18.*
19. *Mikhailov R. L., Danilov D. Yu., Potapov A. A., Grechko P. V. Dinamicheskaya koordinaciya podsistem nablyudeniya i vozdejstviya: metod prognozirovaniya vzaimodejstvij // Sistemy upravleniya, svyazi i bezopasnosti [Systems of Control, Communication and Security], 2024. No 3. pp. 49–77. DOI: 10.24412/2410-9916-2024-3-049-077*
20. *Antipova S. A., Vorob'ev A. A. Celenapravlennaya transformaciya matematicheskih modelej na osnove strategicheskoj refleksii // Komp'yuternye issledovaniya i modelirovanie [Computer Research and Modeling], 2019. vol. 11. No 5. pp. 815–831. DOI: 10.20537/2076-7633-2019-11-5-815-831.*
21. *Alfonseca M., Cebrian M., Anta A. F., Coviello L., Abeliuk A., Rahwan I. Superintelligence cannot be contained: lessons from computability theory // Journal of Artificial Intelligence Research, 2021. No 70. pp. 65–76. DOI: 10.1613/jair.1.12202.*
22. *Kotenko I. V., Khmyrov S. S. Analiz modelej i metodik, ispol'zuemyh dlya atribucii narushitelej kiberbezopasnosti pri realizacii celevyh atak // Voprosy kiberbezopasnosti [Cybersecurity issues], 2022. No 4(50). pp. 52–79. DOI: 10.21681/2311-3456-2022-4-52-79.*
23. *Grusho A. A., Grusho N. A., Zabezhajlo M. I., Timonina E. E., Shorgin S. Ya. Slozhnye prichinno-sledstvennye svyazi // Informatika i ee primeneniya [Informatics and applications], 2023. vol. 17. No 2. pp. 84–89. DOI: 10.14357/19922264230212.*
24. *Vereshchagin N. K., Semyonov A. L., SHen' A. H. Poslednee otkrytie Kolmogorova? (Kolmogorov i algoritmicheskaya statistika) // Teoriya veroyatnostej i ee primeneniya [Theory of Probability and its Applications], 2023. vol. 68. No 4. pp. 719–750. DOI: 10.4213/tvp5650.*

ПРИМЕНЕНИЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Часть 6

Калашников А. О.[1], Аникина Е. В.[2], Бугайский К. А.[3], Молотов А. А.[4]

DOI: 10.21681/2311-3456-2025-1-96-107

Цель исследования: *адаптация логико-вероятностного метода оценивания сложных систем к задачам построения систем защиты информации в многоагентной системе.*

Метод исследования: *при проведении исследования использовались основные положения методологии структурного анализа, системного анализа, теории принятия решений, методов оценивания событий при условии неполной информации, логико-вероятностных методов.*

Полученный результат: *данная статья продолжает рассмотрение вопросов информационной безопасности на основе анализа отношений между субъектами и объектом защиты. В рамках разрабатываемой модели дано определение таких понятий как оценка опасности, поверхность атаки, а также сценария сложной системы. Показано, что данные понятия могут быть количественно определены на основе соответствующих оценок состояний отношений агентов. Показана целесообразность внедрения и место специализированных агентов, обеспечивающих управление процессами мониторинга у агентов. Предложены механизмы каскадирования, обеспечивающие единый логико-функциональный подход при определении оценок опасности. Полученные результаты обеспечивают обоснованное вычисление и использования вероятностных характеристик для последующего анализа отношений между субъектами информационной безопасности на основе применения логико-вероятностного метода при анализе указанных отношений.*

Научная новизна: *рассмотрение вопросов защиты информации с использованием аппарата математических и логических отношений. Разработаны методы количественного оценивания опасности деструктивного воздействия без привлечения информации о наличии актуальных или используемых угроз как с точки зрения программного обеспечения, так и с точки зрения логической структуры ИС. Показана эквивалентность между опасностью деструктивного воздействия и текущим состоянием отношений между агентами. Разработан метод определения устойчивости оценки опасного состояния отношений. Показано, что разработанные методы оценки опасности состояний дают возможность для исключения отдельного рассмотрения ошибок первого и второго рода при оценке реальных намерений нарушителя. Разработаны подходы, позволяющие получить интегральные оценки опасности на уровне как отдельных агентов, так и различных подсистем современных информационных систем и систем в целом за счет управления составом агрегируемых оценок состояния отношений агентов.*

Вклад авторов: *Калашников А. О. выполнил постановку задачи и общую разработку модели применения логико-вероятностного метода в информационной безопасности. Бугайский К. А. и Аникина Е. В. участвовали в подготовке всех разделов статьи. Молотов А. А. участвовал в подготовке раздела о проактивном мониторинге.*

Ключевые слова: *модель информационной безопасности, оценка сложных систем, логико-вероятностный метод, теория отношений, системный анализ.*

Введение

Данная статья является шестой из серии публикаций, посвященных исследованию вопроса применения логико-вероятностного метода при изучении вопросов защиты информации. Метод был разработан Рябининым И. А. [1, см. ссылки на соответствующую литературу там же] и приобрел популярность при проведении исследований, в том числе, связанных с анализом и оценкой рисков сложных систем. Прежде всего для решения вопросов оценки надежности работы систем и анализа причин возникновения аварийных ситуаций. Логико-вероятностный метод предполагает решение следующих задач:

1. Построение структурно-логической модели системы за счет выделения и использования событий с несовместными исходами.
2. Проведение преобразований полученных логических уравнений на основе функций булевой алгебры с целью получения системы уравнений с конечным числом переменных.
3, Теоретически обоснованный переход от уравнений булевой алгебры к уравнениям с вероятностными переменными.

К несомненным достоинствам логико-вероятностного метода следует отнести его способность

1 Калашников Андрей Олегович, доктор технических наук, главный научный сотрудник лаборатории «Безопасности сложных систем» ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: aokalash@ipu.ru

2 Аникина Евгения Владимировна, научный сотрудник лаборатории «Безопасности сложных систем» ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: ajanet@ipu.ru

3 Бугайский Константин Алексеевич, младший научный сотрудник лаборатории «Безопасности сложных систем» ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: kabuga@ipu.ru

4 Молотов Александр Анатольевич, инженер-программист Научно-внедренческого отдела 89 ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: alpha.sphere@ya.ru

обеспечить прозрачность процедур анализа и оценки сложных систем, а также хорошие адаптационные способности к новым задачам. Результатом применения логико-вероятностного метода являются количественные оценки риска как вероятности нарушения работоспособности системы. Интерес к логико-вероятностному методу, помимо типичных вопросов надежности систем, в настоящее время подкрепляется исследованием задач машинного обучения и связанных с ними проблем оптимизации расчетов [см., например, 2–5]. В частности, логико-вероятностный метод обеспечивает хорошую точность и стабильность результатов в задачах распознавания тех или иных объектов. Логико-вероятностный метод также находит свое применение и при решении задач защиты информации [см., например, 6–11].

Тем не менее представляется, что логико-вероятностный метод обладает значительно большим, пока не раскрытым, потенциалом в случае его дальнейшего развития и адаптации к решению различных задач в области информационной безопасности (далее – ИБ).

Постановка задачи

Логико-вероятностный метод обладает достаточно обширным набором подходов и решений по работе с логическими функциями, описывающими функционирование сложных систем, какими являются современные информационные системы (далее – ИС). Исследование применимости логико-вероятностного метода для решения задач ИБ базируется на представлении ИС в виде отношений между агентами.

В рамках достижения общей цели исследования возникает задача разработки формально-логических основ для вычисления вероятности наступления возможных деструктивных последствий, возникающих в ходе взаимодействия агентов из состава ИС. Разработка таких оценок на макроуровне – по совокупной реакции вероятностных параметров, характеризующих состояния отношений конкретного агента с другими агентами из состава ИС – выполнена в настоящей статье.

Проактивный мониторинг

В предыдущих статьях цикла [12–16] была показана возможность формирования оценок состояния отношений между агентами как результата обработки событий и сообщений, формируемых информационными ресурсами и потоками каждого агента вследствие внешних воздействий со стороны других агентов, которые определены как респонденты. Такие состояния отношений $\beta R\gamma$ агента с респондентом, определяемые каждым агентом независимо, описываются базовыми характеристиками:

- $rang$ – показатель состояния отношений $\beta R\gamma$ с конкретным респондентом, выражающийся целым числом $\eta = [1,4]$;
- $prob$ – показатель вероятности $p = [0,1]$ нахождения агента с конкретным респондентом в заданном состоянии;
- $undef$ – показатель возможности ошибки $\upsilon = [0,1]$ или «размытости» границы между доводами «за» и «против» при определении состоянии агента.

Значение величины $rang$ получается в результате комплексного оценивания состояний информационных ресурсов и потоков из состава агентов и упорядочивания множества состояний $R = \{Lr,Dr,Ir,Ur\}$ по степени снижения опасности состояния следующим образом: 4 эквивалентно Dr (Нелояльное), 3 – Ir (Неопределенное), 2 – Lr (Лояльное) и 1 – Ur (Безразличное).

В основе определения каждого из возможных состояний агента лежит оценка правдоподобия гипотезы нахождения в том или ином состоянии или уровень доверия к нахождению в определенном состоянии. Таким образом, состояние отношений агент-респондентов определяется характеристиками $prob$ и $undef$, которые в самом общем виде являются отражением неопределенности относительно реальных намерений респондента. Данную неопределенность будем рассматривать с точки зрения возможного развития дальнейших воздействий на агента в наиболее опасном для нарушения конфиденциальности, целостности и доступности направлении.

Трактовка характеристики $undef$ как показателя ошибочности определяется тем, что она зависит от суммы доказательств, снижающих уверенность в результате комплексного оценивания состояния, то есть она показывает, как часто понижалась оценка состояния при комплексном оценивании.

Отметим, что характеристика $undef$ в равной степени влияет на оценку любого состояния, что позволяет рассматривать ее в качестве ошибки как первого, так и второго типа при определении именно реальных намерений респондента.

Для снижения неопределенности в оценке реальных намерений респондента у агента есть два варианта действий:

- ожидать очередного воздействия со стороны респондента;
- получить оценку состояния отношений с данным респондентом со стороны других агентов.

Рассмотрим эти варианты снятия неопределенности с помощью базовой диаграммы, приведенной на рис. 1.

На рис. 1 узлы γ и $\beta 1$, $\beta 2$ представляют респондента и агентов соответственно. Узлы $\rho 1$ и $\rho 2$ соответствуют оценкам отношений агентов с респондентом. Морфизмы $g1$ и $g2$ представляют собой функции воздействия респондента на агентов, а морфизмы

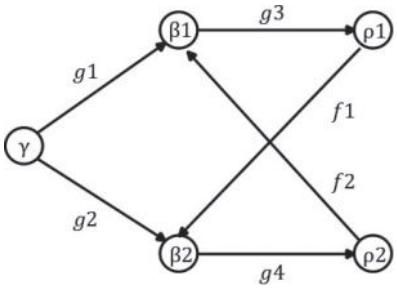


Рис. 1. Базовая диаграмма

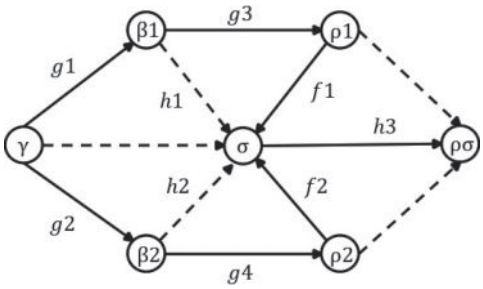


Рис. 2. Модифицированная базовая диаграмма

$g3$ и $g4$ – функции оценки состояния отношений агент – респондент.

Первый вариант фактически является реактивным и не обеспечивает своевременное реагирование на возникающие угрозы, что позволяет исключить его из дальнейшего рассмотрения.

Второй вариант включает морфизмы $f1$ и $f2$ представляющих функции обмена оценками состояния отношений агент-респондент между агентами. Существование данных морфизмов обуславливается наличием этапов разведки и внедрения, а также бокового перемещения нарушителя согласно исследовательским и аналитическим материалам, представленными организациями mitre.org и first.org.

Второй вариант, с одной стороны, обеспечивает возможности для целенаправленного сбора информации о возможных действиях нарушителя, то есть может рассматриваться как проактивный. Но, с другой стороны, необходимо отметить, что базовая диаграмма не является коммутативной в силу невозможности однозначно определить морфизмы $\beta 1 \longrightarrow \beta 2$ и $\rho 1 \longrightarrow \rho 2$.

Некоммутативность базовой диаграммы означает, прежде всего, необходимость наличия у каждого агента практически полной схемы ИС для организации обмена оценками состояний с другими агентами. Такое знание агента является для нарушителя по сути источником достаточно полной и достоверной информации о структуре ИС, что повышает успешность действий при проведении атаки. Кроме того, некоммутативность диаграммы рис. 1 резко увеличивает вычислительную нагрузку на агента, связанную с учетом оценок других агентов.

Построим на основе базовой диаграммы новую, модифицированную диаграмму, как показано на рис. 2.

Модификация базовой диаграммы заключается в ведении дополнительного узла σ и перенаправлении морфизмов f с агентов β на этот узел. На рис. 2 пунктирными линиями обозначены вспомогательные морфизмы, подтверждающие коммутативность модифицированной диаграммы.

Узел $\rho\sigma$ диаграммы может рассматриваться как оценка опасности респондента формируемой узлом σ на основании оценок $\rho 1$ и $\rho 2$, получаемых агентами в процессе их функционирования. Функция оценки опасности респондента, представленная морфизмом $h3$, будет рассмотрена далее в этой статье.

Необходимо обратить внимание на морфизмы $h1$ и $h2$, которые, с одной стороны, подтверждают коммутативность диаграммы рис. 2. Но, с другой стороны, в сочетании с морфизмами $f1$ и $f2$, по сути, не имеют на узле σ адекватной трактовки. Это дает основание продолжить модификацию базовой диаграммы. Для этого введем еще один дополнительный узел δ, на котором замкнем морфизмы $h1$ и $h2$. Это действие не нарушает коммутативности диаграммы рис. 2. Материалы, представленные организациями mitre.org и first.org, показывают, что деятельность нарушителя невозможна без использования в ИС соответствующих каналов управления захваченными агентами со стороны нарушителя. Это дает основание рассматривать морфизмы $h1$ и $h2$ как функции обнаружения таких каналов управления в исходящем трафике агентов $\beta 1$ и $\beta 2$. В итоге проведенной модификации базовой диаграммы получена коммутативная диаграмма оценки опасности респондента, представленная на рис. 3.

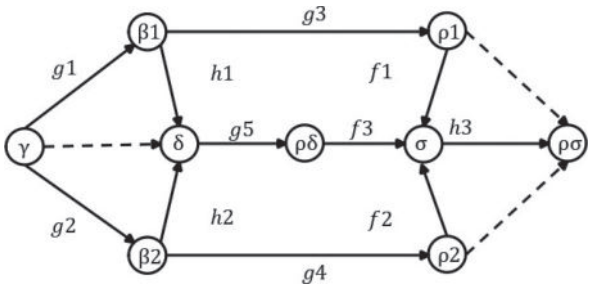


Рис. 3. Диаграмма проактивной оценки респондента

Таким образом, диаграмма на рис. 3 позволяет формировать структуру агентов, обеспечивающих проактивную оценку опасности респондента с точки зрения реальных действий нарушителя. Собственно структура агентов будет рассмотрена в этой статье ниже. На данном этапе отметим только, что для определения оценки опасности респондента должна быть

сформирована так называемая фокусная группа агентов. В состав этой группы должны входить агенты, отношения которых с респондентом базируются на физическом (наличие канала связи) и логическом (наличие протоколов обмена) уровнях. Примем, что с точки зрения состояния отношений в состав фокус-группы входят все агенты, для которых выполняется предикат $Ur = false$.

Опасность респондента

Обозначим все множество агентов из состава информационной системы как A и зафиксируем некоего агента как респондента $\gamma \in A$. Определим фокус-группу агентов для данного респондента $\gamma = const$ как Φ. Тогда условие отбора агента $\beta_i \in A$ на основании его отношения с респондентом $Q_\beta = (range,prob,undef)$ в состав фокус группы запишется как $\beta_i \in \Phi$: Q_β $(\{2,3,4\},\bullet,\bullet)$. Фокус-группа агентов по определению имеет общего респондента, который оказывает некое влияние на агентов группы. Под «опасностью респондента» будем понимать уверенность в том, что респондент может быть источником атаки. Такая уверенность, как было показано ранее, может формироваться только на основе интегральной обработки оценок состояния отношений каждого из агентов из состава группы.

В итоге имеем набор оценок как показано в табл. 1, в левой колонке которой перечислены агенты группы имеющих оценки для данного респондента.

Таблица 1.

Матрица оценок состояний отношений с респондентом

агент	*undef*	*rang*	*prob*
β_1	υ_1	η_1	p_1
β_2	υ_2	η_2	p_2
...	...	...	...
β_N	υ_N	η_N	p_N

Здесь N – число агентов в фокус-группе, $N = |\Phi|$. Каждая строка таблицы содержит величины *undef*, *rang* и *prob*, которые вычисляются каждым агентом независимо и автономно от других. То есть, в самом общем случае имеем отношения вида: $\sum_{i=1}^{N} p_i > 1$ и $\sum_{i=1}^{N} \nu_i > 1$. Отметим, что в силу особенностей процедуры комплексного оценивания мы не знаем связи между величинами rang и prob, и следует полагать, что $\forall i \in N\ p_i + \nu_i \neq 1$ для каждых отношений $\beta R \gamma$ агента с респондентом. При этом, $\forall i \in N\ 0 \le p_i, \nu_i \le 1$.

Для решения задачи оценки опасности респондента на ранних этапах осуществления им атаки введем функцию опасного состояния на основе параметров фокус-группы агентов:

$$Z = f(p|_\eta, \nu|_\eta) \quad (1)$$

Выражение (1) будем трактовать как определение уверенности в том, что данный набор (распределение) параметров состояний агентов может рассматриваться в качестве подтверждения опасности респондента.

Здесь необходимо сделать следующие уточнения:

1) под распределением параметров будем понимать подмножества величин *undef* и *prob*, формируемых для каждого из значений величины *rang*;
2) элементы данных множеств представляют из себя свидетельства в пользу доверия к тому или иному типу состояния респондента;
3) уверенность в опасности респондента будем определять как величину, имеющую значение при условии наличия распределения параметров.

Таким образом, с одной стороны, выражение (1) должно соответствовать условной вероятности, но, с другой стороны, приведенные выше определения для величин *rang* и *prob* не позволяют их трактовать как вероятности полной группы событий.

Вместе с тем функция опасного состояния (1) должна формировать единую шкалу оценки опасности для любых сочетаний величины *undef*, *rang* и *prob* агентов.

С учетом изложенного, используем энтропийный подход. Как известно, энтропия события X при условии наступления события Y определяется правилом Байеса:

$$H(X|Y) = H(X) - H(Y) + H(Y|X) \quad (2)$$

Дадим следующие трактовки компонентам формулы (2) применительно к поставленной задаче (1) и соответственно переопределим переменные.

$H(X|Y) \longrightarrow H(J|D)$. Представляет собой показатель наличия опасности (Jeopardy) при данном наборе (Distribution) оценок. В нашем случае это все оценки *prob* агентов, находящихся в состоянии Dr и $\overline{Lr}$. Из этих оценок посредством единой функции $g(R)$ образуем соответствующие множества оценок. Тогда функция $f(\bullet)$ от объединения этих множеств даст требуемый показатель. Отметим, что $\overline{Lr} \neq Dr$, поскольку имеет место быть отношение вида $\sum_{i=1}^{N} p_i > 1$, которые определены при описании табл. 1. В итоге можем записать

$$H(J|D) = f(g(Dr) \cup g(\overline{Lr})). \quad (3)$$

$H(Y) \longrightarrow H(D)$. По сути является показателем энтропии, то есть неопределенности источника набора оценок. В качестве источника выступает та часть агентов, которые оценивают состояние отношений с респондентом через Неопределенное состояние отношений с респондентом. То есть имеем по аналогии с (3):

$$H(D) = f(g(Ir)). \quad (4)$$

$H(Y|X) \longrightarrow H(D|J)$. Можно рассматривать как показатель достоверности появления данного набора оценок при определенной опасности или как соответствие набора оценок опасности. Отметим, что у нас нет полного описания всего множества опасностей, но поскольку величины undef и prob определены на множестве событий и сообщений агента, то мы можем говорить о полном описании множества оценок. При этом величину *undef* целесообразно рассматривать как ошибки определения состояний. Отсюда можно положить, что

$$H(D|J) = f(g(\overline{undef})). \quad (5)$$

В выражении (2) остается неопределенной переменная $H(X)$, которую можно трактовать как уверенность в том, что респондент является источником атаки. Возвращаясь к выражению (1), целесообразно говорить об оценке опасности респондента, что дает выражение

$$H(Z) = H(J|D) + H(D) - H(D|J). \quad (6)$$

Или в развернутом виде

$$H(Z) = f(g(Dr) \cup g(\overline{Lr})) + f(g(Ir)) - f(g(\overline{undef})). \quad (7)$$

Для сохранения тождественности между выражениями (6) и (7) выполним переход от вероятностных величин *undef* и *prob* к значениям энтропии. Для этого воспользуемся тем фактом, что величины в табл. 1 формируются на основе максимальных значений *prob*, а значения *undef* непосредственно связаны с ними. Следовательно, вместо этих величин будем использовать min-энтропию $H(x) = \ln(P_{max})$. С учетом особенностей логарифмической функции проведем нормировку ее переменных следующим образом: $H(x) = \ln(1 + P_{max})$.

Определим функцию $g(R)$, результатом работы которой должно быть множество оценок агентов из состава фокус-группы, находящихся в том или ином состоянии $\Phi(\cdot)$.

$$g(Dr): \forall i \in N \ln(1 + p_i) \in \Phi(Dr) \longrightarrow \eta = 4, \quad (8)$$

$$g(Ir): \forall i \in N \ln(1 + p_i) \in \Phi(Ir) \longrightarrow \eta = 3. \quad (9)$$

Далее необходимо определить аналогичные функции, содержащие логические отрицания: $g(\overline{Lr})$ и $g(\overline{undef})$. Поскольку речь идет о переходе от вероятностных величин к энтропии, воспользуемся известным выражением из теории вероятностей для чего определим единицу для выражения $p(\overline{x}) = 1 - p(x)$. Тогда, с учетом нормировки, имеем:

$$g(\overline{Lr}): \forall i \in N (2ln2 - \ln(1 + p_i) \in \Phi(Lr) \longrightarrow \eta = 2, \quad (10)$$

$$g(\overline{undef}): \forall i \in N (2ln2 - \ln(1 + v_i) \in \Phi(undef). \quad (11)$$

Поскольку каждый агент из состава фокус-группы определяет величины *undef* и *prob* автономно и независимо, то в соответствии со свойствами энтропии функция $f(\cdot)$ выражения (7) представляет собой сумму значений, получающихся в (8)–(11). Обозначим мощность множеств фокус-групп $\Phi(\cdot)$, полученных из (8)–(11) как $I(\cdot)=|\Phi(\cdot).|$. Соответственно, получаем итоговое выражение для (6):

$$H(Z) = \sum_{I(Dr)}(\ln(1 + p_i)) + \sum_{I(Lr)}(2ln2 - \ln(1 + p_i)) + \\ + \sum_{I(Ir)}(\ln(1 + p_i)) - \sum_{I(undef)}(2ln2 - \ln(1 + v_i)). \quad (12)$$

Исследуем выражение (12) для предельных случаев, когда все агенты дают единую оценку состояний отношений с респондентом.

Первый случай представляет из себя оценивание всеми агентами состояние отношения с респондентом как «Лояльно» с нулевой ошибкой, что приводит выражение (12) к виду $H(Z) = \sum_{I(Lr)}(ln2 - \ln(1 + p_i)) - \sum_{I(undef)}(2ln2 - \ln(1 + v_i))$, где $p_i = 1$, а $v_i = 0$. В результате, получаем $H(Z) = -\sum_{I(undef)}(ln2)$.

Второй случай представляет собой оценивание всеми агентами состояния отношения с респондентом как «Нелояльно» с нулевой ошибкой, что приводит выражение (12) к виду $H(Z) = \sum_{I(Dr)}(\ln(1 + p_i) - - \sum_{I(undef)}(ln2 - \ln(1 + v_i))$, где $p_i = 1$, а $v_i = 0$. В результате, при условии $I(Dr) = I(undef) = N$, получаем $H(Z) = 0$.

Кажущееся противоречие результатов в каждом из случаев обусловлено нормированием величин *undef* и *prob*. Для компенсации этого нормирования нужно ввести «нормировочную единицу» $NlnN$, что дает оценку опасного состояния на основе параметров фокус-группы агентов для выражения (1)

$$Z = NlnN - |H(Z)|, \quad (13)$$

$N = |\Phi|$ – размер фокус-группы, а величина $H(Z)$ берется по абсолютному значению для сохранения логики компенсации.

Отметим, что введение «нормировочной единицы» практически убирает зависимость оценки опасности состояния от размеров фокус-группы, что важно при практическом применении результатов оценивания в сложной системе для сравнения различных фокус-групп.

Рассмотрим предельный случай, когда размер фокус-группы равен единице. Выражение (13) в этом случае дает отрицательный результат, что противоречит общепринятому требованию о положительном значении энтропии. Следовательно, окончательный вариант вычисления опасного состояния примет вид:

$$Z = \sqrt{(NlnN - |H(Z)|)^2}. \quad (14)$$

В качестве примера фокус-группы, имеющей единичный размер, можно привести вариант использования единственного контроллера домена в ИС. Как уже отмечалось, выражение (13) для фокус-группы, состоящей из одного элемента дает отрицательный результат, показывающий невозможность проактивного мониторинга для единственного агента в ИС. Отсюда следует, что проведение проактивного мониторинга в случае единичного размера фокус-группы возможно лишь при условии введения в состав ИС дополнительных специализированных агентов, способных формировать последовательности событий эквивалентные единственному участнику фокус-группы. То есть речь идет о введении в ИС агентов-honeypot или о зеркалировании трафика на агентов с идентичными функциональными характеристиками.

В качестве промежуточного вывода укажем, что, согласно выражению (14), всегда будем иметь $Z > 0$, то есть предложенная оценка опасности соответствует реалиям ИБ, когда не существует абсолютной защиты от деструктивных воздействий.

Макроуровень

Разработанные в предыдущем разделе оценки опасности респондента позволяют перейти к рассмотрению отношений между агентами $\beta \in A$ сложной системы A на макроуровне.

В соответствии с табл. 1 примем, что множество $LC(\gamma) = \bigcup_N LC(\beta|_\gamma)$ включает в себя идентичные по характеристикам (например, одинаковый номер открытого порта) точки доступа агентов фокус-группы. На основании табл. 1 обозначим множество $Q(\gamma)$ как состоящее из векторов $[undef, rang. prob]$, получаемых каждым из агентов фокус-группы в результате оценки состояния отношений агент – респондент. Рассмотрим отношение «респондент – оценка опасности» $\gamma \longrightarrow Z$ посредством множеств с помощью диаграммы, приведенной на рис. 4.

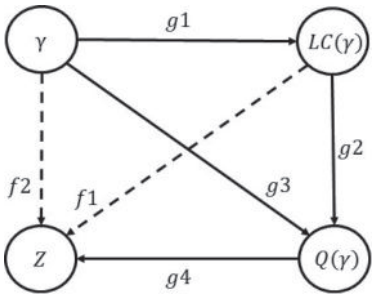


Рис. 4. Диаграмма респондент – опасность

Утверждение 1. Оценка опасности (13) является общей для данного типа точки доступа для всех агентов из состава фокус-группы.

Доказательство утверждения будем проводить на основании диаграммы респондент-опасность, приведенной на рис. 4. Морфизмы $g1$ – $g3$ соответствуют порядку формирования оценки состояния отношений агентов фокус-группы с респондентом на основе доступных респонденту точек доступа агентов. Морфизм $g4$ соответствует формированию оценки опасности респондента на базе состояний отношений агентов. Морфизмы $f1$ и $f2$ обеспечивают коммутативность диаграммы, что подтверждает утверждение. Помимо этого, выражения (1)–(13) показывают, что оценка опасности данного респондента определяется интегрально по всем оценкам состояний со стороны агентов, которые формируются на потоке событий от данных точек доступа и являются отображением возможностей нарушителя.

Отметим, что правая пара узлов диаграммы является множествами, в то время как левая пара представляется как отдельные единичные величины. Но фактически узлы левой пары также являются множествами, формирующимися во временной области:

- узел $Q(\gamma)$ на каждом из агентов может быть сформирован только на основе воздействий со стороны узла γ в течение определенного интервала времени;
- узел Z также формируется в течение заданного временного интервала.

Соответственно, узлы γ и Z диаграммы следует рассматривать как временные ряды определенной длины, что позволяет рассматривать диаграмму рис. 4 как описание пространственно-временного перехода:

- *временной ряд внешних воздействий на фокус группу агентов →;*
- *пространственная структура формирования оценок воздействий каждым из агентов →;*
- *временной ряд оценок опасности респондента.*

В дальнейших рассуждениях будем опираться на общеизвестный факт о том, что по своей сути ИС, как сложная система, естественным образом может быть представлена как мультиграф, поскольку взаимодействие агентов из ее состава основано на использовании нескольких портов и протоколов, или точек доступа, в нашем понимании, каждым из агентов.

Ранее [15-16] предлагалось отождествить респондентов с точками доступа агента. Утверждение 1 подтверждает такой подход. Сделаем следующий шаг в наших рассуждениях и обозначим:

$LC(\beta_i)$ – множество точек доступа i-го агента фокус-группы;

Φ – множество агентов фокус-группы;

$LC(\Phi)$ – множество уникальных точек доступа фокус-группы;

$LC(\beta|_\gamma)$ – множество идентичных точек доступа агентов фокус-группы.

Утверждение 2. При отображении респондента на точку доступа агента фокус-группа может быть представлена как множество уникальных точек доступа всех агентов из ее состава $LC(\Phi) = \bigcup_{i \in N} LC(\beta_i)$.

Доказательство утверждения проведем на основе диаграммы точек доступа, представленной на рис. 5.

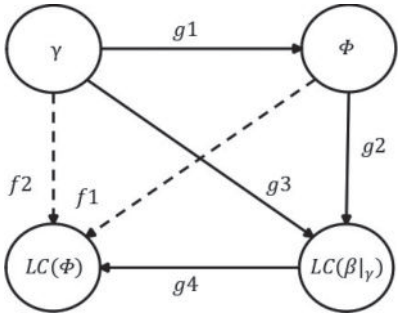


Рис. 5. Диаграмма точек доступа

Морфизмы $g1 - g3$ соответствуют пространственно-временному переходу при проведении проактивного мониторинга агентами фокус-группы. Морфизм $g4$ отображает формирование множества уникальных точек доступа группы. Морфизмы $f1$ и $f2$ обеспечивают коммутативность диаграммы, что свидетельствует в пользу истинности утверждения. В качестве дополнительного аргумента доказательства приведем следующее рассуждение. Представление фокус-группы множеством $LC(\Phi)$ полностью соответствует имеющимся моделями атак в ИБ, базирующимся на том факте, что нарушитель после установления контроля над агентом, оказывающимся в роли респондента, ограничен в своих возможностях только составом точек доступа агентов, с которыми могут быть установлены отношения и составляющих в общем случае фокус-группу.

В качестве примера рассмотрим случай, когда нарушитель-субъект находится вне пределов ИС. По результатам исследований организаций mitre.org и first.org будем полагать, что атака на ИС проводится с разных адресов. Тогда узел γ диаграммы рис. 5 представляет собой подмножество агентов, находящихся под контролем нарушителя. Что является по сути фокус-группой нарушителя, позволяющей ему оценивать свои возможности на основании реакции атакуемых агентов ИС. Соответственно, можно продолжить данное рассуждение и на случай продвижения нарушителя по структуре ИС.

Таким образом, морфизм $f2$ дает основание перейти от понятия «респондент» как атакующего агента к понятию «источник атаки», в роли которого в общем случае выступают агенты той или иной фокус-группы.

Морфизм $f1$, в свою очередь, показывает, что отдельная фокус-группа агентов может отображаться как на отдельную точку доступа, так и на несколько таких точек в случае идентичности агентов из состава группы, что позволяет определить множество точек доступа фокус-группы $LC(\Phi)$ как поверхность атаки для агентов из состава группы.

Следовательно, получаем двойственный характер фокус-группы, которая одновременно может рассматриваться как источник и как поверхность атаки. В самом общем случае это соответствует одновременной деятельности субъектов ИБ – нарушителя и защитника. В свою очередь, двойственный характер фокус-группы позволяет рассматривать выражение (14) и как оценку возможностей нарушителя, и как оценку опасности точек доступа.

Предлагаемый подход позволяет говорить о возможности декомпозиции ИС на основе фокус-групп, манипулируя которыми как источниками и поверхностью атаки, можно проводить декомпозицию до уровня отдельных агентов, выступающих в роли атакующего или защищаемого объектов.

Сделаем следующие предположения.

1. В соответствии с диаграммой проактивной оценки респондента (рис. 3) каждая фокус-группа содержит специализированные агенты, которые обозначим как:
   AL – множество агентов, обеспечивающих функции сбора и обработки событий и сообщений, что соответствует узлу δ диаграммы;
   AK – множество агентов, обеспечивающих манипулирование информационными потоками других агентов, что соответствует узлу σ диаграммы;
   AB – множество агентов, обеспечивающих функции передачи и обработки данных в ИС (то есть все узлы образующие фокус-группы), что соответствует узлу β диаграммы.
2. Каждая фокус-группа может выступать в роли источника атаки своими агентами, что согласуется с понятием сложной системы, поэтому все возможные связи между источниками и поверхностью атаки будем представлять в виде шины.

Итоговое представление ИС на макроуровне как сложной системы на основе фокус-групп приведено на рис. 6.

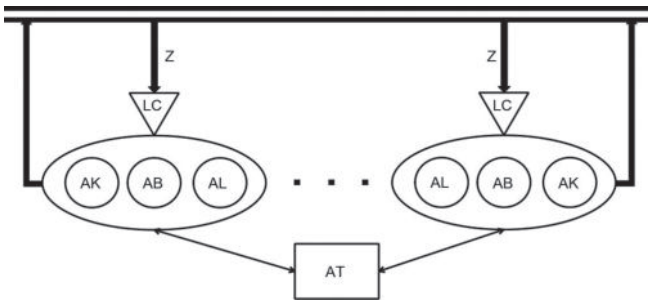


Рис. 6. Макроуровень представления ИС

Широкие стрелки на рисунке обозначают воздействие на или со стороны фокус-группы, которая представлена большим овалом. Треугольники обозначают одну или несколько точек доступа фокус-группы. Буквами Z обозначены оценки опасности точек доступа, получаемые согласно выражению (14), для каждой точки доступа каждой из фокус-групп. Кроме того, на рис. 6 показан орган управления работой фокус-групп:

AT – множество агентов, обеспечивающих функции формирования и доставки правил работы фокус-групп, прежде всего агентов типа AK и AL.

Предлагаемая концепция построения макроуровня ИС как сложной системы позволяет рассматривать ее с точки зрения распределения оценок опасности Z как по фокус-группам, так и по отдельным агентам из состава ИС.

Представляется целесообразным определить данное распределение в качестве состояния сложной системы.

Без потери общности положим, что каждая фокус-группа имеет одну точку доступа, которая испытывает внешнее воздействие со стороны одного источника. Тогда последовательность фокус-групп, представляющих ИС и испытывающих воздействия на точки доступа, может быть определена как *сценарий*. В свою очередь, сценарий может быть представлен взвешенным орграфом, как показано на рис. 7. Отметим, что связи графа сценариев определяются тем фактом, что отношения между агентами базируются на физическом (наличие канала связи и логическом (наличие протоколов обмена) уровне.

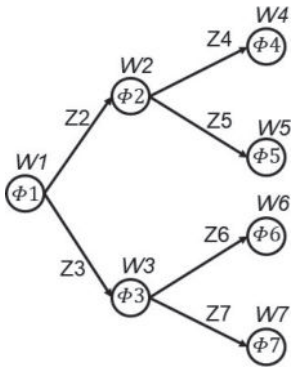


Рис. 7. Орграф сценария

На рис. 7 символом Z обозначены веса связей, определяемые выражением (14), а символом W – веса вершин графа сценария, которые определяются по аналогии с оценкой Z на основе базовых характеристик состояния отношений агентов из состава фокус-группы.

Веса вершин графа должны отражать «степень единообразия» агентов фокус-групп в формировании базовых характеристик $prob$ и $undef$. Представляется целесообразным использовать в этом качестве величину разброса величин $prob$ и $undef$ и определить вес вершины как характеристику устойчивости оценки опасности. Для этого определим два множества, объединяющих величины $prob$ – p и $undef$ – v для всех агентов из состава фокус-группы независимо от показателя состояния, то есть сформируем два различимых множества, содержащих повторяющиеся элементы. Данную операцию обозначим символом $\amalg x$. В итоге получим:

$$P = \amalg_{\beta\in\Phi} p_\beta, \quad (15)$$

$$V = \amalg_{\beta\in\Phi} v_\beta. \quad (16)$$

Величину разброса значений из множеств (15) и (16) определим как расстояние между некоей опорной точкой X и каждым из значений $p_i \in P$ и $v_i \in V$: $\mathrm{d} = (p_i \vee v_i) - X$. Отметим, что $|P| = |V| = N$ и, соответственно, $i = [1,N]$. При определении расстояния будем исходить из следующих условий:

- расстояние определяем на шкале [0,1] в соответствии с областями определения величин $prob$ и $undef$;
- одинаковые значения величин должны давать одинаковое расстояние;
- значения $prob$ должны группироваться как можно ближе к опорной точке, соответствующей «1» шкалы, что будет свидетельствовать о наибольшей согласованности наиболее вероятных оценок состояния отношений со стороны агентов из состава фокус-группы;
- значения $undef$ должны группироваться как можно ближе к опорной точке, соответствующей «0» шкалы, что также будет свидетельствовать о наименьшем числе ошибок при определении оценок состояния отношений со стороны агентов из состава фокус-группы;
- увеличение разброса значений величин $prob$ и $undef$ свидетельствует о снижении устойчивости оценок опасности фокус-группой.

Исходя из перечисленных условий определим расстояния следующим образом

$$d_p = \sum_{i=[1,N]} (p_i - 1)^2, \quad (17)$$

$$d_v = \sum_{i=[1,N]} (v_i)^2. \quad (18)$$

Выражения (17) и (18) имеют прямую аналогию с метрикой нормированного пространства, что позволяет определить «плотность» группирования (с учетом условий) как несмещенную оценку

$$\sigma_P = \sqrt{(1/\mathrm{n} - 1)d_p}, \quad (19)$$

$$\sigma_v = \sqrt{(1/\mathrm{n} - 1)d_v}. \quad (20)$$

Отметим, что одновременное увеличение результатов вычисления выражений (19) и (20) будет приводить к сокращению расстояния между распределениями, представленными множествами P и V. Определим данное расстояние как разницу интервалов

$$\mu = \frac{(p_{max} + p_{min}) - (v_{max} + v_{min})}{2}. \quad (21)$$

С учетом применяемого энтропийного подхода и особенностей логарифмической функции неопределенность устойчивости оценки опасности определится как

$$H(W) = \ln(1 + \sigma_p) + \ln(1 + \sigma_{\_v}) - ln(1 + \mu). \quad (22)$$

Максимальная неопределенность при этом будет достигаться при равномерном распределении значений *prob* и *undef* по шкале [0,1]. При максимальной концентрации величин *prob* и *undef* около границ шкалы – «1» и «0» соответственно – выражение (22) примет отрицательное значение, что обусловлено нормированием величин, получаемых из (19–23). Для компенсации этого нормирования введем «нормировочную единицу» *2ln2*, что дает следующее выражение для определения устойчивости оценки опасного состояния на основе параметров фокус-группы агентов

$$W = 2\ln 2 - |H(W)|. \quad (23)$$

В качестве промежуточного вывода укажем, что, согласно выражению (23), всегда будем иметь $W > 0$, то есть некоторую устойчивость оценки опасности, поскольку в основе расчета опасности лежат реальные события и сообщения, формируемые внешним воздействием.

Еще один вывод заключается в следующем. Поскольку веса ребер и вершин орграфа сценария, приведенного на рис. 7, изменяются во времени по мере развития атаки, то этот факт подтверждает оправданность использования принципа пространственно-временного перехода.

В качестве простейшего подхода к формированию фокус-группы приведем пример на основании таких параметров, описывающих точки доступа, как шлюз по умолчанию, номер и маска подсети агентов. В результате мы можем определить опасность именно точек доступа агентов фокус-группы по результатам внешнего воздействия, который при этом представляет собой несколько различных агентов-нарушителей, осуществляющих доступ к агентам фокус-группы через единую точку – входной шлюз. При этом все агенты группы, имеющие данный тип точки доступа, «стягиваются» в один узел трансформируемого графа ИС. То есть подмножество агентов фокус-групп ИС замещаем набором подмножеств из точек доступа, что позволяет говорить о декомпозиции сложной системы.

Еще один подход к декомпозиции заключается в выделении слоев ИС как сложной системы. Поскольку множества LC(Ф) для каждой фокус-группы, сформированной в ИС, содержат пересекающиеся (и ограниченные) наборы точек доступа, то это дает возможность для представления ИС в виде слоев, содержащих точки доступа одного типа из состава всех фокус-групп ИС. При этом представляет интерес исследование структуры слоев на предмет наличия изолированных или слабо соединенных кластеров, а также обязательных переходов нарушителя между слоями при проведении атаки.

Отметим, что использование сценариев дает возможность для моделирования действия субъекта-нарушителя, а использование слоев позволяет моделировать действия субъекта-защитника, особенно в случаях проведения атак на фиксированные точки доступа.

В любом случае декомпозиция создает условия для опережающей реакции по всем узлам ИС на используемые нарушителем порты и протоколы – точки доступа, что важно в условиях автоматизации деструктивной деятельности. Отличительной чертой предлагаемой декомпозиции является возможность применения единого функционально-логического подхода на всех уровнях – от ИС в целом до отдельных агентов только за счет манипулирования составом подмножеств точек доступа и фокус-групп.

Приведенные в статье типы агентов позволяют рассматривать ИС как систему, состоящую из фокус-групп, каждая из которых имеет в своем составе специализированных агентов, обеспечивающих управление мониторингом и потоками остальных агентов.

Заключение

В рамках общей цели исследования (адаптации логико-вероятностного метода для решения задач ИБ) в статье разработаны формально-логические основы определения количественных и качественных оценок состояний отношений функционально однородных агентов в многоагентных системах как результат агрегирования состояний отдельных агентов. Данные оценки закладывают основы для последующего применения логико-вероятностного метода при рассмотрении вопросов защиты информации в многоагентных системах. Предлагаемые механизмы количественного и качественного оценивания состояния отношений агентов позволяют проводить декомпозицию физической и логической структуры современных ИС как сложных систем. При этом, созданы условия для использования при организации ИБ подходов и методов, лежащих в основе искусственных иммунных систем.

Литература

1. *Рябинин И. А. Решение одной задачи оценки надежности структурно-сложной системы разными логико-вероятностными методами / И. А. Рябинин, А. В. Струков // Моделирование и анализ безопасности и риска в сложных системах, Санкт-Петербург, 19–21 июня 2019 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2019. – С. 159–172.*
2. *Демин А. В. Глубокое обучение адаптивных систем управления на основе логико-вероятностного подхода / А. В. Демин // Известия Иркутского государственного университета. Серия: Математика. – 2021. – Т. 38. – С. 65–83. DOI: 10.26516/1997-7670.2021.38.65.*
3. *Викторова В. С. Вычисление показателей надежности в немонотонных логико-вероятностных моделях многоуровневых систем / В. С. Викторова, А. С. Степанянц // Автоматика и телемеханика. – 2021. – № 5. – С. 106–123. DOI: 10.31857/S000523102105007X.*
4. *Леонтьев А. С. Математические модели оценки показателей надежности для исследования вероятностно-временных характеристик многомашинных комплексов с учетом отказов / А. С. Леонтьев, М. С. Тимошкин // Международный научно-исследовательский журнал. – 2023. – № 1(127). С. 1–13. DOI: 10.23670/IRJ.2023.127.27.*
5. *Пучкова Ф. Ю. Логико-вероятностный метод и его практическое использование / Ф. Ю. Пучкова // Информационные технологии в процессе подготовки современного специалиста: Межвузовский сборник научных трудов / Министерство просвещения Российской Федерации; Федеральное государственное бюджетное образовательное учреждение высшего образования «Липецкий государственный педагогический университет имени П. П. Семенова-Тян-Шанского». Том Выпуск 25. – Липецк: Липецкий государственный педагогический университет имени П. П. Семенова-Тян-Шанского, 2021. – С. 187–193.*
6. *Россихина Л. В. О применении логико-вероятностного метода И. А. Рябинина для анализа рисков информационной безопасности / Л. В. Россихина, О. О. Губенко, М. А. Черноситова // Актуальные проблемы деятельности подразделений УИС: Сборник материалов Всероссийской научно-практической конференции, Воронеж, 20 октября 2022 года. – Воронеж: Издательско-полиграфический центр «Научная книга», 2022. – С. 108–109.*
7. *Карпов А. В. Модель канала утечки информации на объекте информатизации / А. В. Карпов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 марта 2018 года / Под редакцией С. В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2018. – С. 378–382.*
8. *Методика кибернетической устойчивости в условиях воздействия таргетированных кибернетических атак / Д. А. Иванов, М. А. Коцыняк, О. С. Лаута, И. Р. Муртазин // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 марта 2018 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 343–346.*
9. *Елисеев Н. И. Оценка уровня защищенности автоматизированных информационных систем юридически значимого электронного документооборота на основе логико-вероятностного метода / Н. И. Елисеев, Д. И. Тали, А. А. Облаченко // Вопросы кибербезопасности. – 2019. – № 6(34). – С. 7–16. DOI: 10.21681/2311-3456-2019-6-07-16.*
10. *Коцыняк М. А. Математическая модель таргетированной компьютерной атаки / М. А. Коцыняк, О. С. Лаута, Д. А. Иванов // Наукоемкие технологии в космических исследованиях Земли. – 2019. – Т. 11, № 2. – С. 73–81. DOI: 10.24411/2409-5419-2018-10261.*
11. *Белякова Т. В. Функциональная модель процесса воздействия целевой компьютерной атаки / Т. В. Белякова, Н. В. Сидоров, М. А. Гудков // Радиолокация, навигация, связь: Сборник трудов XXV Международной научно-технической конференции, посвященной 160-летию со дня рождения А. С. Попова. В 6-ти томах, Воронеж, 16–18 апреля 2019 года. Том 2. – Воронеж: Воронежский государственный университет, 2019. – С. 108–111.*
12. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 1) / А. О. Калашников, К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда, К. В. Табаков // Вопросы кибербезопасности. – 2023. – № 4 (56). – С. 23–32. DOI:10.21681/2311-3456-2023-4-23-32.*
13. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 2) / А. О. Калашников, К. А. Бугайский, Е. И. Аникина, И. С. Перескоков, Ан. О. Петров, Ал. О. Петров, Е. С. Храмченкова, А. А. Молотов // Вопросы кибербезопасности. – 2023. – № 5 (57). – С. 113–127. DOI:10.21681/2311-3456-2023-5-113-127.*
14. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 3) / А. О. Калашников, К. А. Бугайский, Е. И. Аникина, И. С. Перескоков, Ан. О. Петров, Ал. О. Петров, Е. С. Храмченкова, А. А. Молотов // Вопросы кибербезопасности. – 2023. – № 6 (58). – С. 20–34. DOI: 10.21681/2311-3456-2023-6-20-34.*
15. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 4) / А. О. Калашников, Е. В Аникина, К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда, К. В. Табаков // Вопросы кибербезопасности. – 2024. – № 3 (61). – С. 23–32. DOI: 10.21681/2311-3456-2024-3-23-32.*
16. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 5) / А. О. Калашников, Е. В Аникина, К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда, К. В. Табаков // Вопросы кибербезопасности. – 2024. – № 4 (62). – С. 26–37. DOI: 10.21681/2311-3456-2024-4-26-37.*

APPLICATION OF THE LOGICAL-PROBABILISTIC METHOD IN INFORMATION SECURITY. Part 6

Kalashnikov A. O.[5], Anikina E. V.[6], Bugaisky K. A.[7], Molotov A. A.[8]

Keywords: *information security model, assessment of complex systems, logical-probabilistic method, theory of relations, system analysis.*

The purpose of the article: *adaptation of the logical-probabilistic method of evaluating complex systems to the tasks of building information security systems in a multi-agent system.*

Research method: *during the research, the main provisions of the methodology of structural analysis, system analysis, decision theory, methods of evaluating events under the condition of incomplete information were used.*

The result: *This article continues the consideration of information security issues based on the analysis of the relationship between the subjects and the object of protection. Within the framework of the developed model, the definition of such concepts as hazard assessment, attack surface, as well as the scenario of a complex system is given. It is shown that these concepts can be quantified on the basis of appropriate assessments of the states of agents' relationships. The expediency of the introduction and the place of specialized agents providing control of monitoring processes for agents is shown. Cascading mechanisms are proposed to provide a unified logical and functional approach to determining hazard assessments. The obtained results provide a reasonable calculation and use of probabilistic characteristics for the subsequent analysis of relations between subjects of information security based on the application of the logical-probabilistic method in the analysis of these relations.*

Scientific novelty: *consideration of information security issues using the apparatus of mathematical and logical relations. Methods have been developed for quantifying the danger of destructive impact without involving information about the presence of actual or used threats both from the point of view of software and from the point of view of the logical structure of the IP. The equivalence between the danger of destructive effects and the current state of relations between agents is shown. A method for determining the stability of the assessment of the dangerous state of relations has been developed. It is shown that the developed methods for assessing the danger of states make it possible to exclude separate consideration of errors of the first and second kind when assessing the real intentions of the violator. Approaches have been developed to obtain integrated hazard assessments at the level of both individual agents and various subsystems of modern information systems and systems as a whole by managing the composition of aggregated assessments of the state of agents' relationships.*

References

1. *Ryabinin, I. A. Reshenie odnoj zadachi ocenki nadezhnosti strukturno-slozhnoj sistemy raznymi logiko-veroyatnostnymi metodami / I. A. Ryabinin, A. V. Strukov // Modelirovanie i analiz bezopasnosti i riska v slozhnyh sistemah, Sankt-Peterburg, 19–21 iyunya 2019 goda. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet aerokosmicheskogo priborostroeniya, 2019. – pp. 159–172.*
2. *Demin, A. V. Glubokoe obuchenie adaptivnyh sistem upravleniya na osnove logiko-veroyatnostnogo podhoda / A. V. Demin // Izvestiya Irkutskogo gosudarstvennogo universiteta. Seriya: Matematika. – 2021. – T. 38. – pp. 65–83. DOI: 10.26516/1997-7670.2021.38.65.*
3. *Viktorova, V. S. Vychislenie pokazatelej nadezhnosti v nemonotonnyh logiko-veroyatnostnyh modelyah mnogourovnevyh sistem / V. S. Viktorova, A. S. Stepanyanc // Avtomatika i telemekhanika. – 2021. – № 5. – pp. 106–123. DOI: 10.31857/S000523102105007X.*
4. *Leont'ev, A. S. Matematicheskie modeli ocenki pokazatelej nadezhnosti dlya issledovaniya veroyatnostno-vremennyh harakteristik mnogomashinnyh kompleksov s uchetom otkazov / A. S. Leont'ev, M. S. Timoshkin // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. – 2023. – № 1(127). – pp. 1–13. DOI: 10.23670/IRJ.2023.127.27.*
5. *Puchkova, F. YU. Logiko-veroyatnostnyj metod i ego prakticheskoe ispol'zovanie / F. YU. Puchkova // Informacionnye tekhnologii v processe podgotovki sovremennogo specialista: Mezhvuzovskij sbornik nauchnyh trudov / Ministerstvo prosveshcheniya Rossijskoj Federacii; Federal'noe gosudarstvennoe byudzhetnoe obrazovatel'noe uchrezhdenie vysshego obrazovaniya «Lipeckij gosudarstvennyj pedagogicheskij universitet imeni P. P. SEMENOVA-TYAN-SHANSKOGO». Tom Vypusk 25. – Lipeck: Lipeckij gosudarstvennyj pedagogicheskij universitet imeni P. P. Semenova-Tyan-SHanskogo, 2021. – pp. 187–193.*
6. *Rossihina, L. V. O primenenii logiko-veroyatnostnogo metoda I. A. Ryabinina dlya analiza riskov informacionnoj bezopasnosti / L. V. Rossihina, O. O. Gubenko, M. A. CHernositova // Aktual'nye problemy deyatel'nosti podrazdelenij UIS: Sbornik materialov Vserossijskoj nauchno-prakticheskoj konferencii, Voronezh, 20 oktyabrya 2022 goda. – Voronezh: Izdatel'sko-poligraficheskij centr «Nauchnaya kniga», 2022. – pp. 108-109.*

5 Andrey O. Kalashnikov, Dr. Sc. (Eng), Chief Researcher, Laboratory of Complex Systems Safety, V. A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia. E-mail: aokalash@ipu.ru

6 Evgeniya V. Anikina, Researcher, Laboratory of Complex Systems Safety, V. A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia. E-mail: ajanet@ipu.ru

7 Konstantin A. Bugaisky, Junior Researcher, Laboratory of Complex Systems Safety, V. A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia. E-mail: kabuga@ipu.ru

8 Alexander A. Molotov, Software Engineer of the Research and Implementation Department 89 of the V. A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia. E-mail: alpha.sphere@ya.ru

7. *Karpov, A. V. Model' kanala utechki informacii na ob"ekte informatizacii / A. V. Karpov // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2018): VII Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya. Sbornik nauchnyh statej. V 4-h tomah, Sankt-Peterburg, 28 fevralya – 01 marta 2018 goda / Pod redakciej S. V. Bachevskogo. Tom 2. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M. A. Bonch-Bruevicha, 2018. – pp. 378–382.*
8. *Metodika kiberneticheskoj ustojchivosti v usloviyah vozdejstviya targetirovannyh kiberneticheskih atak / D. A. Ivanov, M. A. Kocynyak, O. S. Lauta, I. R. Murtazin // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2018): VII Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya. Sbornik nauchnyh statej. V 4-h tomah, Sankt-Peterburg, 28 fevralya – 01 marta 2018 goda / Pod redakciej S.V. Bachevskogo. Tom 2. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M. A. Bonch-Bruevicha, 2018. – pp. 343–346.*
9. *Eliseev, N. I. Ocenka urovnya zashchishchennosti avtomatizirovannyh informacionnyh sistem yuridicheski znachimogo elektronnogo dokumentooborota na osnove logiko-veroyatnostnogo metoda / N. I. Eliseev, D. I. Tali, A. A. Oblanenko // Voprosy kiberbezopasnosti. – 2019. – № 6(34). – pp. 7–16. DOI: 10.21681/2311-3456-2019-6-07-16.*
10. *Kocynyak, M. A. Matematicheskaya model' targetirovannoj komp'yuternoj ataki / M. A. Kocynyak, O. S. Lauta, D. A. Ivanov // Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. – 2019. – T. 11, № 2. – pp. 73–81. DOI: 10.24411/2409-5419-2018-10261.*
11. *Belyakova, T. V. Funkcional'naya model' processa vozdejstviya celevoj komp'yuternoj ataki / T. V. Belyakova, N. V. Sidorov, M. A. Gudkov // Radiolokaciya, navigaciya, svyaz': Sbornik trudov XXV Mezhdunarodnoj nauchno-tekhnicheskoj konferencii, posvyashchennoj 160-letiyu so dnya rozhdeniya A. S. Popova. V 6-ti tomah, Voronezh, 16–18 aprelya 2019 goda. Tom 2. – Voronezh: Voronezhskij gosudarstvennyj universitet, 2019. – pp. 108–111.*
12. *Kalashnikov A. O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 1) / A. O. Kalashnikov, K. A. Bugaiskii, D. S. Birin, B. O. Deriabin, S. O. Tsependa, K. V. Tabakov // Voprosy kiberbezopasnosti. – 2023. – №4(56). – pp. 23–32. DOI:10.21681/2311-3456-2023-4-23-32.*
13. *Kalashnikov A. O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 2) / A. O. Kalashnikov, K. A. Bugaiskii, E. I. Anikina, I. S. Pereskokov, An. O. Petrov, Al. O. Petrov, E. S. Khramchenkova, A. A. Molotov // Voprosy kiberbezopasnosti. – 2023. – №5(57). – pp. 113–127. DOI:10.21681/2311-3456-2023-5-113-127.*
14. *Kalashnikov A. O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 3) / A. O. Kalashnikov, K. A. Bugaiskii, E. I. Anikina, I. S. Pereskokov, An. O. Petrov, Al. O. Petrov, E. S. Khramchenkova, A. A. Molotov // Voprosy kiberbezopasnosti. – 2023. – №6(58). – pp. 20–34. DOI: 10.21681/2311-3456-2023-6-20-34.*
15. *Kalashnikov A. O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 4) / A. O. Kalashnikov, K. A. Bugaiskii, E. I. Anikina, I. S. Pereskokov, An. O. Petrov, Al. O. Petrov, E. S. Khramchenkova, A. A. Molotov // Voprosy kiberbezopasnosti. – 2024. – №3 (61). – pp. 23–32. DOI: 10.21681/2311-3456-2024-3-23-32.*
16. *Kalashnikov A. O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 5) / A. O. Kalashnikov, K.A. Bugaiskii, E. I. Anikina, I. S. Pereskokov, An. O. Petrov, Al. O. Petrov, E. S. Khramchenkova, A. A. Molotov // Voprosy kiberbezopasnosti. – 2024. – №4 (62). – pp. 26–37. DOI: 10.21681/2311-3456-2024-4-26-37.*

АРХИТЕКТУРА СИСТЕМЫ ДЛЯ ПРОВЕДЕНИЯ ГЕНЕТИЧЕСКОГО РЕИНЖИНИРИНГА ПРОГРАММЫ С ПОДДЕРЖКОЙ ПОИСКА РАЗНОУРОВНЕВЫХ УЯЗВИМОСТЕЙ

Израилов К. Е.[1]

DOI: 10.21681/2311-3456-2025-1-108-116

Цель исследования: *повышение эффективности поиска уязвимостей в машинном коде программ путем его реверс-инжиниринга на базе генетического реинжиниринга, для чего предлагается архитектура соответствующей программной системы.*

Методы исследования: *обзор работ, системный анализ, структурный синтез архитектуры, аналитическое моделирование.*

Полученные результаты: *создана архитектура системы, представляющая собой совокупность последовательно выполняемых однотипных компонентов для деэволюции представлений исследуемой программы (ее машинного, ассемблерного и исходного кода, алгоритмов и пр.); на каждом из таких представлений осуществляется поиск соответствующих уязвимостей.*

Научная новизна *заключается в качественно новом развитии направления реверс-инжиниринга путем его интеллектуализации, для чего предлагается высокоуровневое описание архитектуры авторской системы генетического реинжиниринга, а также производится формализация функционирования ее элементов.*

Ключевые слова: *обратная разработка, обратный инжиниринг, генетический алгоритм, уязвимость, машинный код, архитектура, формализация.*

Введение

Уязвимости в программном обеспечении (далее – ПО) представляют существенную проблему для безопасности обрабатываемой информации [1]. Одним из наиболее эффективных путей противодействия является их поиск в программном коде с последующей нейтрализацией или отказом от использования небезопасного ПО [2, 3]. В случае отсутствия исходного кода программ применение ручного поиска уязвимостей в выполняемом (машинном, байт-, ином) коде имеет высокую трудоемкость и низкую оперативность, а автоматические средства – недостаточную результативность [4].

Уязвимости имеют наиболее явное отражение в тех представлениях программы (далее – Представление), в которых они были заложены и под которыми понимается состояние программы на некотором из этапов ее создания. В [5] были выделены следующие Представления – от наиболее высокоуровневых и человеко-ориентированных к низкоуровневым и машинно-ориентированным: идея, концептуальная модель, архитектура, алгоритмы, исходный код, ассемблерный код, машинный (далее – МК) или байт-код. Это принципиально усложняет задачу поиска всех уязвимостей только по одному («финишному») Представлению – выполняемому коду.

В этих обстоятельствах предпочтительным подходом может явиться предварительный реверс-инжиниринг (т.н. обратная разработка или реинжиниринг, далее – РИ) низкоуровневых Представлений к более высокоуровневым с применением соответствующих методов поиска уязвимостей на каждом из них. Данная задача РИ также считается сложной как с технической, так и с практической точек зрения и является отдельным научным направлением [6]. В связи с этим автором исследуется возможность деэволюции Представлений, основанная на применении искусственного интеллекта в части генетических алгоритмов (далее – ГА) для восстановления предыдущих Представлений по текущему (что позволяет говорить о полноценном *эволюционном реинжиниринге* программы). Суть такой генетической деэволюции заключается в итеративном решении оптимизационной задачи подбора кода программы (в текущей терминологии – искомой) в предыдущем Представлении, из которого был получен код заданной программы (в текущей терминологии – исследуемой) в текущем Представлении, что было многократно описано в авторских публикациях [7–10]. Согласно [9] любая программа представима в виде хромосомы их набора генов, каждый из которых в общем

1 Израилов Константин Евгеньевич, кандидат технических наук, доцент, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург, ORCHID: http://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56122749800. E-mail: konstantin.izrailov@mail.ru

случае ответственен за одну из конструкций языка программирования (символ, токен, синтаксическое правило и т.п.). Тогда задача сводится к «умному» (с позиции качественной минимизации количества вариантов) подбору генов для получения искомой программы, преобразуемой (например, компиляцией из языка С в язык Ассемблер) в исследуемую. Для этого создается популяция программ (т.е. множество особей с различными хромосомами), селекция их экземпляров, преобразуемых в близкие к искомой программе (оценка близости осуществляется с помощью так называемой фитнес-функции), скрещивание генов полученных таким образом хромосом (т.е. две «наилучшие» программы дают некоторую третью, близкую к им обоим), мутация отдельных генов (т.е. случайное изменение конструкций программы для избежания локальных экстремумов) и повторение процесса с момента селекции; когда одна из программ оказывается в точности преобразуемой в исследуемую (т.е. найден глобальный экстремум), то это означает решение задачи деэволюции Представлений.

Ранее был получен ряд моделей, методов и алгоритмов, теоретически решающих данную задачу, а частные эксперименты показали подтверждение данной (авторской) концепции. Для уточнения возможности практического создания необходимых программных средств изначально требуется проектирование архитектуры системы для проведения генетического РИ программы с поддержкой поиска разноуровневых уязвимостей (далее – Система), что и будет предложено в настоящей статье.

Обзор работ

Проведем обзор работ, в которых освещаются принципы и функциональные возможности систем поиска уязвимостей, основанных на РИ Представлений программы от низкоуровневых – ассемблерных, к более высокоуровневым – исходному коду, алгоритмам и т.п.

В качестве классических и хорошо известных систем можно привести IDA Pro [11] и Ghidra [12], предназначенные для дизассемблирования МК программ и поддерживающие большое количество семейств процессоров. Также в состав первой системы входит плагин декомпиляции Hex-Rays [6], во второй же данный функционал является встроенным; впрочем, восстановление исходного кода ограничено заданным набором поддерживаемых процессоров. Также ассемблерное представление программы может быть отображено в виде блок-схем, которые не являются полноценными алгоритмами, поскольку в их элементах все также содержатся машинные инструкции, а граф управления строится исключительно по низкоуровневым конструкциям условного перехода (и их аналогам). Поиск уязвимостей в обеих системах может осуществляться либо вручную экспертом (т.е. высококвалифицированным специалистом по безопасности кода, далее – Эксперт), либо с применением внешних анализаторов через программные интерфейсы (на языках Python и Java для продуктов, соответственно).

В работе [13] представлена архитектура программного комплекса для динамического анализа МК, состоящая из собственно среды анализа, а также среды выполнения кода и средств разработки виртуальных машин. Комплекс производит запуск исследуемой программы в виртуальной среде и собирает информацию об ее работе (трассы выполнения, снимки памяти и т.п.). Строится статико-динамическое отображение программы, позволяющее получать блок-схемы МК и восстанавливать форматы данных. Одним из сценариев работы комплекса является символьное выполнение программы, позволяющее расширить покрытие кода и выявить условия, приводящие к реализации уязвимостей различного типа. Могут быть добавлены новые сценарии за счет имеющегося программного интерфейса.

В ранней авторской работе [14] описывается архитектура комплекса, предназначенная для преобразования МК в форму, подходящую Эксперту для анализа на предмет уязвимостей. Особенностями архитектуры является наличие модулей для получения метаинформации об уязвимостях, визуализации кода, оценки качества восстановленного кода и корректировки процесса декомпиляции Экспертом.

Работа [15] посвящена созданию средств автоматического поиска уязвимостей в МК, основанных на расширенном представлении его алгоритмов и архитектуры, заданном парадигмой из 7 положений. При этом каждое из средств может работать с единым отображением программы, но обнаруживать уязвимости своего класса. Описан типовой шаблон архитектуры таких средств, состоящих из алгоритмов поиска – сигнатурного, эвристического, интеллектуального и статического фаззинга; архитектура поддерживает подключение внешних модулей для алгоритмической обработки Представлений программы, спецификации уязвимостей и взаимодействия с Экспертом.

В исследовании [16] описывается программный комплекс для совместного применения РИ и алгоритмов машинного обучения с целью обнаружения вредоносного ПО для Android. В качестве признаков классификации выбраны такие, как разрешения приложений, вызовы системных функций, используемые сервисы и др. Для РИ применяется внешняя утилита Jadx-Gui [17], получающая исходный Java-код и файлы манифеста из APK-файлов (архивных исполняемых пакетов для Android).

В [18] приводится программный продукт SLaDe (близкий к полноценному комплексу), предназначенный для декомпиляции и отличающийся от аналогов генерацией более человеко-ориентированного исходного кода за счет интеллектуализации. Показано преимущество продукта по сравнению с Ghidra и моделью ChatGPT (в части улучшения читаемости кода) на функциях из датасета ExeBench [19].

Согласно проведенному обзору, существует определенное количество комплексов, использующих РИ для поиска уязвимостей и применяющих различные техники. Тем не менее, все они ограничены лишь рядом Представлений программы, языками программирования, платформами и способами последующего поиска, а также применяют частные архитектурные решения. Однако, комплексов или их аналогов, хотя бы близких к решению текущей задачи, обнаружено не было.

Функциональные требования

Исходя из предыдущих (более теоретико- и прототип-ориентированных) исследований разных авторов, были выдвинуты следующие условно пронумерованные требования к архитектуре Системы:

1. Преобразование Представлений от низкоуровневых к высокоуровневым;
2. Применение единого шаблона ГА для преобразования Представлений;
3. Независимость алгоритмов деэволюции от синтаксисов кода в Представлениях;
4. Возможность поиска уязвимостей в каждом из Представлений;
5. Автоматическое определение длины хромосомы – важнейшего элемента ГА [20], используемого при составлении программы в искомом Представлении и существенно ускоряющего решение задачи деэволюции;
6. Частичная оптимизация самого процесса ГА;
7. Поддержка неограниченного количества Представлений, применяемых в программном инжиниринге для последовательного преобразования между ними;
8. Возможность управления процессом Экспертом.

Все указанные функциональные требования могут быть удовлетворены следующими способами, системно связанными друг с другом. Последовательное преобразование между Представлениями программы реализуемо путем построения каскада из однотипных компонентов деэволюции, выход каждого из которых является входом для следующего (требование 1). Каждая такая деэволюция должна строиться на базе ГА без использования строго заданных алгоритмов преобразований или статистических закономерностей между конструкциями языков программирования; а исходя из сути ГА (как последовательного создания популяций особей-программ, заданных хромосомами, с выбором наилучших представителей, над которыми осуществляются операции скрещивания и мутации их хромосом), его ядро должно использовать сравнение программ в исследуемом и искомом Представлениях (требование 2). Поскольку Представления, входные и выходные для компонента деэволюции, задаются формальным синтаксисом, то реализация самого ядра преобразований может быть общей и располагаться в одном модуле (требование 3). Для каждого такого Представления должен существовать набор методов поиска уязвимостей, как общих – например, сигнатурных, так и специализированных – например, экспертных (требование 4). Определение длины хромосомы может осуществляться путем генерации множества программ в искомом Представлении и преобразования их в исследуемое Представление с определением длины последних, что даст статистическое соответствие между этими длинами (требование 5). Также возможна частичная оптимизация процесс ГА на основании обрабатываемого им Представления программы; например, выбором более «подходящей» первоначальной популяции, отличной от случайно сгенерированной, или уточнением алгоритмов ГА (требование 6). Построение стека из последовательности однотипных компонентов деэволюции гипотетически позволит производить преобразование между Представлениями программы любой длины и состава (требование 7). Для последовательного преобразования Представлений посредством стека компонентов деэволюции, а также поиска в них уязвимостей, целесообразно иметь отдельный компонент управления, взаимодействующий с Экспертом (требование 8).

Схема архитектуры

Концептуальная схема архитектуры Системы, соответствующая заданным требованиям и способам их удовлетворения, предлагаемая автором, состоит из последовательности компонентов деэволюции Представлений, соответствующей pipeline-дизайну [21] – т.е. когда данные из одного компонента поступают на вход другого. При этом логика работы каждого такого компонента не зависит от синтаксисов Представлений, а сами синтаксисы (и ряд других данных) являются его параметрами. Исходя из того, что компоненты и их модули фактически представляют собой некоторые обработчики данных – т.е. классические функции, их можно формализовать следующим образом:

$$R_{i-1} = Compoment^{Deevolution}(R_i P_i^D),$$

где $Component^{Deevolution}(\ldots)$ – компонент деэволюции i-го Представления (Deevolution – *перев. на русс.*

Деэволюция); P_i^D – параметры компонента (D – *аббр. от англ.* Deevolution); R_{i-1} и R_i – программа в искомом (предыдущем) и исследуемом (текущем) Представлениях, соответственно. Тогда вся совокупность компонентов деэволюции представима в следующем формальном виде:

$$R_1 = Compoment^{Deevolution}(R_2, P_2^D) \circ \ldots \circ Compoment^{Deevolution}(R_n, P_n^D),$$

где «∘» – оператор последовательного применения $Compoment^{Deevolution}(R,\ldots)$, выходные данные которого являются входными для следующего компонента, передаваемого в него через 1-й параметр (т.е. R_i).

Для поиска уязвимостей предназначен собственный компонент, принимающий на вход необходимое Представление, а также дополнительные параметры; его формальная запись следующая:

$$V_i = Compoment^{FindVulnerability}(R_i, P_i^{FV}),$$

где $Compoment^{FindVulnerability}(\ldots)$ – компонент поиска уязвимостей в i-ом Представлении (FindVulnerability – *перев. на русс.* Поиск Уязвимостей); V_i – уязвимости, найденные в i-ом Представлении; P_i^{FV} – параметры компонента (FV – *аббр. от англ.* FindVulnerability).

В результате работы компонента $Compoment^{FindVulnerability}(\ldots)$ происходит выявление уязвимостей в определенном Представлении, что также может осуществляться по обобщенным алгоритмам, параметрически настраиваемым (например, передачей в них сигнатур искомых объектов) [22, 23].

Компонент, контролирующий весь процесс, получает на вход некоторые управляющие команды от Эксперта, выполняя определенную логику запуска деэволюции и поиска уязвимостей. Формальная запись компонента будет опущена, поскольку он не обрабатывает какие-либо существенные информационные потоки, а лишь последовательно вызывает другие компоненты.

Более детальная компонентно-модульная схема архитектуры Системы, соответствующая заданным требованиям и способам реализации (отражающая только один компонент деэволюции кроме всего стека – т.н. архитектурный блок), представлена на Рисунке 1; использованы следующие обозначения: серый пунктирный прямоугольник – компонент, синий прямоугольник – модуль компонента, зеленый прямоугольник с прямыми краями – внешнее программное средство (вызываемое компонентом), зеленый

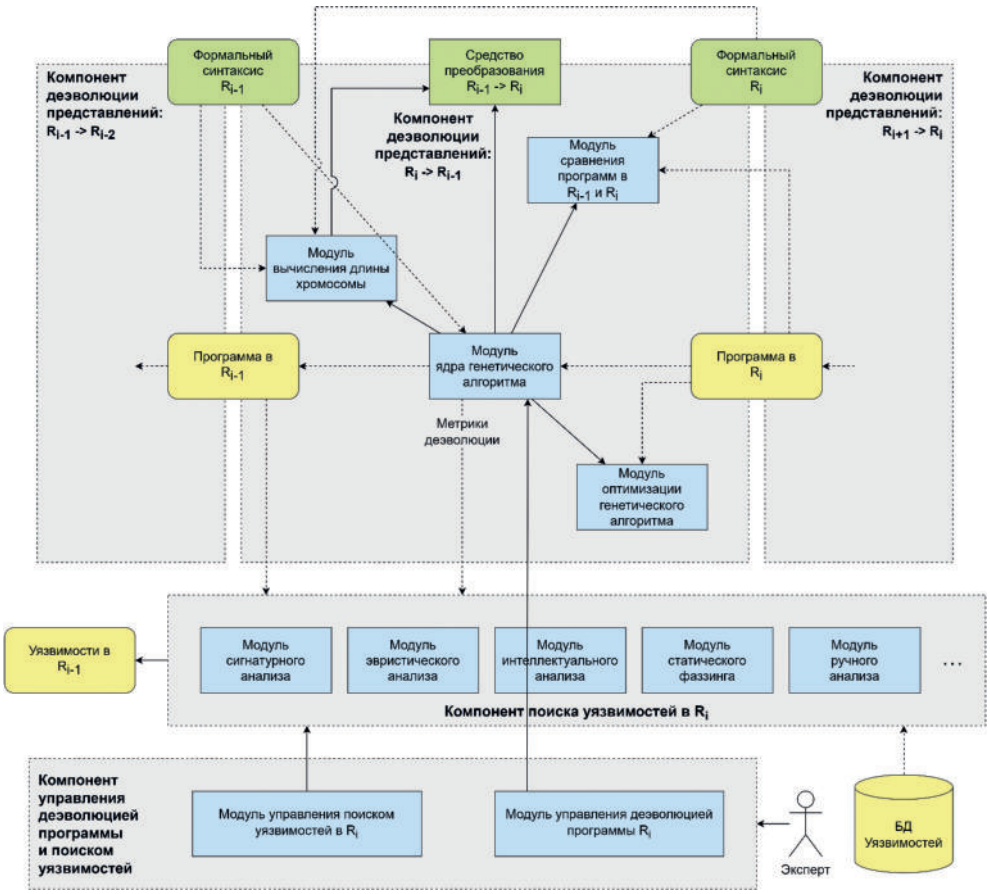


Рис. 1. Схема архитектуры системы для проведения генетического реинжиниринга программы с поддержкой поиска разноуровневых уязвимостей

прямоугольник со сглаженными краями – внешние данные (передаваемые в компоненты), желтый прямоугольник – генерируемые компонентами данные, сплошная линия – передача управления между модулями и компонентами (включая обмен данными), пунктирная линия – передача данных между модулями и компонентами, подписи к пунктирным стрелкам – передаваемые между модулями и компонентами данные.

Дадим описание элементов схемы (см. Рис. 1) и их частичную формальную запись с указанием основных параметров и возвращаемых данных.

Компонент деэволюции $Compoment^{Deevolution}$ (…) помимо программы в i-ом Представлении принимает на вход следующий параметр (указанный ранее):

$$P_i^D \equiv \langle S_i, S_{i-1}, Tool_i \rangle,$$

где S_i и S_{i-1} – формальный синтаксис i-го и $i-1$-го Представлений; $Tool_i$ – внешнее средство прямого преобразования программы из $i-1$-го Представления в i-ое Представление, т.е.:

$$R_i = Tool_i\ (R_{i-1}).$$

Примером средства преобразования является классический компилятор программ на языке С (т.е. в предыдущем Представлении), получающий ее в ассемблерном или бинарном виде (т.е. в текущем Представлении).

Компонент деэволюции состоит из набора взаимодействующих модулей, что определяет его следующим образом:

$$Compoment^{Deevolution} \equiv \langle Module_{Core}, Module_{ChromLength}, Module_{Comparison}, Module_{Optimization} \rangle,$$

где $Module_{Core}$ – модуль ядра ГА (*от англ.* Core, *перев. на русс.* Ядро), ответственного за решения задачи подбора программы в $i-1$-ом Представлении, преобразуемой в i-ое Представление; $Module_{ChromLength}$ – модуль вычисления длины хромосомы (*от англ.* Chromosome Length, *перев. на русс.* Длина Хромосомы) для записи программы в $i-1$-ом Представлении, которая может быть преобразована в i-ое Представление путем подбора конструкций программы (т.е. генов хромосомы особи популяции); $Module_{Comparison}$ – модуль нахождения близости двух программ (*от англ.* Comparison, *перев. на русс.* Сравнение) в одном Представлении (т.е. реализация фитнес-функции ГА); $Module_{Optimization}$ – модуль, оптимизирующий работу ГА (*от англ.* Optimization, *перев. на русс.* Оптимизация), т.е. уменьшающий количества создаваемых популяций (например, путем выбора изначальной популяции, близкой к искомой, улучшения точности фитнес-функции или уточнения настроек алгоритмов селекции, скрещивания и мутации).

Работа каждого из модулей компонента деэволюции может быть формально записана следующим образом:

1) модуль вычисления длины хромосомы:

$$Length_{i-1} = Module_{ChromLength}\ (S_i, S_{i-1}, \overline{Tool_i}),$$

где $Length_{i-1}$ – длина хромосомы для записи программы в $i-1$-ом Представлении; здесь и далее черта над параметром означает передачу управления (с обменом данными) – т.е. средство прямого преобразования $Tool_i$ не передается в модуль, а вызывается (с передачей в него программы в $i-1$-ом Представлении и возвратом из него программы в i-ом Представлении).

2) модуль сравнения программ:

$$Fitness = Module_{Comparison}\ (S_i, R1_i, R2_i),$$

где $Fitness$ – результат оценки близости двух программ в одном Представлении (т.е. S_i); $R1_i$ и $R2_i$ – первая и вторая программа в i-ом Представлении (согласно логике работы ГА, ими являются одна из особей популяции и исследуемая программа).

3) модуль оптимизации ГА:

$$GAS = Module_{Optimization}\ (R_i),$$

где GAS – набор настроек ГА (*аббр. от англ.* Genetic Algorithm Settings, *перев. на русс.* Настройки Генетического Алгоритма), определенных анализом исследуемой программы в i-ом Представлении.

4) модуль ядра ГА (в отличие от остальных модулей возвращающий кортеж данных):

$$\langle R_{i-1}, Metrics \rangle = Module_{Core}\ (R_i, Length_{i-1}, GAS, \overline{Module_{Comparison}}, \overline{Tools_i}),$$

где $Metrics$ – множество метрик деэволюции, отражающих признаки уязвимостей в программе (например, аномалии в процессе деэволюции Представлений в виде чрезмерно длительного подбора блоков конструкций программы могут служить о частичном внешнем разрушении ее структуры из-за внедрения уязвимости в более низкоуровневое Представление).

Компонент $Compoment^{FindVulnerability}$ () помимо программы в i-ом Представлении принимает на вход следующий параметр (указанный ранее):

$$P_i^{FV} \equiv \langle Metrics, DB^{Vulnerability} \rangle,$$

где $DB^{Vulnerability}$ – полная база уязвимостей с их разделением по Представлениям (включая характеристики, необходимые для поиска).

Компонент поиска уязвимостей состоит из набора модулей, что определяет его следующим образом:

$$Compoment^{FindVulnerability} \equiv \langle Module_{Analysis_1}, \ldots, \ldots, \langle Module_{Analysis_N} \rangle,$$

где $Module_{Analysis_i}$ – модуль анализа, работающий по i-ому принципу, такому, как сигнатурный анализ

(поиск уязвимостей по определенным шаблонам) [24], интеллектуальный анализ (применение искусственного интеллекта для обнаружения уязвимостей) [25], статический фаззинг (перебор параметров программы или одной из ее подпрограмм для выявления системных исключений [26]), ручной анализ (т.е. исследование программы в текущем Представлении Экспертом) и др. Модули могут работать параллельно, анализируя восстановленное Представление и формируя список найденных уязвимостей (в более общем случае – подозрительных мест, метрик безопасности и пр.). Также модули компонента могут иметь принципы работы, инвариантные к анализируемому преставлению, а специфика их работы в этом случае будет учитываться характеристиками уязвимостей, передаваемыми через параметры:

$$V_{i-1,k} = Module_{Analysis_k}(R_{i-1}, P_i^A),$$

где $V_{i-1,k}$ – множество уязвимостей, найденных в $i-1$-ом Представлении с помощью k-го модуля поиска, т.е. все уязвимости в i-ом Представлении:

$$V_i = \bigcup_k V_{i,k};$$

а P_i^A – параметр для работы модулей по анализу i-го Представления, который определяется следующим образом:

$$P_i^A \equiv \langle DB_i^{Vulnerability} \rangle,$$

где $DB_i^{Vulnerability}$ – база данных уязвимостей, относящихся к i-ому Представлению, где содержатся в том числе их характеристики, необходимые для поиска (например, сигнатуры [27]); данная частная база данных входит в более общую, передаваемую в компонент поиска уязвимостей, которая может быть записана, как:

$$DB^{Vulnerability} \equiv \bigcup_i DB_i^{Vulnerability}.$$

Компонент управления деэволюцией программы Compoment^Control (от англ. Управление) и поиском уязвимостей может быть формально записан следующим образом:

$$Compoment^{Control} \equiv$$
$$\equiv \langle Module_{ControlDeevolution}, Module_{ControlFindVulnerability} \rangle,$$

где $Module_{ControlDeevolution}$ и $Module_{ControlFindVulnerability}$ – модули управления процессом деэволюции и поиска уязвимости, соответственно.

В простейшем случае, компонент управления последовательно запускает компоненты деэволюции исследуемого Представления, применяя для восстанавливаемых (т.е. предыдущих) Представлений компонент поиска уязвимостей, обновляя тем самым их множество; следовательно, он может быть записан следующим образом:

$$\langle R,V \rangle = Compoment^{Control}(\overline{Component^{Deevolution}}, \overline{Component^{FindVulnerability}}),$$

где R – множество всех восстановленных Представлений, а V – множество всех найденных уязвимостей, т.е.:

$$\begin{cases} R = \bigcup_i R_i \\ V = \bigcup_j V_j \end{cases}.$$

Естественно, каждый компонент может быть дополнен другими необходимыми модулями без нарушения общей схемы функционирования Системы. Например, возможно расширение компонента деэволюции дополнительными оптимизирующими алгоритмами на базе машинного обучения, используя информацию о соответствии конструкций Представлений [28], получаемых при прямом преобразовании в процессе классической работы ГА; компонент поиска уязвимостей может совместно со статическими методами применять и динамический анализ в виде псевдо-выполнения на виртуальной машине кода программы для выявления ее опасных действий [29]; управление же процессом РИ может происходить не только линейно, но итеративно, корректируя деэволюцию на более ранних Представлениях исхода из качества деэволюции на более поздних.

Следуя схеме (см. Рис. 1) и формализации ее элементов можно утверждать о реализуемости архитектуры, по крайне мере, в виде программного прототипа.

Заключение

Работа относится к заключительной части большого авторского исследования по созданию методологии и технологии генетического РИ программ, главным предназначением которого является поиск в них разноуровневых уязвимостей.

Основным результатом текущего этапа исследования является создание архитектуры генетического РИ программы, состоящей из совокупности последовательно выполняемых однотипных компонентов деэволюции ее Представлений – т.е. их расширяемого стека, а также компонентов поиска уязвимостей и управления процессом.

Новизна результата состоит как в программном высокоуровневом описании принципиально новой системы РИ, так и в формализации элементов ее архитектуры.

Теоретическая значимость результата заключается в расширении шаблонов проектирования программных решений для РИ, а практическая значимость – в возможности непосредственной реализации и применения системы генетического РИ с последующим поиском уязвимостей, основанных на авторских моделях, методах, алгоритмах и архитектуре.

Продолжением исследования будет последовательная реализация и проведение экспериментов для следующих полноценных прототипов: компонента генетической деэволюции для получения программы на языке С из ее МК, компонента дальнейшей деэволюции в алгоритмы программы, компонента поиска уязвимостей (с внешними алгоритмами анализа Представлений), компонента управления процессом, а также всей такой двух-деэволюционной системы. Успешность проведенных экспериментов подтвердит обоснованность всех научно-технических результатов, полученных авторами ранее, работоспособность их практических прототипов, а также существенную значимость системы генетического РИ для области информационной безопасности ПО.

Литература

1. *Леонов Н.В., Буйневич М.В. Проблемные вопросы поиска уязвимостей в программном обеспечении промышленных ИТ-устройств // Автоматизация в промышленности. 2023. № 12. С. 59–63.*
2. *Леонов Н.В. Противодействие уязвимостям программного обеспечения. Часть 1. Онтологическая модель // Вопросы кибербезопасности. 2024. № 2 (60). С. 87–92. DOI: 10.21681/2311-3456-2024-2-87-92.*
3. *Леонов Н.В. Противодействие уязвимостям программного обеспечения. Часть 2. Аналитическая модель и концептуальные решения // Вопросы кибербезопасности. 2024. № 3 (61). С. 90–95. DOI: 10.21681/2311-3456-2024-3-90-95.*
4. *Абитов Р.А., Павленко Е.Ю. Выявление уязвимостей в программном обеспечении для процессоров ARM с использованием символьного выполнения // Проблемы информационной безопасности. Компьютерные системы. 2021. № 3. С. 9–15.*
5. *Kotenko, I., Izrailov, K., Buinevich, M., Saenko I., Shorey R. Modeling the Development of Energy Network Software, Taking into Account the Detection and Elimination of Vulnerabilities // Energies. 2023. Vol. 16. Iss. 13. PP. 5111. DOI: 10.3390/en16135111.*
6. *Николаенко В.С. Сравнительный анализ обратной разработки проприетарных программ в зависимости от алгоритмического языка программирования // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет». 2022. Т. 1. № 14. С. 189–192.*
7. *Израилов К.Е. Концепция генетической деэволюции представлений программы. Часть 1 // Вопросы кибербезопасности. 2024. № 1 (59). С. 61–66. DOI: 10.21681/2311-3456-2024-1-61-66.*
8. *Израилов К.Е. Концепция генетической деэволюции представлений программы. Часть 2 // Вопросы кибербезопасности. 2024. № 2 (60). С. 81–86. DOI: 10.21681/2311-3456-2024-2-81-86.*
9. *Израилов К.Е. Концепция генетической декомпиляции машинного кода телекоммуникационных устройств // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 10–17. DOI:10.31854/1813-324X-2021-7-4-95-109.*
10. *Израилов К.Е. Применение генетических алгоритмов для декомпиляции машинного кода // Защита информации. Инсайд. 2020. № 3 (93). С. 24–30.*
11. *Аёшин И.Т. Реверс-инжиниринг программного продукта с использованием IDA Pro // Актуальные проблемы авиации и космонавтики. 2018. Т. 3. № 4 (14). С. 808–809.*
12. *Воробьев А.М., Боцвин А.С., Нагибин Д.В. Анализ функциональных возможностей Ghidra - фреймворка для реверс-инжиниринга // Методы и технические средства обеспечения безопасности информации. 2019. № 28. С. 86–88.*
13. *Бугеря А.Б., Ефимов В.Ю., Кулагин И.И., Падарян В.А., Соловьев М.А., Тихонов А.Ю. Программный комплекс для выявления недекларированных возможностей в условиях отсутствия исходного кода // Труды Института системного программирования РАН. 2019. Т. 31. № 6.С. 33–64. DOI: 10.15514/ISPRAS-2019-31(6)-3.*
14. *Израилов К.Е., Покусов В.В. Архитектура программной платформы преобразования машинного кода в высокоуровневое представление для экспертного поиска уязвимостей // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2021. № 6. С. 93–111.*
15. *Голубева Т.В., Тайлаков В.А., Василенко К.Д., Якубова Е.А. Исследование архитектуры прототипов средств для автоматического поиска уязвимостей в устройствах IOT и M2M // Вестник Алматинского университета энергетики и связи. 2022. № 2 (57). С. 122–134. DOI: 10.51775/2790-0886_2022_57_2_122.*
16. *Urooj B., Shah M.A., Maple C., Abbasi M.K., Riasat S. Malware Detection: A Framework for Reverse Engineered Android Applications Through Machine Learning Algorithms // IEEE Access. 2022. Vol. 10. PP. 89031-89050 2022. DOI: 10.1109/ACCESS.2022.3149053.*
17. *Mauthe N., Kargén U., Shahmehri N. A Large-Scale Empirical Study of Android App Decompilation // In proceedings of IEEE International Conference on Software Analysis, Evolution and Reengineering (Honolulu, HI, USA, 09-12 March 2021). 2021. PP. 400–410. DOI: 10.1109/SANER50967.2021.00044.*
18. *Armengol-Estapé J., Woodruff J., Cummins C., O'Boyle M.F.P. SLaDe: A Portable Small Language Model Decompiler for Optimized Assembly // In proceedings of IEEE/ACM International Symposium on Code Generation and Optimization (Edinburgh, United Kingdom, 02–06 March 2024). 2024. PP. 67-80. DOI: 10.1109/CGO57630.2024.10444788.*
19. *Armengol-Estapé J., Woodruff J., Brauckmann A., Magalhães J.W. de S. , O'Boyle M.F.P. ExeBench: an ML-scale dataset of executable C functions // In Proceedings of the 6th ACM SIGPLAN International Symposium on Machine Programming (New York, USA, 13 June 2022). 2022. PP. 50–59. DOI: 10.1145/3520312.3534867.*
20. *Aliefa M.H., Suyanto S. Variable-Length Chromosome for Optimizing the Structure of Recurrent Neural Network // In proceedings of International Conference on Data Science and Its Applications (Bandung, Indonesia, 05-06 August 2020). 2020. PP. 1–5. DOI: 10.1109/ICoDSA50139.2020.9213012.*
21. *Jiang W., Sha E.H.-M., Zhuge Q., Yang L., Dong H., Chen X. On the Design of Minimal-Cost Pipeline Systems Satisfying Hard/Soft Real-Time Constraints // IEEE Transactions on Emerging Topics in Computing. Vol. 9. No. 1. PP. 24–34. DOI: 10.1109/TETC.2017.2788800.*
22. *Леонов Н.В., Буйневич М.В. Машинное обучение vs поиск уязвимостей в программном обеспечении: анализ применимости и синтез концептуальной системы // Труды учебных заведений связи. 2023. Т. 9. № 6. С. 83–94. DOI: 10.31854/1813-324X-2023-9-6-83-94.*

23. Кубрин Г. С., Зегжда Д. П. Поиск уязвимостей программного обеспечения с применением ансабля алгоритмов анализа графов // Методы и технические средства обеспечения безопасности информации. 2023. № 32. С. 49–50.
24. Гетьман А. И., Горюнов М. Н., Мацкевич А. Г., Рыболовлев Д. А. Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации // Труды Института системного программирования РАН. 2022. Т. 34. № 5. С. 111–126. DOI: 10.15514/ISPRAS-2022-34(5)-7.
25. Пидченко И. А., Выборнова О. Н. Применение машинного обучения совместно с эвристическим анализом для задач антивирусного сканирования // Математические методы в технике и технологиях – ММТТ. 2020. Т. 5. С. 96–99.
26. Самарин Н. Н. Метод поиска ошибок в программном коде на базе фаззинга «в памяти» // Проблемы информационной безопасности. Компьютерные системы. 2024. № 2 (59). С. 130–137. DOI: 10.48612/jisp/39tp-t61k-29uv.
27. Иванов В. А., Конышев М. Ю., Шаповалов С. Л. Имитационная и аналитическая модели для исследования сигнатур и обнаружения модифицированных компьютерных вирусов и вредоносного программного обеспечения в вычислительных системах и сетях специального назначения // Информационная безопасность – актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. 2021. № 1 (14). С. 11–15.
28. Грибков Н. А., Овасапян Т. Д., Москвин Д. А. Анализ восстановленного программного кода с использованием абстрактных синтаксических деревьев // Проблемы информационной безопасности. Компьютерные системы. 2023. № 2 (54). С. 47–60. DOI: 10.48612/jisp/ruar-u6he-kmd4.
29. Довгалюк П. М., Климушенкова М. А., Фурсова Н. И., Степанов В. М., Васильев И. А., Иванов А. А., Иванов А. В., Бакулин М. Г., Егоров Д. И. Natch: определение поверхности атаки программ с помощью отслеживания помеченных данных и интроспекции виртуальных машин // Труды Института системного программирования РАН. 2022. Т. 34. № 5. С. 89–110. DOI: 10.15514/ISPRAS-2022-34(5)-6.

ARCHITECTURE OF THE SYSTEM FOR GENETIC REENGINEERING OF THE PROGRAM WITH SEARCH SUPPORT MULTI-LEVEL VULNERABILITIES

Izrailov K. E.[2]

Keywords: *reverse engineering, genetic algorithm, vulnerability, machine code, architecture, formalization.*

The goal of the investigation: *increasing the efficiency of searching for vulnerabilities in machine code of programs by reverse engineering it based on genetic reengineering, for which the architecture of the corresponding software system is proposed.*

Research methods: *works survey, system analysis, structural synthesis of architecture, analytical modeling.*

Result: *a system architecture has been created, which is a set of sequentially executed some-template components for the de-evolution of the representations of the program being investigated (its machine, assembler and source code, algorithms, etc.); on each of these representations, a search for corresponding vulnerabilities is carried out.*

The scientific novelty *consists in the qualitatively new development of the reverse engineering direction through its intellectualization, for which a high-level description of the author's genetic reengineering system architecture is proposed, and the formalization of the its elements functioning is also carried out.*

References

1. Leonov N. V., Bujnevich M. V. Problemnye voprosy poiska ujazvimostej v programmnom obespechenii promyshlennyh IT-ustrojstv // Avtomatizacija v promyshlennosti. 2023. № 12. S. 59–63.
2. Leonov N. V. Protivodejstvie ujazvimostjam programmnogo obespechenija. Chast' 1. Ontologicheskaja model' // Voprosy kiberbezopasnosti. 2024. № 2 (60). S. 87–92. DOI: 10.21681/2311-3456-2024-2-87-92.
3. Leonov N. V. Protivodejstvie ujazvimostjam programmnogo obespechenija. Chast' 2. Analiticheskaja model' i konceptual'nye reshenija // Voprosy kiberbezopasnosti. 2024. № 3 (61). S. 90–95. DOI: 10.21681/2311-3456-2024-3-90-95.
4. Abitov R. A., Pavlenko E. Ju. Vyjavlenie ujazvimostej v programmnom obespechenii dlja processorov ARM s ispol'zovaniem simvol'nogo vypolnenija // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2021. № 3. S. 9–15.
5. Kotenko, I., Izrailov, K., Buinevich, M., Saenko I., Shorey R. Modeling the Development of Energy Network Software, Taking into Account the Detection and Elimination of Vulnerabilities // Energies. 2023. Vol. 16. Iss. 13. PP. 5111. DOI: 10.3390/en16135111
6. Nikolaenko V. S. Sravnitel'nyj analiz obratnoj razrabotki proprietarnyh programm v zavisimosti ot algoritmicheskogo jazyka programmirovanija // Vestnik studencheskogo nauchnogo obshhestva GOU VPO «Doneckij nacional'nyj universitet». 2022. T. 1. № 14. S. 189–192.
7. Izrailov K. E. Koncepcija geneticheskoj dejevoljucii predstavlenij programmy. Chast' 1 // Voprosy kiberbezopasnosti. 2024. № 1 (59). S. 61–66. DOI: 10.21681/2311-3456-2024-1-61-66

2 Konstantin E. Izrailov, Ph.D., Docent, Senior Researcher of Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg. ORCHID: http://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56123238800. E-mail:konstantin.izrailov@mail.ru

8. *Izrailov K. E. Koncepcija geneticheskoj dejevoljucii predstavlenij programmy. Chast' 2 // Voprosy kiberbezopasnosti. 2024. № 2 (60). S. 81–86. DOI: 10.21681/2311-3456-2024-2-81-86*
9. *Izrailov K. E. Koncepcija geneticheskoj dekompiljacii mashinnogo koda telekommunikacionnyh ustrojstv // Trudy uchebnyh zavedenij svjazi. 2021. T. 7. № 4. S. 10–17. DOI:10.31854/1813-324X-2021-7-4-95-109.*
10. *Izrailov K. E. Primenenie geneticheskih algoritmov dlja dekompiljacii mashinnogo koda // Zashhita informacii. Insajd. 2020. № 3 (93). S. 24–30.*
11. *Ajoshin I. T. Revers-inzhiniring programmnogo produkta s ispol'zovaniem IDA Pro // Aktual'nye problemy aviacii i kosmonavtiki. 2018. T. 3. № 4 (14). S. 808–809.*
12. *Vorob'ev A. M., Bocvin A. S., Nagibin D. V. Analiz funkcional'nyh vozmozhnostej Ghidra – frejmvorka dlja revers-inzhiniringa // Metody i tehnicheskie sredstva obespechenija bezopasnosti informacii. 2019. № 28. S. 86–88.*
13. *Bugerja A. B., Efimov V. Ju., Kulagin I. I., Padarjan V. A., Solov'ev M. A., Tihonov A. Ju. Programmnyj kompleks dlja vyjavlenija nedeklarirovannyh vozmozhnostej v uslovijah otsutstvija ishodnogo koda // Trudy Instituta sistemnogo programmirovanija RAN. 2019. T. 31. № 6.S. 33–64. DOI: 10.15514/ISPRAS-2019-31(6)-3.*
14. *Izrailov K. E., Pokusov V. V. Arhitektura programmnoj platformy preobrazovanija mashinnogo koda v vysokourovnevoe predstavlenie dlja jekspertnogo poiska ujazvimostej // Jelektronnyj setevoj politematicheskij zhurnal «Nauchnye trudy KubGTU». 2021. № 6. S. 93–111.*
15. *Golubeva T. V., Tajlakov V. A., Vasilenko K. D., Jakubova E. A. Issledovanie arhitektury prototipov sredstv dlja avtomaticheskogo poiska ujazvimostej v ustrojstvah IOT i M2M // Vestnik Almatinskogo universiteta jenergetiki i svjazi. 2022. № 2 (57). S. 122–134. DOI: 10.51775/2790-0886_2022_57_2_122.*
16. *Urooj B., Shah M. A., Maple C., Abbasi M. K., Riasat S. Malware Detection: A Framework for Reverse Engineered Android Applications Through Machine Learning Algorithms // IEEE Access. 2022. Vol. 10. PP. 89031–89050 2022. DOI: 10.1109/ACCESS.2022.3149053.*
17. *Mauthe N., Kargén U., Shahmehri N. A Large-Scale Empirical Study of Android App Decompilation // In proceedings of IEEE International Conference on Software Analysis, Evolution and Reengineering (Honolulu, HI, USA, 09-12 March 2021). 2021. PP. 400–410. DOI: 10.1109/SANER50967.2021.00044.*
18. *Armengol-Estapé J., Woodruff J., Cummins C., O'Boyle M. F. P. SLaDe: A Portable Small Language Model Decompiler for Optimized Assembly // In proceedings of IEEE/ACM International Symposium on Code Generation and Optimization (Edinburgh, United Kingdom, 02–06 March 2024). 2024. PP. 67–80. DOI: 10.1109/CGO57630.2024.10444788.*
19. *Armengol-Estapé J., Woodruff J., Brauckmann A., Magalhães J. W. de S. , O'Boyle M. F. P. ExeBench: an ML-scale dataset of executable C functions // In Proceedings of the 6th ACM SIGPLAN International Symposium on Machine Programming (New York, USA, 13 June 2022). 2022. PP. 50–59. DOI: 10.1145/3520312.3534867.*
20. *Aliefa M. H., Suyanto S. Variable-Length Chromosome for Optimizing the Structure of Recurrent Neural Network // In proceedings of International Conference on Data Science and Its Applications (Bandung, Indonesia, 05-06 August 2020). 2020. PP. 1–5. DOI: 10.1109/ICoDSA50139.2020.9213012.*
21. *Jiang W., Sha E. H.-M., Zhuge Q., Yang L., Dong H., Chen X. On the Design of Minimal-Cost Pipeline Systems Satisfying Hard/Soft Real-Time Constraints // IEEE Transactions on Emerging Topics in Computing. Vol. 9. No. 1. PP. 24–34. DOI: 10.1109/TETC.2017.2788800.*
22. *Leonov N. V., Bujnevich M. V. Mashinnoe obuchenie vs poisk ujazvimostej v programmnom obespechenii: analiz primenimosti i sintez konceptual'noj sistemy // Trudy uchebnyh zavedenij svjazi. 2023. T. 9. № 6. S. 83–94. DOI: 10.31854/1813-324X-2023-9-6-83-94.*
23. *Kubrin G. S., Zegzhda D. P. Poisk ujazvimostej programmnogo obespechenija s primeneniem ansablja algoritmov analiza grafov // Metody i tehnicheskie sredstva obespechenija bezopasnosti informacii. 2023. № 32. S. 49–50.*
24. *Get'man A. I., Gorjunov M. N., Mackevich A. G., Rybolovlev D. A. Sravnenie sistemy obnaruzhenija vtorzhenij na osnove mashinnogo obuchenija s signaturnymi sredstvami zashhity informacii // Trudy Instituta sistemnogo programmirovanija RAN. 2022. T. 34. № 5. S. 111–126. DOI: 10.15514/ISPRAS-2022-34(5)-7.*
25. *Pidchenko I. A., Vybornova O. N. Primenenie mashinnogo obuchenija sovmestno s jevristicheskim analizom dlja zadach antivirusnogo skanirovanija // Matematicheskie metody v tehnike i tehnologijah – MMTT. 2020. T. 5. S. 96–99.*
26. *Samarin N. N. Metod poiska oshibok v programmnom kode na baze fazzinga «v pamjati» // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2024. № 2 (59). S. 130–137. DOI: 10.48612/jisp/39tp-t61k-29uv.*
27. *Ivanov V. A., Konyshev M. Ju., Shapovalov S. L. Imitacionnaja i analiticheskaja modeli dlja issledovanija signatur i obnaruzhenija modificirovannyh komp'juternyh virusov i vredonosnogo programmnogo obespechenija v vychislitel'nyh sistemah i setjah special'nogo naznachenija // Informacionnaja bezopasnost' – aktual'naja problema sovremennosti. Sovershenstvovanie obrazovatel'nyh tehnologij podgotovki specialistov v oblasti informacionnoj bezopasnosti. 2021. № 1 (14). S. 11–15.*
28. *Gribkov N. A., Ovasapjan T. D., Moskvin D. A. Analiz vosstanovlennogo programmnogo koda s ispol'zovaniem abstraktnyh sintaksicheskih derev'ev // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023. № 2 (54). S. 47–60. DOI: 10.48612/jisp/ruar-u6he-kmd4.*
29. *Dovgaljuk P. M., Klimushenkova M. A., Fursova N. I., Stepanov V. M., Vasil'ev I. A., Ivanov A. A., Ivanov A. V., Bakulin M. G., Egorov D. I. Natch: opredelenie poverhnosti ataki programm s pomoshh'ju otslezhivanija pomechennyh dannyh i introspekcii virtual'nyh mashin // Trudy Instituta sistemnogo programmirovanija RAN. 2022. T. 34. № 5. S. 89–110. DOI: 10.15514/ISPRAS-2022-34(5)-6.*

ПАТТЕРН ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИЛОЖЕНИЯ ПРИ УГРОЗЕ МОДИФИКАЦИИ МОДЕЛИ МАШИННОГО ОБУЧЕНИЯ

Корнеев Н. В.[1], Котрини Е. С.[2]

DOI: 10.21681/2311-3456-2025-1-117-127

Цель статьи: *разработка шаблонного механизма защиты для обеспечения безопасности приложения при угрозе модификации модели машинного обучения.*

Метод исследования: *анализ принципов проведения атак с искажением модели ML и возможностей нарушителя на этапе обучения модели. Синтез сценария атаки с помощью двух стратегий атаки: стратегии ввода данных и модификации данных модели ML. Основу модели ML сформировали на базе прогнозной модели Bank Customer Churn Prediction, а для угрозы был выбран внешний нарушитель, который способен изменить выборку данных для модели машинного обучения через сеть путем реализации сценария атаки отравления обучающих данных. С использованием методов криптографии предложен новый механизм защиты, обеспечивающий целостность дата-сета обучающих данных благодаря хешированию и хранению подписанных электронной цифровой подписью хэш-сумм. Исследование выполнено путем натурного моделирования приложения на основе Docker в средах с поддержкой контейнеризации, его развёртывания и тестирования при угрозе модификации модели машинного обучения.*

Результат: *проведен анализ угрозы модификации модели машинного обучения и показана актуальность проблемы разработки универсальных шаблонных механизмов безопасности, называемых паттернами. В частности, рассмотрены три применимые стратегии атаки для модификации модели машинного обучения, основанные на возможностях нарушителя – adversarial example, evasion attack, и модификации данных модели машинного обучения – adversarial example, evasion attack. Рассмотрен сценарий атаки отравления обучающих данных. Построена микросервисная архитектура для обеспечения безопасности приложения при угрозе модификации модели машинного обучения для широкого круга приложений в облачной инфраструктуре. Разработан паттерн безопасности для защиты приложения от атаки отравления обучающих данных на основе микросервисов, интегрированных в контейнеры и стека технологий: Java 17; Spring 5; Docker, docker-compose; PostgreSQL; RabbitMQ; Git; Log4j2; Logstash; Elasticsearch; Kibana; Swagger. В рамках проведённого исследования были разработаны 5 микросервисов: eureka – service, users – api, api – gateway, wrapper – api, config – server. С целью защиты данных, поступающих в модель машинного обучения, разработан микросервис wrapper – api. Механизм защиты заключается в том, что все вызовы к микросервису машинного обучения проходят через него и проверяются на факт порчи и/или подмены, данные, поступающие извне также проходят валидацию на стороне микросервиса. Перед добавлением в БД обучающих данных запись усиливается электронной подписью, происходит хэширование исходных данных, соединённых с секретным ключом. Разработан программный код микросервисов, включая коды специальных методов и алгоритмы их реализации, обеспечивающие механизм защиты приложения от атаки отравления обучающих данных. Развёрнута система мониторинга атаки отравления обучающих данных на базе открытого программного обеспечения Elasticsearch, Logstash, Kibana через объекты журнала событий (appender): ошибку (warn) и информирование (info), которая может быть использована в системах SIEM.*

Практическая ценность: *практическая значимость предлагаемого решения включает шаблонный механизм защиты в виде паттерна, который можно применить для широкого круга приложений, в том числе перенести разрабатываемое решение на любую отрасль: топливно-энергетическую, экономическую и не только, ввиду кроссплатформенности самого решения.*

Ключевые слова: *облачные вычисления, набор данных, шаблон, атака с искажением модели машинного обучения, состязательный пример, атака уклонения, каузативная атака, контейнер, машинное обучение, журнал событий, система мониторинга.*

Введение

Использование новых технологий, связанных с искусственным интеллектом и машинным обучением, активно применяется во многих областях деятельности человека. Новые алгоритмы помогают распознавать знаки дорожного движения, водить беспилотники, фильтровать спам, распознавать лица и т.д. Однако с развитием таких технологий встает вопрос об их безопасности и надежности. По мере роста потребления продуктов и услуг, созданных на основе машинного обучения, стало необходимо предпринимать специальные меры, чтобы защитить не только пользователей и их данные, но и сам искусственный интеллект и алгоритмы от нарушения их работоспособности.

1 Корнеев Николай Владимирович, доктор технических наук, доцент, РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия. E-mail: niccyper@mail.ru
2 Котрини Елена Сергеевна, студент РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия. E-mail: kotrini.elena@mail.ru

За последние годы многими исследователями было предложено и реализовано значительное количество работ, касающихся безопасности технологий, связанных с искусственным интеллектом и машинным обучением, например [1–6]. Однако пробелом остается разработка универсальных шаблонных механизмов безопасности, называемыми паттернами. В частности в данной статье мы ставим целью разработку шаблонного механизма защиты для обеспечения безопасности приложения при угрозе модификации модели машинного обучения.

Паттерн безопасности описывает конкретную повторяющуюся проблему безопасности, которая возникает в определенных известных контекстах, а также предлагает хорошо зарекомендовавшую себя общую схему решения такой проблемы безопасности.

Машинное обучение (ML) – это техника обучения информационной системы на основе предоставленных наборов данных (dataset) без использования предопределенных правил, является частным случаем искусственного интеллекта. Общей задачей машинного обучения является построение алгоритма (программы) на основании предоставленных входных данных и заданных верных результатов: таким образом, процесс работы ML-системы разделен на первоначальное обучение на предоставляемых наборах данных и на последующее принятие решений уже обученной системой.

Системы машинного обучения напрямую зависят от данных. Изменение данных, в свою очередь, изменяет работу модели. Однако модели машинного обучения всегда обучаются на некотором подмножестве данных – тренировочном наборе (dataset). А уже затем на этапе эксплуатации модель встречается с реальными данными из генеральной совокупности. И вот эти данные могут по своим характеристикам отличаться от тех, на которых модель обучалась и тренировалась. Изменение данных приводит к модификации работы модели и появления угрозы безопасности информации.

Согласно банку угроз безопасности информации ФСТЭК России, такая угроза безопасности информации называется УБИ 221. Она может быть осуществлена внешним нарушителем (с высоким потенциалом) или внутренним нарушителем (со средним или высоким потенциалом) путем искажения («отравления») обучающих данных. Угроза обусловлена недостатками алгоритмов машинного обучения и осуществления процесса машинного обучения. Реализация угрозы возможна при наличии у нарушителя возможности воздействовать на процесс машинного обучения.

Анализ и методы исследования

Атаки с искажением модели ML (Poisoning Attack) [7] представляют собой целенаправленное злоумышленное изменение данных во время машинного обучения для компрометации всего процесса машинного обучения. Анализ возможностей нарушителя на этапе обучения состоят в следующем. Нарушитель пытается модифицировать модель ML, изменяя набор данных, используемый для обучения. Сценарий атаки включает доступ к частичным или полным данным обучения. На сегодня выделяются две применимые стратегии атаки для модификации модели ML, основанные на возможностях нарушителя – это стратегии ввода данных и модификации данных модели ML.

Стратегия ввода данных реализуется через состязательный пример (adversarial example) [8] или через атаку уклонения (evasion attack) [9]. Она используется, когда нарушитель не имеет никакого доступа к обучающим данным, а также к алгоритму обучения, но имеет возможность добавить новые данные в обучающий набор. Нарушитель может исказить целевую модель ML, вставив ложные выборки в обучающий набор данных. Например, к изображению он может добавить специально подобранный незначительный шум, после чего результат предсказания модели полностью изменится. Это влечет за собой некорректность работы приложения с использованием модели машинного обучения.

Стратегия модификации данных используется, когда нарушитель не имеет доступа к алгоритму обучения, но имеет полный доступ к обучающим данным. Атаки с изменением обучающих данных носят название атак отравления (data poisoning) [10], или каузативных атак (causative attack) [11]. В этом случае нарушитель напрямую искажает обучающие данные, например, путем прямого изменения меток обучающих данных, изменяя их до того, как они будут использованы целевой моделью ML. С помощью подобной атаки он воздействует на рабочую модель в процессе обучения с целью влияния на ее дальнейшее поведение. Благодаря такому подходу нарушитель может опубликовать неверные данные для искажения рабочих процессов в приложении. Стоит также отметить, что данная угроза особенно серьёзна в связи с тем, что многие разработчики ML-решений, включая крупных производителей систем безопасности, используют публичные обучающие выборки, которые могут быть легко «отравлены» третьими сторонами. Соответственно, изменение этих данных повлечет за собой некорректность работы приложений, созданных на основе обученной модели ML.

Для ограничения зоны применимости разрабатываемого шаблонного механизма защиты определим, что нами будет рассматривается приложение

Рис. 1. Сценарий атаки отравления обучающих данных

для компании, оказывающей финансовые услуги, например, банк, который использует модель ML для прогнозирования оттока клиентов. Основу модели ML сформируем на базе прогнозной модели Bank Customer Churn Prediction [12], разработанной сообществом специалистов Kaggle. Выбор модели обусловлен ее широким применением на практике. Данная модель будет анализировать поведение клиентов, исходя из их транзакций, активности, истории обращений и других факторов, чтобы предсказать вероятность того, что клиент может уйти из банка в ближайшем будущем. В качестве входных данных будут использованы следующие переменные с типами данных: CreditScore – int64, Geography – object, Gender – object, Age – int64, Tenure – int64, Balance – float64, NumOfProducts – int64, HasCrCard – int64, IsActiveMember – int64, EstimatedSalary – float64, Exited – int64, dtype – object. На основании этих данных модель машинного обучения должна предсказать, что 20% клиентов уйдут из банка [12].

Идентификация клиентов, которые склонны к оттоку, позволяет банку принимать меры по их удержанию. Раннее обнаружение потенциальных уходящих клиентов позволяет банку предпринимать действия для совершенствования опыта обслуживания, предлагать персонализированные услуги или бонусов для уменьшения оттока и удержания клиентов.

В статье в качестве угрозы был выбран внешний нарушитель, который способен изменить выборку данных для модели машинного обучения через сеть. В качестве внешнего нарушителя будем рассматривать сотрудника банка имеющего доступ к БД обучающих данных (рис. 1). Рассмотрим сценарий атаки отравления обучающих данных, когда нарушитель подменит обучающие данные, например, внедрив неверные или искаженные данные о клиентах, то это приводит к искажению прогнозов модели.

Нарушитель изменяет данные о поведении клиентов, чтобы модель считала, что надежные клиенты склонны к оттоку, или наоборот. В результате банк

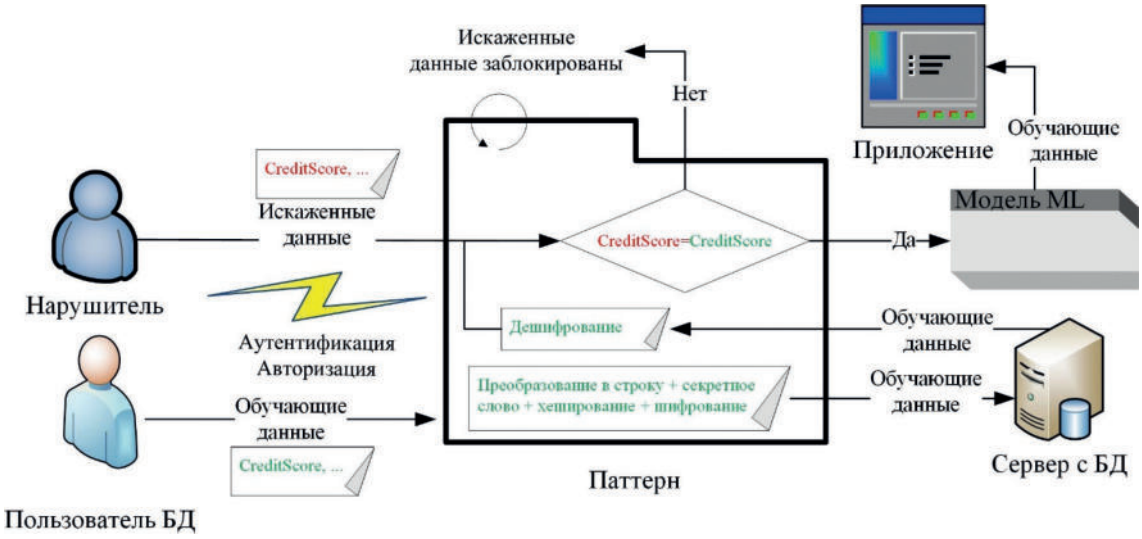


Рис. 2. Сценарий защиты приложения от атаки отравления обучающих данных

принимает неправильные решения на основе искаженных прогнозов, например, направляет усилия на удержание клиентов, которые на самом деле не собираются уходить, или наоборот, упускает возможности предотвратить отток уязвимых клиентов. В свою очередь это приведет к финансовым потерям для банка, ухудшению качества обслуживания клиентов, потере доверия со стороны клиентов и ущербу репутации банка. Поэтому важно обеспечить безопасность данных, использованных для обучения модели машинного обучения, чтобы избежать подобных проблем и сохранить качество работы модели.

Для решения данной проблемы необходимо реализовать паттерн безопасности, включающий в себя механизм защиты приложения (рис. 2), Механизм защиты строится на применении методов криптографии. Так, целостность дата-сета обучающих данных будет обеспечена благодаря хешированию и хранению подписанных электронной цифровой подписью хэш-сумм.

На рис. 2 видно, что обучающие данные проходят операцию хеширования, т.е. преобразования массива входных данных произвольной длины в выходную битовую строку установленной длины. В таком процессе генерации применяется набор методов хеширования с использованием математических формул (хеш-функций). Суть процесса заключается в том, что определенные данные проходят проверку на их соответствие оригиналу, причем сам подлинник в этом действии не участвует. При сравнении информации оценивается идентичность хеш-значений. Важно упомянуть, что при любом изменении данных (например, изменении слова), хеш-значение также изменится, что позволит обнаружить действия нарушителя и сообщить о компрометации целостности. В этом случае искаженные данные будут заблокированы.

Разрабатываемый нами паттерн может быть использован не только для защиты описанного приложения, но и в более широком контексте – для обеспечения безопасности приложений в целом, например, в системе SIEM (Security Information and Event Management).

Новизна предлагаемого решения определяется возможностью обеспечения безопасности приложения при угрозе модификации модели машинного обучения в облачной информационной инфраструктуре России при переходе на импортозамещение.

Практическая значимость предлагаемого решение включает шаблонный механизм защиты в виде паттерна, который можно применить для широкого круга приложений, в том числе перенести разрабатываемое решение на любую отрасль: топливно-энергетическую, экономическую и не только, ввиду кроссплатформенности самого решения.

Паттерн безопасности для приложения

Для реализации паттерна использован следующий стек технологий: Java 17; Spring 5; Docker, docker-compose; PostgreSQL; RabbitMQ; Git; Log4j2; Logstash; Elasticsearch; Kibana; Swagger. Паттерн безопасности (рис. 3) построен на основе микросервисной архитектуры. За основу взят язык Java, основной фреймворк – Spring, в частности, Spring Cloud, необходимый для создания систем, на основе микросервисной архитектуры.

Все входящие HTTP запросы проходят и обрабатываются в шлюзе, который создан на основе Spring Cloud Gateway, который также выступает в роли балансировщика нагрузки (Load balancer) для распределения трафика между несколькими экземплярами одного и того же микросервиса (рис. 3). На уровне шлюза отрабатывает фильтр авторизации (gateway), который пропускает неавторизованные запросы

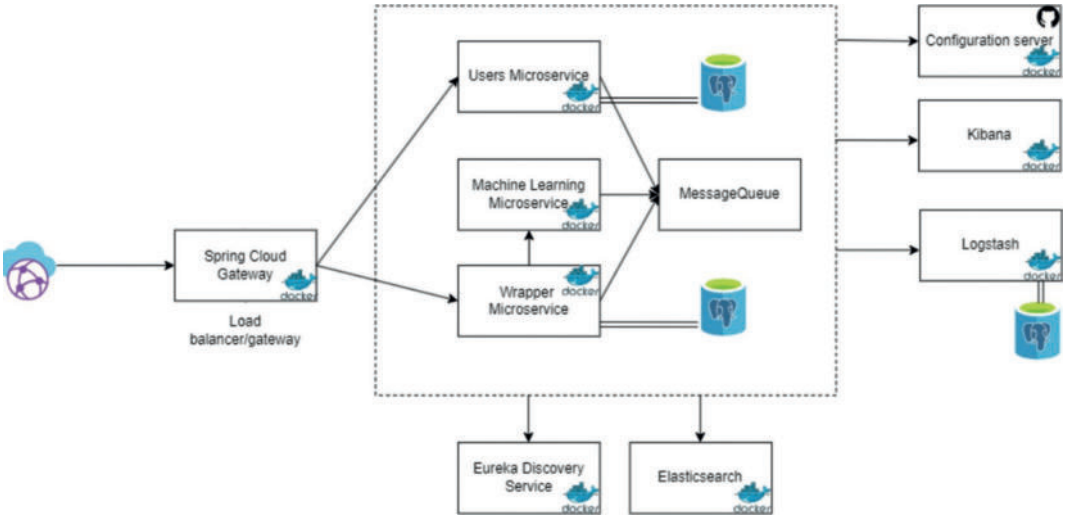


Рис. 3. Микросервисная архитектура паттерна безопасности для приложения

только на те URI, которые необходимы для прохождения аутентификации и авторизации, т.е. работает на JSON Web Token (JWT) аутентификации [13].

За аутентификацию и авторизацию пользователей отвечает пользовательский микросервис (Users Mircoservice). Работа последнего основана на части Spring framework – Spring Security, работающего в режиме Stateless аутентификации, т.е. без хранения сессии пользователя и без назначения cookies. Выбор сделан в пользу JWT, так как для работы в Statefull режиме сессия должна храниться на каждом сервисе, и все они должны обновляться синхронно, что затратно в плане памяти и быстродействия. Данный сервис хранит информацию о пользователях в базе данных PostgreSQL, конфиденциальные данные пользователя шифруются при помощи класса шифрования, интегрированного в Spring Security – BCryptPasswordEncouder.

Микросервис машинного обучения (Machine Learning Mircoservice) отвечает за генерацию предсказаний о заинтересованности того или иного клиента в дальнейшем использовании услуг банка. Модель ML предварительно обучается на заготовленном наборе данных.

С целью защиты данных, поступающих в модель ML, разработан отдельный микросервис на основе паттерна проектирования Wrapper. Механизм защиты заключается в том, что все вызовы к микросервису машинного обучения проходят через него. За счёт этого появляется возможность реализации предварительных проверок поступающих данных на факт порчи и/или подмены. Кроме того, данные, поступающие извне, также проходят валидацию на стороне микросервиса. Вместе с этим перед добавлением данных в БД обучающих данных запись усиливается электронной подписью, то есть, происходит хэширование исходных данных, соединённых с секретным ключом. За счёт добавления данного микросервиса появляется прослойка между данными и моделью ML, способствующая защите данных, а также контролю над ними.

За отправку асинхронных сообщений отвечает микросервис MessageQueue, в паттерне такая функциональность необходима только во время обновления конфигурации, то есть при изменении файлов конфигурации на сервере конфигурации в очередь отправляется сообщение о необходимости повторного чтения файлов свойств; сервисы, подписанные на данную очередь, получают данное сообщение и выполняют обновление. Это позволяет выполнять обновление свойств приложения в горячем режиме, то есть без необходимости останавливать работу кластера, на котором развернуты микросервисы. В качестве брокера сообщений выбран RabbitMQ [14], так как в условиях рассматриваемого сценария атаки нет необходимости создавать шину данных, а достаточно простой пересылки асинхронных сообщений.

Вместе с сервисом отправки асинхронных сообщений стоит упомянуть сервис, отвечающий за конфигурацию всей системы (паттерн и приложение). С целью облегчения конфигурирования принято решение вынести все файлы свойств каждого микросервиса, а также общие настройки в приватный Git репозиторий. Для работы с ним используется микросервис ConfigurationServer, который основан на Spring Cloud Config Server. За счёт последнего осуществляется считывание данных из репозитория и их чтения микросервисами. Также именно эта структура отвечает за обновление конфигурации в горячем режиме.

Для агрегации логирования в едином месте и наблюдения за состоянием системы будет использован ряд микросервисов, основанных на стеке ELK – Elasticsearch, Logstash, Kibana [15]. Каждый микросервис в системе генерирует свой файл логов. Для удобства работы необходимо агрегировать все файлы журнала в одном месте, для этого используется Logstash. Он собирает файлы журнала, сортирует их, фильтрует и отправляет выше по цепочке в Elasticsearch, который, в свою очередь, индексирует файлы журнала и сохраняет их. Kibana позволяет визуализировать полученные данные. Чтобы собирать данные с каждого микросервиса, используется библиотека log4j2, предоставляющая функционал для журналирования. Все указанное в совокупности дает возможность реализовать мониторинг атаки отравления обучающих данных.

Ещё один микросервис, необходимый для функционирования всей системы – Eureka Discovery Service. Данный микросервис был разработан нами для регистрации всех остальных микросервисов и обеспечения связи между ними, а также он даёт возможность контролировать состояние каждого микросервиса.

Таким образом, согласно сценарию защиты (рис. 2) система развёрнута в облаке, на распределяющем сервере установлена защита от вредоносного трафика (Firewall), таких как DDoS, DoS, ReDoS, SSI. Группа пользователей, включая нарушителя, взаимодействуют с системой при помощи сетевых устройств связи, те, в свою очередь, отправляют HTTP запрос, который приходит на локальный маршрутизатор, где, в свою очередь, происходит преобразование доменного имени по протоколу DNS в IP-адрес распределяющего сервера. После прохождения запроса через защиту последний попадает на сетевой балансировщик нагрузки (в рассматриваемом примере – это

один и тот же микросервис), который используется для маршрутизации TCP-трафика (трафика четвертого уровня OSI). Они работают на транспортном уровне и способны принимать решения о маршрутизации на основе IP-адреса и номера порта запроса. Последние зачастую используются в облачных средах.

После прохождения через балансировщик нагрузки запрос попадает на наименее загруженную ноду кластера. Физически все ноды представлены кластером серверов, а количество вычислительных машин на базе одного кластера в каждом конкретном случае определяется нагрузкой [16]. Все ноды повторяют друг друга и внутри представлены сущностью микросервиса, каждый из которых работает под управлением docker-compose. Он, в свою очередь, организует взаимодействие между микросервисами, отвечает за их дублирование и непрерывную работу. Все микросервисы представлены Docker контейнерами, которые обеспечивают изолированную работу сервисов друг от друга, также на базе каждой ноды работает Logstash, Kibana, Elasticsearch, необходимые для отслеживания работы приложения.

К каждой машине можно получить доступ при помощи ssh тунеля, который позволяет получить доступ к удалённой машине с любого устройства, на котором есть необходимые ssh ключи. Все ноды работают с базами данных, которые представлены отдельным кластером, в данном случае шардирование базы данных не используется по причине отсутствия значительной нагрузки на узел данных.

Разработка сервисов паттерна безопасности

В рамках проведённого исследования были разработаны 5 микросервисов: eureka – service, users – api, api – gateway, wrapper – api, config – server. В дальнейшем мы более подробно рассмотрим только один из них – wrapper – api, так как именно он обеспечивает основной механизм защиты данных, поступающих в модель ML от атаки отравления обучающих данных.

Микросервис eureka – service является основным. Он отвечает за регистрацию всех остальных сервисов и обеспечивает связь между ними, а также даёт возможность контролировать состояние каждого микросервиса. Остальные сервисы – вспомогательные. Без них работа первого невозможна.

Микросервис config – service предоставляет конфигурацию для всех остальных микросервисов. Все конфигурации лежат на удаленном git – репозитории.

Микросервис api – gateway – это шлюз, через который проходят все запросы в систему. Он откидывает все неавторизованные запросы, то есть те, у которых токен либо неверный, либо его нет, и пропускает запросы только на сервис, который авторизует пользователей. Как только пользователь получает этот токен, он может проходить дальше. Код этого сервиса содержит только описание фильтра JwtAuthorizationFilter. Этот фильтр отвечает за авторизацию пользователей, используя JWT. Он обеспечивает безопасность системы, отклоняя неавторизованные запросы и проверяя валидность JWT токенов перед передачей запросов дальше по цепочке обработки.

Микросервис user – api выполняет функцию управления пользователями в системе, обеспечивая регистрацию пользователей, аутентификацию и авторизацию, а также предоставляя доступ к защищенным ресурсам с помощью JWT токенов.

Микросервис wrapper – api включает в себя:

1. класс DataRouterController – это контроллер, который отвечает за обработку HTTP запросов;
2. класс PersonDTO – это DTO (Data Transfer Object), который представляет данные пользователя. Он содержит поля, соответствующие определенным нами ранее входным данным: кредитный рейтинг (CreditScore), страна проживания (Geography), пол (Gender), возраст (Age) и т.д.;
3. класс PersonDTOBuilder – это строитель для объекта PersonDTO. Он предоставляет методы для установки различных полей объекта PersonDTO поэтапно;
4. класс EncryptedPerson представляет модель данных, которая описывает сущность «зашифрованный пользователь» в контексте базы данных. Модель содержит поля, которые соответствуют атрибутам зашифрованного пользователя, таким как CreditScore, Geography, Gender, Age и т.д. Модель используется для работы с данными в базе данных, выполнения операций CRUD (создание, чтение, обновление, удаление) и отображения данных в приложении;
5. класс EncryptedPersonBuilder – это строитель для объекта EncryptedPerson;
6. классы ошибок (Exeptions), которые могут быть в процессе выполнения программы;
7. класс EncryptedPeopleRepository – это репозиторий, который используется для взаимодействия с базой данных и выполнения операций CRUD сущностей типа EncryptedPerson;
8. классы ответов Responses: IntegrityViolationOfDataResponse – класс, который представляет ответ на ситуацию, когда происходит нарушение целостности данных; NoSuchPersonResponse – класс представляет ответ на ситуацию, когда запрашиваемый пользователь не найден; PersonNotValidResponse – класс представляет ответ на ситуацию, когда данные пользователя не прошли валидацию; PersonSaveProcessingResponse –класс представляет ответ на ситуацию, когда возникает ошибка при обработке сохранения данных пользователя;

9. PeopleService – это класс контроллера принятия запроса на добавление пользователя, и его обработку;

Класс PeopleService включает в себя два основных метода: addPerson(PersonDTO person) и getPerson(long id).

Код метода addPerson(PersonDTO person):

```
public void addPerson(PersonDTO person) {
   EncryptedPerson personToAdd;
   try {
      personToAdd = messageCoder.
      code(person);
      encryptedPeopleRepository.
      save(personToAdd);
   } catch (RuntimeException e) {
      logger.error(e.getCause().
      getMessage());
      throw e;
   }
}
```

Метод addPerson(PersonDTO person) принимает объект PersonDTO, что представляет данные о пользователе, которого необходимо добавить. Сначала данные пользователя кодируются с помощью объекта messageCoder, чтобы зашифровать информацию о пользователе. Затем зашифрованные данные сохраняются в базе данных с помощью метода save() репозитория encryptedPeopleRepository. В случае возникновения исключения при сохранении данных ошибка логируется и исключение пробрасывается дальше.

Код метода getPerson(long id):

```
public PersonDTO getPerson(long id) {
   EncryptedPerson person =
   encryptedPeopleRepository.findById(id).
   orElseThrow(
      () -> new NoSuchPersonException
      (String.format("Person with id %d not
      found", id))
   );
   Optional<PersonDTO> personToReturn;
   try {
      personToReturn = messageDecoder.
      decode(person);
   } catch (RuntimeException e) {
      throw new IntegrityViolationOfData
      Exception(String.format("Person with
      id %d has data violation", id));
   }
        return personToReturn.get();
}
```

Метод getPerson(long id) принимает уникальный идентификатор пользователя (id) и возвращает информацию о пользователе. Сначала происходит поиск зашифрованных данных пользователя в базе данных по id с помощью метода findById() репозитория encryptedPeopleRepository. Если пользователь не найден, выбрасывается исключение NoSuchPersonException. Затем зашифрованные данные декодируются с помощью объекта messageDecoder, чтобы получить исходные данные пользователя. В случае возникновения ошибки при декодировании данных выбрасывается исключение IntegrityViolationOfDataException и информация о пользователе возвращается в виде объекта PersonDTO.

10. класс MessageCoder отвечает за шифрование данных объекта PersonDTO в объект EncryptedPerson, чтобы сохранить его в базе данных;

Основной метод класса MessageCoder – метод code(PersonDTO dto), который принимает объект PersonDTO и возвращает зашифрованный объект EncryptedPerson. Код метода code(PersonDTO dto):

```
public EncryptedPerson code(PersonDTO dto) {
   KeyStore keyStore; //Private key
   loading PrivateKey privateKey;
   try {
      keyStore= KeyStore.getInstance
      ("PKCS12");
      char[] passwordToKeyFile =
      environment.getProperty("encryption.
      passwordToPrivateKeyFile").
      toCharArray();
   keyStore.load(new FileInputStream("../
   wrapper-api/src/main/resources/sender_
   keystore.p12"), passwordToKeyFile);
      privateKey =
         (PrivateKey) keyStore.getKey
         ("senderKeyPair", passwordToKey
         File);
   } catch (IOException | NoSuchAlgorithm
      Exception | CertificateException |
      KeyStoreException |
         UnrecoverableKeyException e) {
      throw new RuntimeException(e);}
```

В методе реализуется следующий алгоритм:

1. загружается закрытый ключ (privateKey) из хранилища ключей (KeyStore);
2. объект PersonDTO преобразуется в строку (string ToEncrypt) с помощью метода toString();
3. Генерируется хеш сообщения (messageHash) из строки stringToEncrypt с использованием алгоритма SHA-256;
4. хеш сообщения шифруется с помощью закрытого ключа (privateKey) и алгоритма RSA с использованием объекта Cipher;
5. полученная цифровая подпись (digitalSignature) преобразуется в строку и сохраняется в поле signature объекта EncryptedPerson;
6. создается объект EncryptedPerson с зашифрованными данными и возвращается в качестве

результата метода, а впоследствии этот объект будет добавлен в БД.

11. класс MessageDecoder отвечает за декодирование зашифрованных данных объекта EncryptedPerson, которые хранятся в базе данных, а также за проверку подлинности цифровой подписи.

Основной метод класса MessageDecoder – метод decode(EncryptedPerson encryptedPerson), который получает зашифрованный объект EncryptedPerson из базы данных и возвращает объект PersonDTO после декодирования.

В методе реализуется следующий алгоритм:

1. загружается открытый ключ (publicKey) из хранилища ключей (KeyStore);
2. зашифрованная цифровая подпись (encryptedMessageHash) декодируется из объекта EncryptedPerson. Таким образом, она декодируется из формата Base64 в виде строки;
3. расшифровывается подпись с использованием открытого ключа (publicKey) и алгоритма RSA с помощью объекта Cipher. Получается дешифрованный хеш (decryptedMessageHash);
4. вычисляется хеш (messageHash) строки объекта EncryptedPerson;
5. сравнивается дешифрованный хеш с вычисленным хешем для проверки подлинности данных;
6. если подпись корректна, создается объект PersonDTO на основе данных объекта EncryptedPerson с помощью PersonDTOBuilder;
7. возвращается объект PersonDTO, если подпись верна, иначе логируется ошибка валидации подписи.

Мониторинг атаки отравления обучающих данных и обсуждение результатов

Была разработана система мониторинга атаки отравления обучающих данных, основанная на стеке ELK [17]. Рассмотрим логику работы этой системы: все микросервисы пишут свои логи либо через стандартный логгер от spring – logback, либо через log4j2. Данные логгеры конфигурируются следующим образом: добавляется один объект журнала событий (appender), который отправляет логи на host logstash, на порт 5000, один appender – стандартный, в консоль, порог логов для первого appender выставляется на ошибку (warn), для второго – информирование (info).

Для отображения этой информации необходимо настроить logstash, в нём необходимо указать, что логи будут приходить на порт 5000, а отправляются на хост elasticsearch, порт 9200, в формате json. Также нужно явно указать, что logstash будет слушать подключения от всех хостов, не только от локального.

На этом этапе важно убедиться, что в docker – compose данные микросервисы находятся в одной сети, иначе логи не будут доходить до logstash, а затем до elasticsearch. В настройках kibana нужно указать, что необходимо слушать подключения на порт 5601, а также явно указать, где находится elasticsearch, хост и порт, соответственно. Таким образом, мы получаем рабочую систему агрегации логов. Для просмотра графиков необходимо перейти на хост, на котором запущен кластер ELK, на порт 5601. Таким образом будет получен доступ к графическому интерфейсу kibana. Далее необходимо настроить data view, представления данных, перейдя на вкладку index management мы увидим, что основные микросервисы начали писать свои логи (рис. 4). На рис. 4 показан журнал и графики логов для микросервиса users – api.

Анализ журнала и графиков логов в режиме реального времени позволяет видеть попытки атак отравления обучающих данных через информирование (info) и ошибки (warn). Метрики этих ошибок могут быть настроены более гибко через соответствующие события, например, для метода addPerson(PersonDTO person) в случае возникновения исключения при сохранении данных; для метода getPerson(long id) в случае возникновения ошибки при декодировании данных на основе исключения IntegrityViolationOfDataException; для метода decode(EncryptedPerson encryptedPerson) в случае когда логируется ошибка валидации подписи.

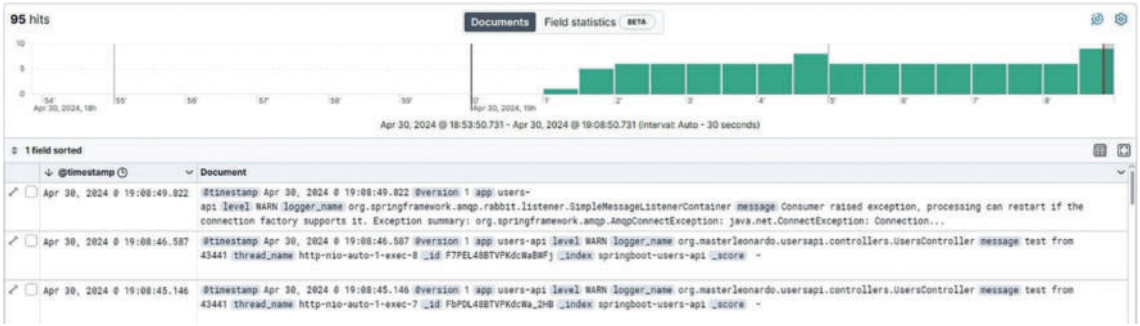


Рис. 4. Витрина с результатами мониторинга микросервиса users – api

Выводы

Построена микросервисная архитектура для обеспечения безопасности приложения при угрозе модификации модели машинного обучения для широкого круга приложений в облачной инфраструктуре. Рассмотрен сценарий атаки отравления обучающих данных. Разработан паттерн безопасности для защиты приложения от атаки отравления обучающих данных на основе микросервисов, интегрированных в контейнеры. В рамках проведённого исследования были разработаны 5 микросервисов: eureka – service, users – api, api – gateway, wrapper – api, config – server. С целью защиты данных, поступающих в модель ML, разработан микросервис wrapper – api. Механизм защиты заключается в том, что все вызовы к микросервису машинного обучения проходят через него и проверяются на факт порчи и/или подмены, данные, поступающие извне, также проходят валидацию на стороне микросервиса. Перед добавлением данных в БД обучающих данных запись усиливается электронной подписью, происходит хэширование исходных данных, соединённых с секретным ключом. Разработан программный код микросервисов, включая коды специальных методов и алгоритмы их реализации, обеспечивающих механизм защиты приложения от атаки отравления обучающих данных. Развёрнута система мониторинга атаки отравления обучающих данных на базе открытого программного обеспечения через объекты журнала событий (appender): ошибку (warn) и информирование (info), которые могут быть использованы в системах SIEM. Метрики этих ошибок могут быть гибко настроены через соответствующие события специальных методов, что дает возможность гибко настраивать сам паттерн и применять его для широкого круга приложений.

Литература

1. *Shameer Mohammed, S. Nanthini, N. Bala Krishna, Inumarthi V. Srinivas, Manikandan Rajagopal, M. Ashok Kumar, A new lightweight data security system for data security in the cloud computing, Measurement: Sensors, Volume 29, 2023, 100856. DOI: 10.1016/j.measen.2023.100856.*
2. *S. Achar, Cloud computing security for multi-cloud service providers: controls and techniques in our modern threat landscape, International Journal of Computer and Systems Engineering, 16(9), 2022, 379–384. DOI: 10.5281/zenodo.7084251.*
3. *Oludare Isaac Abiodun, Moatsum Alawida, Abiodun Esther Omolara, Abdulatif Alabdulatif, Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey, Journal of King Saud University – Computer and Information Sciences, Volume 34, Issue 10, Part B, 2022, 10217–10245. DOI: 10.1016/j.jksuci.2022.10.018.*
4. *Chakraborti, A., Curtmola, R., Katz, J., Nieh, J., Sadeghi, A. R., Sion, R., Zhang, Y., Cloud Computing Security: Foundations and Research Directions. Foundations and Trends in Privacy and Security, 3(2), 2022, 103–213. DOI: 10.1561/3300000028.*
5. *Ukeje, N., Gutierrez, J., Petrova, K., Information security and privacy challenges of cloud computing for government adoption: a systematic review, International Journal of Information Security, Volume 23, 2024, 1459–1475. DOI: 10.21203/rs.3.rs-3351319/v1.*
6. *Fatemeh Khoda Parast, Chandni Sindhav, Seema Nikam, Hadiseh Izadi Yekta, Kenneth B. Kent, Saqib Hakak, Cloud computing security: A survey of service-based models, Computers & Security,Volume 114, 2022, 102580. DOI: 10.1016/j.cose.2021.102580.*
7. *Ting Zhou, Hanshu Yan, Bo Han, Lei Liu, Jingfeng Zhang, Learning a robust foundation model against clean-label data poisoning attacks at downstream tasks, Neural Networks, Volume 169, 2024, 756–763. DOI: 10.1016/j.neunet.2023.10.034.*
8. *Ade Kurniawan, Yuichi Ohsita, Masayuki Murata, Detection of sensors used for adversarial examples against machine learning models, Results in Engineering, Volume 24, 2024, 103021. DOI: 10.1016/j.rineng.2024.103021.*
9. *Hamid Bostani, Veelasha Moonsamy, EvadeDroid: A practical evasion attack on machine learning for black-box Android malware detection, Computers & Security, Volume 139, 2024, 103676. DOI: 10.1016/j.cose.2023.103676.*
10. *Mahdee Jodayree, Wenbo He, Dr. Ryszard Janicki, Preventing Image Data Poisoning Attacks in Federated Machine Learning by an Encrypted Verification Key, Procedia Computer Science, Volume 225, 2023, 2723–2732. DOI: 10.1016/j.procs.2023.10.264.*
11. *Michael Gallagher, Nikolaos Pitropakis, Christos Chrysoulas, Pavlos Papadopoulos, Alexios Mylonas, Sokratis Katsikas, Investigating machine learning attacks on financial time series models, Computers & Security, Volume 123, 2022, 102933. DOI: 10.1016/j.cose.2022.102933.*
12. *Pahul Preet Singh, Fahim Islam Anik, Rahul Senapati, Arnav Sinha, Nazmus Sakib, Eklas Hossain, Investigating customer churn in banking: a machine learning approach and visualization app for data science and management, Data Science and Management, Volume 7, Issue 1, 2024, 7–16. DOI: 10.1016/j.dsm.2023.09.002.*
13. *Badr Eddine Sabir, Mohamed Youssfi, Omar Bouattane, Hakim Allali, Authentication and load balancing scheme based on JSON Token For Multi-Agent Systems, Procedia Computer Science, Volume 148, 2019, 562–570. DOI: 10.1016/j.procs.2019.01.029.*
14. *Esquembre F., Chacón J., Saenz J., Vega J., Dormido-Canto S., A programmable web platform for distributed access, analysis, and visualization of data, Fusion Engineering and Design, Volume 197, 2023, 114049. DOI: 10.1016/j.fusengdes.2023.114049.*
15. *Dongyeop Lee, Daesik Lim, Jongseok Park, Soojeong Woo, Youngho Moon, Aesol Jung, Management Architecture With Multimodal Ensemble AI Models for Worker Safety, Safety and Health at Work, Volume 15, Issue 3, 2024, 373–378. DOI: 10.1016/j.shaw.2024.04.008.*
16. *Miguel Correia, Wellington Oliveira, José Cecílio, Monintainer: An orchestration-independent extensible container-based monitoring solution for large clusters, Journal of Systems Architecture, Volume 145, 2023, 103035. DOI: 10.1016/j.sysarc.2023.103035.*
17. *Adabi Raihan Muhammad, Parman Sukarno, Aulia Arif Wardana, Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning, Procedia Computer Science, Volume 217, 2023, 1406–1415. DOI: 10.1016/j.procs.2022.12.339.*

PATTERN FOR SECURING APPLICATIONS UNDER THREAT OF MODIFICATION MACHINE LEARNING MODEL

Korneev N. V.[3], Kotrini E. S.[4]

Keywords: *cloud computing, dataset, template, poisoning attack, adversarial example, evasion attack, causative attack, container, machine learning, event log, monitoring system.*

The purpose of this article: *development of a template protection mechanism to ensure application security in the event of a threat of modification of a machine learning model.*

Research method: *analysis of the principles of attacks with ML model distortion and the capabilities of the intruder at the model training stage. Synthesis of an attack scenario using two attack strategies: data input strategy and ML model data modification strategy. The ML model was based on the Bank Customer Churn Prediction model, and an external intruder was selected for the threat, which is capable of changing the data sample for the machine learning model via the network by implementing a training data poisoning attack scenario. Using cryptographic methods, a new protection mechanism is proposed that ensures the integrity of the training data set due to hashing and storing hash sums signed with an electronic digital signature. The study was carried out by natural modeling of a Docker-based application in environments with containerization support, its deployment and testing in the event of a threat of modification of the machine learning model.*

Result: *the analysis threat of modification machine learning model and shows the relevance of the problem developing universal template security mechanisms, called patterns. In particular, three applicable attack strategies for modifying a machine learning model based on the capabilities of the intruder are considered – adversarial example, evasion attack and modification of machine learning model data – adversarial example, evasion attack. Scenario of poisoning attack on training data is considered. The article analyzes the threat of modification of machine learning model and shows the relevance of the problem of developing universal template security mechanisms, called patterns. In particular, three applicable attack strategies for modifying a machine learning model based on the capabilities of the intruder are considered – adversarial example, evasion attack and modification of machine learning model data – adversarial example, evasion attack. A scenario of an attack on training data poisoning is considered. A microservice architecture is built to ensure application security under the threat of modification of a machine learning model for a wide range of applications in the cloud infrastructure. A security pattern is developed to protect the application from an attack on poisoning training data based on microservices integrated into containers and a stack of technologies: Java 17; Spring 5; Docker, docker-compose; PostgreSQL; RabbitMQ; Git; Log4j2; Logstash; Elasticsearch; Kibana; Swagger. As part of the study, 5 microservices were developed: eureka – service, users – api, api – gateway, wrapper – api, config – server. In order to protect data coming into the machine learning model, the wrapper – api microservice was developed. The protection mechanism is that all calls to the machine learning microservice go through it and are checked for damage and/or substitution, data coming from the outside is also validated on the microservice side. Before adding data to the training data DB, the record is reinforced with an electronic signature, the source data is hashed, connected with a secret key. The program code of the microservices has been developed, including codes of special methods and algorithms for their implementation, providing a mechanism for protecting the application from a training data poisoning attack. A monitoring system for a training data poisoning attack was deployed based on the open source software Elasticsearch, Logstash, Kibana through event log objects (appender): error (warn) and information (info), which can be used in SIEM systems.*

Practical value: *the practical value of the proposed solution includes a template protection mechanism in the form of a pattern that can be applied to a wide range of applications, including transferring the developed solution to any industry: fuel and energy, economics and more, due to the cross-platform nature of the solution itself.*

References

1. *Shameer Mohammed, S. Nanthini, N. Bala Krishna, Inumarthi V. Srinivas, Manikandan Rajagopal, M. Ashok Kumar, A new lightweight data security system for data security in the cloud computing, Measurement: Sensors, Volume 29, 2023, 100856. DOI: 10.1016/j.measen.2023.100856.*
2. *S. Achar, Cloud computing security for multi-cloud service providers: controls and techniques in our modern threat landscape, International Journal of Computer and Systems Engineering, 16(9), 2022, 379–384. DOI: 10.5281/zenodo.7084251.*
3. *Oludare Isaac Abiodun, Moatsum Alawida, Abiodun Esther Omolara, Abdulatif Alabdulatif, Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey, Journal of King Saud University – Computer and Information Sciences, Volume 34, Issue 10, Part B, 2022, 10217–10245. DOI: 10.1016/j.jksuci.2022.10.018.*
4. *Chakraborti, A., Curtmola, R., Katz, J., Nieh, J., Sadeghi, A. R., Sion, R., Zhang, Y., Cloud Computing Security: Foundations and Research Directions. Foundations and Trends in Privacy and Security, 3(2), 2022, 103–213. DOI: 10.1561/3300000028.*
5. *Ukeje, N., Gutierrez, J., Petrova, K., Information security and privacy challenges of cloud computing for government adoption: a systematic review, International Journal of Information Security, Volume 23, 2024, 1459–1475. DOI: 10.21203/rs.3.rs-3351319/v1.*

3 Nikolai V. Korneev, Dr.Sc., Professor, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia. E-mail: niccyper@mail.ru
4 Elena S. Kotrini, student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia. E-mail: kotrini.elena@mail.ru

6. *Fatemeh Khoda Parast, Chandni Sindhav, Seema Nikam, Hadiseh Izadi Yekta, Kenneth B. Kent, Saqib Hakak, Cloud computing security: A survey of service-based models, Computers & Security,Volume 114, 2022, 102580. DOI: 10.1016/j.cose.2021.102580.*
7. *Ting Zhou, Hanshu Yan, Bo Han, Lei Liu, Jingfeng Zhang, Learning a robust foundation model against clean-label data poisoning attacks at downstream tasks, Neural Networks, Volume 169, 2024, 756-763. DOI: 10.1016/j.neunet.2023.10.034.*
8. *Ade Kurniawan, Yuichi Ohsita, Masayuki Murata, Detection of sensors used for adversarial examples against machine learning models, Results in Engineering, Volume 24, 2024, 103021. DOI: 10.1016/j.rineng.2024.103021.*
9. *Hamid Bostani, Veelasha Moonsamy, EvadeDroid: A practical evasion attack on machine learning for black-box Android malware detection, Computers & Security, Volume 139, 2024, 103676. DOI: 10.1016/j.cose.2023.103676.*
10. *Mahdee Jodayree, Wenbo He, Dr. Ryszard Janicki, Preventing Image Data Poisoning Attacks in Federated Machine Learning by an Encrypted Verification Key, Procedia Computer Science, Volume 225, 2023, 2723–2732. DOI: 10.1016/j.procs.2023.10.264.*
11. *Michael Gallagher, Nikolaos Pitropakis, Christos Chrysoulas, Pavlos Papadopoulos, Alexios Mylonas, Sokratis Katsikas, Investigating machine learning attacks on financial time series models, Computers & Security, Volume 123, 2022, 102933. DOI: 10.1016/j.cose.2022.102933.*
12. *Pahul Preet Singh, Fahim Islam Anik, Rahul Senapati, Arnav Sinha, Nazmus Sakib, Eklas Hossain, Investigating customer churn in banking: a machine learning approach and visualization app for data science and management, Data Science and Management, Volume 7, Issue 1, 2024, 7–16. DOI: 10.1016/j.dsm.2023.09.002*
13. *Badr Eddine Sabir, Mohamed Youssfi, Omar Bouattane, Hakim Allali, Authentication and load balancing scheme based on JSON Token For Multi-Agent Systems, Procedia Computer Science, Volume 148, 2019, 562–570. DOI: 10.1016/j.procs.2019.01.029.*
14. *Esquembre F., Chacón J., Saenz J., Vega J., Dormido-Canto S., A programmable web platform for distributed access, analysis, and visualization of data, Fusion Engineering and Design, Volume 197, 2023, 114049. DOI: 10.1016/j.fusengdes.2023.114049.*
15. *Dongyeop Lee, Daesik Lim, Jongseok Park, Soojeong Woo, Youngho Moon, Aesol Jung, Management Architecture With Multi-modal Ensemble AI Models for Worker Safety, Safety and Health at Work, Volume 15, Issue 3, 2024, 373–378. DOI: 10.1016/j.shaw.2024.04.008.*
16. *Miguel Correia, Wellington Oliveira, José Cecílio, Monintainer: An orchestration-independent extensible container-based monitoring solution for large clusters, Journal of Systems Architecture, Volume 145, 2023, 103035. DOI: 10.1016/j.sysarc.2023.103035.*
17. *Adabi Raihan Muhammad, Parman Sukarno, Aulia Arif Wardana, Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning, Procedia Computer Science, Volume 217, 2023, 1406–1415. DOI: 10.1016/j.procs.2022.12.339.*

ПРОБЛЕМА МОНИТОРИНГА ИНФОРМАЦИОННЫХ ПОТОКОВ, ВОЗНИКАЮЩИХ В ХОДЕ СБОРКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Тихомиров Н. А.[1], Ключарёв П. Г.[2]

DOI: 10.21681/2311-3456-2025-1-128-135

Цель исследования: *доказательство невозможности выявления информационных потоков, возникающих в ходе сборки программного обеспечения.*

Метод исследования: *математическое моделирование типового процесса сборки с последующим анализом полученных результатов в контексте фундаментальных математических задач.*

Результаты исследования: *в настоящей работе доказана фундаментальная невозможность точного детектирования информационного потока в рамках работы сборочной программы, а также рассмотрены предпосылки этой задачи и предложен перечень шагов, которые могут быть предприняты при организации эвристического решения. В составе предложенного эвристического решения рассмотрены популярные методы реализации отдельных его шагов, а само оно основано на необходимых условиях существования информационных потоков, что говорит о потенциале низкого уровня ложноотрицательных срабатываний.*

Научная новизна: *заключена в анализе применимости фундаментального подхода к решению поставленной задачи, а также в представлении эвристического подхода с низким уровнем ложноотрицательных срабатываний. Настоящая работа также в достаточно широкой мере рассматривает предпосылки поставленной задачи, что подчеркивает её важность.*

Ключевые слова: *теорема Райса, безопасность цепи поставок, избыточность на уровне файлов, недекларированные возможности, заимствованные компоненты, мониторинг сборки, сборочные системы, эвристические методы обеспечения безопасности.*

Введение

Первоначальным назначением процессов сборки программного обеспечения являлась (на примере проектов на языках C и C++) автоматизированная компиляция большого количества файлов с последующей линковкой их друг с другом. С другой стороны, в возможности всех сборочных инструментов (Make, Gradle и многих других) всегда входили в том или ином виде, – пусть даже с помощью вызова сторонних программ, – автоматическая генерация исходного кода, прямая модификация результирующих бинарных файлов и даже загрузка дополнительных материалов из сети во время сборки [1-3].

Более того, на основании выросших темпов разработки и повысившейся доступности пригодных к заимствованию компонентов ПО с открытым исходным кодом можно без сомнения говорить о предпосылках к снижению уровня понимания состава программного обеспечения его же разработчиком. Вполне рядовой становится ситуация, когда разработчик располагает десятками гигабайт кода его приложения, однако не может точно сказать, все ли имеющиеся у него файлы нужны для сборки итогового продукта.

С другой стороны, при формировании перечня исходников разработчик почти наверняка не учитывает файлы, которые берутся из его операционной системы. К примеру, для языка C++ это могут быть заголовочные файлы стандартной библиотеки. В то же время эти файлы в значительной степени влияют на структуру итогового исполняемого кода и его безопасность – к примеру, для некоторых проектов с открытым исходным кодом было выявлено, что более 90% обрабатываемых компилятором функций и структур проекта попадает в него именно из заголовочных файлов, включая системные[3].

Всё это не могло не привести к появлению атак на программное обеспечение, связанных с компрометацией системы сборки в ходе работы с заимствованным кодом. Подобные атаки могут быть отнесены к подмножеству семейств атак на цепи поставок [4, 5]. К примеру, в конце 2023 года и начале 2024 года появилось сразу несколько новостей о внедрении

1 Тихомиров Никита Александрович, студент кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н. Э. Баумана, Москва, Россия. E-mail: nicktikhomirov02@gmail.com

2 Ключарёв Пётр Георгиевич, доктор технических наук, профессор кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н. Э. Баумана, Москва, Россия. E-mail: pk.iu8@yandex.ru

3 Савицкий В.О. Инкрементальный анализ исходного кода на языках C/C++ // Труды Института системного программирования РАН, 2012. № 22. С. 119–130.

вредоносного кода в открытые пакеты для проектов на языке Python: arrapi, tmdbapis, nagerapi, pmmutils и PyTorch.

Аналогично, атаки могут проводиться и при помощи используемых средств разработки, включая сами инструменты сборки. На сегодняшний день для разработчика крайне важной становится задача идентификации и контроля используемых инструментов. Подобный подход активно продвигается как со стороны самих разработчиков, так и на уровне отечественных нормативных документов для разрабатываемых средств защиты информации[4].

Ещё одной типовой задачей в рамках обеспечения безопасности собираемого программного обеспечения является избавление от избыточности его исходного кода – по крайней мере, на уровне файлов исходных текстов. В некоторых случаях это является обязательным требованием, предъявляемым к ПО [7].

Более того, можно утверждать, что отсутствие мер по контролю избыточности исходных текстов программного обеспечения ведёт к затягиванию процесса разработки. К примеру, если применяемый разработчиком инструмент статического анализа не использует механизмы перехвата сборки, то исследование будет проведено для всей кодовой базы разработчика, – в этом случае всякая избыточность в исходных текстах приведёт к увеличению количества ложноположительных срабатываний.

Таким образом, можно говорить о необходимости контроля сборочной системы, что на формальном уровне может быть представлено в виде задачи валидации наличия или отсутствия соответствующих информационных потоков, возникающих в ходе процесса сборки программного обеспечения.

Основные понятия, используемые в поставленной задаче

Определение 1. В рамках данной работы будем определять процесс сборки программного обеспечения как процесс получения целевых файлов сборки при помощи некоторой программы, которую далее будем называть сборочной программой.

Для простоты модели будем считать список целевых файлов заданным (известным поэлементно) и не требующим валидации. Данный список конечен.

К примеру, в состав процесса сборки (для компилируемых языков) могут входить препроцессинг, компиляция и ассемблирование множества отдельных объектных файлов с их последующей линковкой в один общий исполняемый файл. Также в рамках настоящей работы допускается возможность генерации кода или ресурсных файлов, упаковки каких-либо файлов в архивы или же, наоборот, их распаковки. Типичными примерами сборочных программ могут служить Make, Maven, Gradle и их аналоги.

В рамках настоящей работы сборочная программа обладает следующими свойствами:

- исполняется пошагово, то есть ход исполнения программы может быть представлен в виде конечного или счётного списка состояний;
- состояние памяти процесса сборки может быть закодировано строкой конечной длины в некотором конечном алфавите (при этом не вводятся ограничения, что все состояния должны кодироваться строками одной и той же длины);
- число шагов процесса сборки конечно;
- исходный текст программы можно представить в виде строки конечной длины в некотором конечном алфавите (при этом не вводятся ограничения, что все сборочные программы должны кодироваться строками одной и той же длины).

Очевидно, что приведённый перечень ограничений не создаёт противоречия с практической областью.

Аналогично предположим, что любой файл (в том числе, любой целевой файл) может быть представлен конечной строкой в некоторой конечном алфавите, описывающей состояние его свойств (например, конкретное содержимое файла и конкретные права доступа к нему). Будем называть такую строку состоянием свойств файла. При этом не вводятся ограничения, что все состояния свойств файлов должны кодироваться строками одной и той же длины.

Информационным потоком, неформально говоря, можно называть перенос (с возможным преобразованием) информации между двумя файлами (объектами) при участии некоторого субъекта, являющегося инициатором этого преобразования. Эквивалентное, но более формальное определение можно встретить в национальном стандарте ГОСТ Р 59453.1-2021. Например, при распаковке архива можно говорить об информационном потоке из него в получаемые файлы при участии программы распаковки, а при компиляции можно говорить об информационном потоке из препроцессированного файла в файл с кодом на языке ассемблера при участии компилятора. Формальное определение информационного потока будет дано далее.

Используемая вычислительная модель

На практике в качестве вычислительной модели используются вычислительные устройства с достаточно сложной внутренней организацией. Упрощённой моделью этих вычислительных устройств можно считать равнодоступную адресную машину (РАМ).

Необходимо отметить, что данная модель не в полной мере соответствует её реальным аналогам, так как характеризуется бесконечной внутренней памятью, что неверно для прикладных устройств, конечность памяти которых говорит о, соответственно,

4 Сертификация программного обеспечения по требованиям доверия / Бегаев А. Н., Кашин С. В., Макаревич Н. А., Марченко А. А., Павлов Д. Д. // СПб.: Университет ИТМО, 2020. 40 с.

конечности множества состояний свойств файлов и множества состояний шагов исполнения сборочной программы.

Будем полагать это несоответствие незначительным, поскольку на практике затруднительно было бы использовать какие-либо из специфических для конечных множеств приёмов решения математических задач, включая, к примеру, табличные методы и методы полного перебора.

В представленной модели будем считать файлом некую последовательность ячеек памяти RAM (длина этой последовательности может меняться), а адресация по множеству ячеек осуществляется при помощи некоторой таблицы, подобной файловой системе в прикладных моделях. Во избежание необходимости математической формализации проблемы фрагментации памяти будем считать, что ячейки памяти одного файла не обязаны идти подряд и собраны в связный список.

Состояния свойств файлов могут быть представлены в виде конечных битовых строк, включающих сведения об имени файла, сведения о нём из таблицы, а также сведения, записанные в ячейки файла.

Исследуемая задача

Введём следующие основные для данной работы множества:

- M – множество сборочных программ;
- V – множество состояний свойств файлов, каждый элемент $v \in V$ этого множества сообщает информацию о некотором состоянии одного какого-либо файла;
- Q – множество пошаговых состояний всех процессов сборки для программ из M, которые эти процессы принимают в ходе исполнения; для этого множества определена функция $S{:}M \longrightarrow 2^Q$, которая ставит сборочной программе в соответствие множество состояний соответствующего ей процесса;
- $P = \{p \subset V | p\text{-конечное}\}$ – множество конечных подмножеств V.

Заметим, что нельзя говорить о множестве V как о множестве файлов в файловой системе. Подразумевается, что в него входят все состояния свойств всех файлов, то есть если в некоторый файл с состоянием свойств $v \in V$ произвести запись, то он будет иметь новое состояние $v^* \in V$.

С учётом оговоренных в прошлом разделе свойств рассматриваемых объектов сделаем следующие заключения о мощностях введённых множеств:

- множество M счётное как объединение счётного числа конечных множеств, так как любая программа однозначно кодируется конечной строкой в конечном алфавите, поэтому для любой фиксированной длины можно выделить конечное количество программ, а сами длины, очевидно, образуют ряд натуральных чисел;
- множество V счётное по аналогичным рассуждениям;
- множество P счётное по свойству множества конечных подмножеств счётного множества (если бы в P входили бесконечные подмножества, то оно было бы континуально);
- множество Q счётное как объединение счётного числа конечных множеств, так как у шагов каждого процесса сборки конечное число состояний;
- $\forall m_i \in M$, $S(m_i)$ – конечное множество.

По сделанному в прошлом разделе замечанию для сборочной программы $m_i \in M$ без уменьшения общности будем считать заданным множество результатов сборки и соответствующее ему множество результирующих состояний свойств результирующих файлов $V_i^{(res)} \subset V$.

Определение 2. Определим информационный поток как трёхместное отношение $(src,rcv,init)$ (источник, приёмник, инициатор), которое свидетельствует о том, что при участии субъекта $init$ часть информации в объекте rcv была сформирована на основании информации src.

В контексте настоящей работы информационный поток инициируется сборочной программой и связывает два состояния свойств файлов (различных, или же одного и того же), поэтому можно уточнить определение как $(src,rcv,init) \in V \times V \times M$.

В рамках исполнения сборочной программы $m_i \in M$ реализуется множество $T_i = \{(src,rcv,m_i) | src,rcv \in V\}$, то есть множество потоков, инициированных одним и тем же субъектом m_i. С учётом этого можно исключить из всех элементов T_i общий компонент, задав множество двуместных отношений (рёбер) E_i, как показано в (1). Это множество примечательно тем, что вместе с V образует орграф $G_i = \langle V,E_i \rangle$, который далее будем называть графом сборки для сборочной программы $m_i \in M$.

$$E_i = \{(src,rcv) | (src,rcv,m_i) \in T_i\}. \quad (1)$$

Множество информационных потоков, возникающих в ходе работы сборочной программы, $m_i \in M$ определяется множеством состояний $S(m_i)$ по некоторому соотношению, которое обозначим для графа сборки как функцию φ: $M \times 2^Q \longrightarrow (V \times V) \cup \{\sigma\}$, где «$\sigma$» – некорректная связь (т. к. функция φ, очевидно, с практической точки зрения может не иметь смысла для некоторых сочетаний программ с множествами состояний). Тогда можем дать определение множеству рёбер сборочного графа через данную функцию, как показано в соотношении (2). Будем обозначать связь между программой и множеством рёбер её сборочного графа, как показано в (3), так как связь через нижний индекс не всегда удобна для

$$m_i \in M, \quad E_i = \{\varphi(m_i,s) | s \subseteq S(m_i)\} \setminus \{\sigma\}. \quad (2)$$

$$E_i = E(m_i). \quad (3)$$

Достижимость вершины $v_2 \in V$ из вершины $v_1 \in V$ на графе G_i будем обозначать $v_1 \mapsto_{G_i} v_2$. Тогда можно ввести определение множеству исходных файлов сборки как $V_i^{(src)} = \{v \in V | (\exists v_1 \in V_i^{(res)}, v \mapsto_{G_i} v_1) \wedge \wedge (\nexists v_2 \in V: v_2 \mapsto_{G_i} v\}$, то есть это множество таких состояний свойств файлов, из которых существует информационный поток в результирующее множество и которые при этом не являются промежуточными этапами преобразования информации.

Необходимо заметить, что если бы вместо множества состояний свойств файлов в модели использовалось бы множество файлов, то необходимо было бы ввести временной параметр, поскольку для файлов потоки данных могут возникать в неестественном порядке наподобие приведённого в системе (4). Очевидно, что в приведённом примере неуместно было бы говорить о связи объектов a и c.

$$\begin{cases} (b,c,m_i) \text{ при } time = t \\ (a,b,m_i) \text{ при time} = t+1 \end{cases} \quad (4)$$

Также очевидно, что существует конструирующая функция ψ: $P \longrightarrow V$, для любого конечного множества состояний свойств файлов она строит такую программу, что выполняются утверждения:

1. $\forall p \in P$, если $\psi(p) = m_i$, то в графе $G_i = \langle V, E(m_i) \rangle$ выполняется $\forall v_{res} \in p$, $\exists v \in V: (v, v_{res}) \in E(m_i)$ – сконструированная программа гарантировано кодирует в числе прочего те рёбра, которые заходят в эти вершины;
2. $\forall p \in P$, для $\psi(p) = m_i$ выполняется $p \subseteq V_i^{(res)}$.

В прикладной области эта совокупность условий означает, что для любого конечного множества состояний свойств файлов можно написать сборочную программу, которая каким-либо образом их генерирует (однако, конечно же, не гарантируется, что у результирующей программы не будет побочных эффектов).

Функция ψ считается вычислимой и одинаковой для любой частной задачи.

Для моделирования результата сборочной программы $m_i \in M$ введём семейство характеристических (т.е. бинарных) векторов β_i множества V. Вектор β_i является представлением файловой системы компьютера после работы сборочной программы m_i, ставя в соответствие имеющимся состояниям свойств файлов единицу, а отсутствующим – ноль. Вектор β_i обладает следующими (обоснованными с прикладной точки зрения) свойствами:

1. если после работы сборочной программы $m_i \in M$ имеется результат сборки $v_k \in V_i^{(res)}$, то $\beta_{ik} = 1$;
2. $\|\beta_{ik}\|$ – конечное число (т.е. по результатам работы сборочной программы $m_i \in M$ в файловой системе не может быть бесконечное число файлов).

Из приведённых свойств следует, что вектор β_i, хотя и является бесконечномерным как характеристический вектор счётного множества, может быть представлен конечной строкой, кодирующей конечный перечень индексов (натуральных чисел), обозначающих координаты, в которых характеристический вектор β_i принимает ненулевое значение. Таким образом, можно сказать, что программа $m_i \in M$ вычисляет вектор β_i.

В рамках настоящей работы для сборочных программ нет необходимости в формализации входных данных (можно считать входные данные зашитыми в код программы), однако для единообразия с принятой для Машин Тьюринга и вычисляемых ими функций нотацией введём λ – фиктивный вход функций, вычисляемых сборочными программами. Проще говоря, программа $m_i \in M$ будет вычислять функцию $m_i(\lambda) = \beta_i$ (вычисляемую программой функцию будем обозначать так же, как и саму программу). Здесь следует напомнить, что по изначальному предположению сборочные программы останавливаются за конечное количество шагов, то есть функция $m_i(\lambda)$ вычислима.

Таким образом, исследование некоторой программы сборки имеет следующие входные сведения:

- сборочную программу $m_i \in M$ с процессом, который завершается за конечное число шагов и имеет множество состояний $S(m_i)$;
- считающееся известным и (для простоты) неоспоримым конечное множество результирующих состояний свойств файлов $V_i^{(res)} \subset V$, являющихся результатами сборки для программы $m_i \in M$;
- общий для всех задач ранее описанный объект ψ.

Из приведённых ранее рассуждений следует, что задача выявления информационных потоков сводится к задаче восстановления рёбер графа G_i. Из тех же рассуждений справедлива и обратная сводимость. Далее будем рассматривать именно постановку задачи с использованием графа G_i. Выпишем её полную постановку.

Задача 1. Имеется сборочная программа $m_i \in M$, для неё известны её результирующие состояния свойств файлов $V_i^{(res)} \subset V$ и все состояния её исполнения $S(m_i)$ – для описанной программы необходимо восстановить граф.

В рамках настоящей работы далее будет продемонстрировано, что задача 1 не имеет математически корректного алгоритма решения.

Утверждение 1. Задача 1 алгоритмически неразрешима.

Анализ поставленной задачи

Построим семейство множеств $F_{vw} = \{m_j(\lambda) | (m_j \in M) \wedge \wedge ((v,w) \in E(m_j))\}$ с параметрами $v,w \in V$. Проще говоря, для пары состояний свойств файлов $v,w \in V$

множество F_{vw} содержит все вычисляемые сборочными программами функции, сборочные графы которых содержат ребро (v,w), которое, будучи ребром в некотором графе G_j, по ранее приведённым рассуждениям однозначно соответствует информационному потоку (v,w,m_j). Множество F_{vw} можно неформально назвать множеством-признаком – если программа принадлежит ему, то она обладает некоторым свойством, и наоборот.

Определение 3. Нетривиальной парой состояний свойств файлов будем называть пару $v^*,w^* \in V$, для которой верно, что $F_{v^*w^*} \neq \emptyset$ и $\bar{F}_{v^*w^*} \neq \emptyset$.

Утверждение 2. Нетривиальная пара состояний свойств файлов существует.

Доказательство утверждения 2.

Возьмём произвольную программу $m_j \in M$ с конечным множеством состояний $S(m_j)$. Справедливо, что $|E_j| \leq 2^{|S(m_j)|}$, что следует из соотношения (2), требования конечности числа шагов исполнения программы, а также свойств множества подмножеств конечного множества. Возьмём произвольные различные $2^{|S(m_j)|}+1$ состояний свойств файлов, полученное множество будем обозначать $p^* \in P$, после чего применим к нему конструирующую функцию ψ, которая возвращает сборочную программу, генерирующую заданные состояния свойств файлов. Из свойств ψ следует, что полученная программа $\psi(p^*)$ гарантировано будет реализовывать в своём графе сборки рёбра, инцидентные с вершинами из множества p^*.

Таким образом, произвольно взятая программа m_j содержит не более, чем $2^{|S(m_j)|}$ рёбер в своём сборочном графе, а сконструированная программа $\psi(p^*)$ в силу свойств конструирующей функции ψ имеет не менее, чем $|p^*| = 2^{|S(m_j)|}+1$ ребёр. Из мощностных соображений очевидно существование нетривиальной пары состояний, как показано в соотношении (5).

$$\exists v^*,w^* \in V: \begin{cases} ((v^*,w^*) \in E(\psi(p^*)) \\ ((v^*,w^*) \notin E_j \end{cases} \quad (5)\ )$$

Конец доказательства утверждения 2.

С использованием утверждения 2 можно доказать утверждение 1, обратившись к теореме Райса.

Доказательство утверждения 1.

Задача выявления информационного потока в ходе исполнения сборочной программы является тривиальным следствием теоремы Райса.

Теорема Райса гласит, что если имеется нетривиальное свойство вычислимых функций (непустое множество с непустым дополнением), то задача отнесения программы к этому множеству либо же его дополнению является алгоритмически неразрешимой[5].

5 Емельченков Е. П., Емельченков В. Е. Вычислимость. Введение в теорию алгоритмов // Математическая морфология: электронный математический и медико-биологический журнал. 2000. № 3–3. С. 121–130. EDN: BJIQOL

Соответствие поставленной задачи условию данной теоремы показано в табл. 1.

Таблица 1.
Удовлетворение условия теоремы Райса, описанной в настоящей работе моделью

Требование теоремы	Удовлетворение требования
Некоторое свойство (множество) функций	F_{vw} для некоторых $v,w \in V$
Свойство нетривиально	Существование нетривиальных $v,w \in V$ показано в доказательстве утверждения 2.
Функции вычислимы	Аргумент функции: введённый фиктивно объект λ Результат функции: характеристический вектор из множества $\{\beta\}$ По изначальному предположению настоящей работы: все сборочные процессы завершают свою работу, т.е. функция вычислима

Конец доказательства утверждения 1.

По соотношению (1) можно совершить обратный переход от доказанного утверждения 1 к (эквивалентной) постановке задачи через понятие информационного потока.

Таким образом, для любого (нетривиального) информационного потока задача его выявления в рамках исполнения сборочной программы является алгоритмически неразрешимой по Теореме Райса.

Эвристический подход к решению поставленной задачи

Решение рассмотренной задачи в том или ином виде является этапом многих этапов обеспечения информационной безопасности при разработке программного обеспечения – к примеру, оно может использоваться для улучшения качества статического анализа [8].

Так как разработка математически корректных методов решения данной задачи не представляется возможной, рассмотрим эвристический подход.

Методы эвристического решения поставленной задачи напрямую связаны с методом вычисления введённого ранее множества $S(m_i)$, которое, напомним, содержит все закодированные каким-либо образом промежуточные состояния хода исполнения

сборочной программы, а также, соответственно, с применяемым методом кодирования этих состояний.

Прямолинейным и громоздким решением является симуляция всего программного окружения при помощи соответствующего инструмента с пошаговым анализом преобразований, осуществляющихся над памятью симулируемого устройства, это в достаточной степени решает задачу формирования перечня промежуточных состояний [9, 10].

Для этого может быть использован, к примеру, общедоступный инструмент QEMU международной совместной разработки ([11]), либо его модификация от Института системного программирования им. В. П. Иванникова Российской академии наук, либо же отечественный инструмент Korycat от отечественной компании ООО «Инфорион» [12, 13].

К сожалению, для реализации какого-либо эвристического решения описанный подход является крайне неудобным, так как требует восстановления данных о состоянии из набора двоичных данных, которым является снимок памяти процесса сборочной программы. На основании этого предлагается обратиться к менее доскональным, но более универсальным методам мониторинга – например, к мониторингу обращений к файловой системе.

Избранные методы мониторинга обращений к файловой системе

Мониторинг действий с файловой системой может осуществляться, например, при помощи того же эмулятора QEMU[6]. Альтернативным подходом является мониторинг системных вызовов, который может осуществляться либо через прямой мониторинг при помощи соответствующей утилиты (например, Strace или какое-либо иное решение на базе системного вызова ptrace), либо же через подмену разделяемой динамически линкуемой библиотеки (посредством переопределения переменной окружения «LD_PRELOAD»), которая предоставляет интерфейс системных вызовов программам пользовательского уровня, включая сборочную программу – переопределению могут подвергаться, например, библиотечные функции, являющиеся интерфейсами для системного вызова «execve», аргументы которого во время сборки проверяются на предмет вызова компилятора[7].

Менее популярным решением является прямая подмена файлов, содержащих логику сборочной программы (например, подмена компилятора для языков C и C++) [14, 15].

В результате мониторинга действий над файловой системой может быть сформирована последовательность файлов и доступов к ним – примеры доступов можно почерпнуть, например, из области построения SIEM-систем, где в «усреднённый» перечень видов доступа к абстрактной сущности включают шесть основных действий:

- создание сущности;
- удаление сущности;
- коммуникация с сущностью;
- манипуляция данными сущности;
- манипуляция работой сущности;
- получение дополнительных сведений о сущности (например, размер и время создания).

Подобный перечень видов доступа (в значительно более подробной форме) используется, например, при категоризации событий в MaxPatrol SIEM 10 версии.

Заметим, что классические модели разграничения доступа, опирающиеся на понятие информационного потока, к примеру, модель Белла-ЛаПадулы, вводят другой набор доступов, включающий чтение, запись и, в некоторых моделях, исполнение. Далее будем считать, что «манипуляция данными сущности» соответствует доступу на запись, «манипуляция работой сущности» соответствует доступу на исполнение, «коммуникация с сущностью» соответствует неразделимой совокупности доступов на запись и чтение, а для доступа на чтение аналога в приведённом перечне нет, поэтому дополним его соответствующим седьмым действием.

Описание предлагаемого подхода

Нетрудно заметить, что любой информационный поток имеет два необходимых условия для своего существования:

- субъект-инициатор производит чтение из источника (либо осуществляет коммуникацию с ним);
- субъект-инициатор производит манипуляцию данными приёмника (либо осуществляет коммуникацию с ним).

С учётом приведённых ранее рассуждений, предлагаемый эвристический подход заключается в том, что выполнение необходимого условия считается признаком потенциального существования потока.

В соответствии с предлагаемым подходом следует с использованием некоторой системы мониторинга доступов к файловой системе зафиксировать перечень файлов доступов к ним во время работы сборочной программы, после чего для всех сочетаний

6 Stepanov V. M., Dovgalyuk P. M., Poletaev D. N. Tracing ext3 file system operations in the QEMU emulator. Trudy ISP RAN/Proc. ISP RAS, vol. 30, issue 5, 2018. pp. 101–108. DOI: 10.15514/ISPRAS-2018-30(5)-6.

7 Белеванцев А. А. Многоуровневый статический анализ исходного кода для обеспечения качества программ: дис. ... доктора физико-математических наук 05.13.11 / Белеванцев А. А. – М., 2017. – 229 с.

«чтение»-«запись» зарегистрировать наличие информационных потоков.

После указанных действий предлагается упорядочить перечень потоков по метке времени, – подобные метки можно определить для любого из рассмотренных методов (симуляция, системные вызовы и т.д.), – в паре «чтение»-«запись» следует при этом ориентироваться на второе действие («запись»). В отсортированном перечне информационных потоков можно распознать конкретный интересующий проверяющего сборку эксперта (в рамках некоторой поставленной задачи) посредством валидации прямого или транзитивного наличия такового потока.

В целях фильтрации ложноположительных (или не имеющих смысла) информационных потоков предлагается также дополнительно удалить из перечня потоков те, которые приводят в удаляемый либо создаваемый (пересоздаваемый) объект файловой системы.

Также стоит заметить, что использование необходимого условия в достаточной для эвристического подхода мере снижает риск возникновения ложноотрицательных срабатываний детектирующего алгоритма.

Заключение

В настоящей работе рассмотрены предпосылки задачи выявления информационных потоков в рамках работы сборочной программы, доказана фундаментальная невозможность точного решения этой задачи, а также предложен перечень шагов, которые могут быть предприняты при организации эвристического решения.

В рамках предложенного эвристического решения рассмотрены популярные методы перехвата состояний хода исполнения сборочной программы и подходы к интерпретации полученных данных.

Полученный в данной работе результат может быть также дополнен иными моделями, однако все они также будут носить эвристический характер по оговоренным причинам.

Потенциальным развитием настоящей работы может являться реализация описанного подхода и его дальнейшее расширение.

Литература

1. *Фигловский К. С., Никифоров И. В., Юсупова О. А. Использование Gradle build cache для оптимизации времени сборки // Современные Технологии в Теории и Практике Программирования. Сборник материалов научно-практической конференции. – СПб: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», 2021. С. 127–129.*
2. *Арустамян С. С., Антипов И. С. Интеллектуальные методы фаззинг-тестирования в рамках цикла безопасной разработки программ // Безопасные Информационные Технологии. Сборник трудов Двенадцатой международной научно-технической конференции. – М.: Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет), 2023. С. 11–15.*
3. *Poeplau S., Francillon A. Symbolic Execution with SymCC: Don't Interpret, Compile! // Proc. of 29-th USENIX Security Symposium, 2020, pp. 181–198.*
4. *Леонов Н. В. Противодействие уязвимостям программного обеспечения. Часть 2. Аналитическая модель и концептуальные решения // Вопросы кибербезопасности. 2024, № 3 (61). С. 90–95. DOI: 10.21681/2311-3456-2024-3-90-95.*
5. *On the prevalence of software supply chain attacks: Empirical study and investigative framework / Andreoli A., Lounis A., Debbabi M., Hanna A. // Proceedings of the Tenth Annual DFRWS Europe Conference, 2023. № 44. DOI: 10.1016/j.fsidi.2023.301508.*
6. *Практические аспекты выявления уязвимостей при проведении сертификационных испытаний программных средств защиты информации / В. В. Вареница, А. С. Марков, В. В. Савченко, В. Л. Цирлов // Вопросы кибербезопасности. – 2021. – № 5(45). – С. 36–44. – DOI 10.21681/2311-3456-2021-5-36-44. – EDN TBQOCG.*
7. *Kotlin с точки зрения разработчика статического анализатора / Афанасьев В. О., Поляков С. А., Бородин А. Е., Белеванцев А. А. // Труды Института системного программирования РАН, 2021. № 33 (6). С. 67–82.*
8. *Девянин, П. Н. Формирование методологии разработки безопасного системного программного обеспечения на примере операционных систем / П. Н. Девянин, В. Ю. Тележников, А. В. Хорошилов // Труды Института системного программирования РАН. – 2021. – Т. 33, № 5. – С. 25–40. – DOI 10.15514/ISPRAS-2021-33(5)-2. – EDN WBXBTQ.*
9. *Natch: Определение поверхности атаки программ с помощью отслеживания помеченных данных и интроспекции виртуальных машин / П. М. Довгалюк, М. А. Климушенкова, Н. И. Фурсова [и др.] // Труды Института системного программирования РАН. – 2022. – Т. 34, № 5. – С. 89–110. – DOI 10.15514/ISPRAS-2022-34(5)-6. – EDN JNKSTV.*
10. *Коваленко Р. Д., Макаров А. Н. Динамический анализ IoT-систем на основе полносистемной эмуляции в QEMU // Труды Института системного программирования РАН. 2021. № 33–5. С. 155–166.*
11. *Аристов Р. С., Гладких А. А., Давыдов В. Н., Комахин М. О. Разработка программной платформы Korycat эмуляции сложных вычислительных систем // Наноиндустрия, 2019. № S (89). С. 350–352.*
12. *Гладких А. А., Кемурджиан А. Л., Комахин М. О. Отладка и анализ устройств и приложений с операционной системой на базе Linux в эмуляторе Korycat // Наноиндустрия, 2020. № S5-2 (102). С. 406–408.*
13. *Вишняков А. В. Поиск ошибок в бинарном коде методами динамической символьной интерпретации: дис. ... кандидата физико-математических наук 2.3.5 / Вишняков А. В. – М., 2022. – 131 с.*
14. *Шимчик, Н. В. Irbis: статический анализатор помеченных данных для поиска уязвимостей в программах на C/C++ / Н. В. Шимчик, В. Н. Игнатьев, А. А. Белеванцев // Труды Института системного программирования РАН. – 2022. – Т. 34, № 6. – С. 51–66. – DOI: 10.15514/ISPRAS-2022-34(6)-4.*

DATA FLOW MONITORING PROBLEM IN SOFTWARE BUILDING PROCESS

Tikhomirov N. A.[8], Klyucharev P. G.[9]

Keywords: *Rice's theorem, supply chain security, file-level redundancy, undeclared capabilities, open-source software, build process monitoring, build systems, heuristic approaches to enforcement of information security.*

The purpose of the study *is a formal proof for impossibility of precise identification of data flows, that occur in process of software building.*

Research methods: *analysis of typical building process mathematical model in relation to fundamental problems of mathematics.*

Study results: *in the proposed study a formal proof is suggested, that it is fundamentally impossible to identify data flow in software building process precisely. Practical applications of mentioned precise identification are also covered by this work as well as heuristic resolution steps for the problem are suggested. Implementation means for some of suggested steps overview is also provided. Proposed algorithm is aware of necessary conditions for data flows to exist, which leads to a potentially low level of false negatives.*

The scientific novelty *consists in applicability analysis of a fundamental approach to named problem resolution as well as made suggestion for heuristic algorithm with potentially low level of false negatives. Practical reasons for the problem to be researched are also covered by the study, that strengthens its importance.*

References

1. *Figlovskij K. S., Nikiforov I. V., Jusupova O. A. Ispol'zovanie Gradle build cache dlja optimizacii vremeni sborki // Sovremennye Tehnologii v Teorii i Praktike Programmirovanija. Cbornik materialov nauchno-prakticheskoj konferencii. – SPb: Federal'noe gosudarstvennoe avtonomnoe obrazovatel'noe uchrezhdenie vysshego obrazovanija «Sankt-Peterburgskij politehnicheskij universitet Petra Velikogo», 2021. S. 127–129.*
2. *Arustamjan S. S., Antipov I. S. Intellektual'nye metody fazzing-testirovanija v ramkah cikla bezopasnoj razrabotki programm // Bezopasnye Informacionnye Tehnologii. Sbornik trudov Dvenadcatoj mezhdunarodnoj nauchno-tehnicheskoj konferencii. – M.: Moskovskij gosudarstvennyj tehnicheskij universitet imeni N. Je. Baumana (nacional'nyj issledovatel'skij universitet), 2023. S. 11–15.*
3. *Poeplau S., Francillon A. Symbolic Execution with SymCC: Don't Interpret, Compile! // Proc. of 29-th USENIX Security Symposium, 2020, pp. 181–198.*
4. *Leonov N. V. Protivodejstvie ujazvimostjam programmnogo obespechenija. Chast' 2. Analiticheskaja model' i konceptual'nye reshenija // Voprosy kiberbezopasnosti. 2024, № 3 (61). S. 90–95. DOI: 10.21681/2311-3456-2024-3-90-95.*
5. *On the prevalence of software supply chain attacks: Empirical study and investigative framework / Andreoli A., Lounis A., Debbabi M., Hanna A. // Proceedings of the Tenth Annual DFRWS Europe Conference, 2023. № 44. DOI: 10.1016/j.fsidi.2023.301508.*
6. *Prakticheskie aspekty vyjavlenija ujazvimostej pri provedenii sertifikacionnyh ispytanij programmnyh sredstv zashhity informacii / V. V. Varenica, A. S. Markov, V. V. Savchenko, V. L. Cirlov // Voprosy kiberbezopasnosti. – 2021. – № 5(45). – S. 36-44. – DOI 10.21681/2311-3456-2021-5-36-44. – EDN TBQOCG.*
7. *Kotlin s tochki zrenija razrabotchika staticheskogo analizatora / Afanas'ev V. O., Poljakov S. A., Borodin A. E., Belevancev A. A. // Trudy Instituta sistemnogo programmirovanija RAN, 2021. № 33 (6). S. 67–82.*
8. *Devjanin, P. N. Formirovanie metodologii razrabotki bezopasnogo sistemnogo programmnogo obespechenija na primere operacionnyh sistem / P. N. Devjanin, V. Ju. Telezhnikov, A. V. Horoshilov // Trudy Instituta sistemnogo programmirovanija RAN. – 2021. – T. 33, № 5. – S. 25–40. – DOI 10.15514/ISPRAS-2021-33(5)-2. – EDN WBXBTQ.*
9. *Natch: Opredelenie poverhnosti ataki programm s pomoshh'ju otslezhivanija pomechennyh dannyh i introspekcii virtual'nyh mashin / P. M. Dovgaljuk, M. A. Klimushenkova, N. I. Fursova [i dr.] // Trudy Instituta sistemnogo programmirovanija RAN. – 2022. – T. 34, № 5. – S. 89–110. – DOI 10.15514/ISPRAS-2022-34(5)-6. – EDN JNKSTV.*
10. *Kovalenko R. D., Makarov A. N. Dinamicheskij analiz IoT-sistem na osnove polnosistemnoj jemuljacii v QEMU // Trudy Instituta sistemnogo programmirovanija RAN. 2021. № 33–5. S. 155–166.*
11. *Aristov R. S., Gladkih A. A., Davydov V. N., Komahin M. O. Razrabotka programmnoj platformy Kopycat jemuljacii slozhnyh vychislitel'nyh sistem // Nanoindustrija, 2019. № S (89). S. 350–352.*
12. *Gladkih A. A., Kemurdzhian A. L., Komahin M. O. Otladka i analiz ustrojstv i prilozhenij s operacionnoj sistemoj na baze Linux v jemuljatore Kopycat // Nanoindustrija, 2020. № S5-2 (102). S. 406–408.*
13. *Vishnjakov A. V. Poisk oshibok v binarnom kode metodami dinamicheskoj simvol'noj interpretacii: dis. ... kandidata fiziko-matematicheskih nauk 2.3.5 / Vishnjakov A.V. – M., 2022. – 131 s.*
14. *Shimchik, N. V. Irbis: staticheskij analizator pomechennyh dannyh dlja poiska ujazvimostej v programmah na C/C++ / N. V. Shimchik, V. N. Ignat'ev, A. A. Belevancev // Trudy Instituta sistemnogo programmirovanija RAN. – 2022. – T. 34, № 6. – S. 51–66. – DOI 10.15514/ISPRAS-2022-34(6)-4.*

8 Nikita A. Tikhomirov, student of the «Information Security» department, Bauman Moscow State Technical University, Moscow, Russian Federation. E-mail: nicktikhomirov02@gmail.com

9 Petr G. Klyucharev, Dr.Sc. Associate Professor of Information Security department, Bauman Moscow State Technical University, Moscow, Russian Federation. E-mail: pk.iu8@yandex.ru

КИБЕРБЕЗОПАСНОСТЬ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ В УСЛОВИЯХ ОСУЩЕСТВЛЕНИЯ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ

Стародубцев Ю. И.[1], Закалкин П. В.[2], Карасев С. В.[3]

DOI: 10.21681/2311-3456-2025-1-136-146

Цель исследования: *рассмотреть порядок осуществления информационно-технических воздействий на системы видеонаблюдения; оценить существующие требования информационной безопасности к системам видеонаблюдения в Российской Федерации; сформировать обобщенные предложения по обеспечению информационной безопасности существующих систем видеонаблюдения в условиях преднамеренных информационно-технических воздействий.*

Методы исследования: *системный анализ, классификация, сравнительный анализ.*

Полученные результаты: *сформирована обобщенная схема порядка осуществления информационно-технических воздействий на системы видеонаблюдения; сформулированы обобщенные предложения по обеспечению информационной безопасности существующих систем видеонаблюдения; сформулированы предложения по разработке нормативно-правовой документации регуляторами (в области информационной безопасности).*

Научная новизна: *осуществлен анализ конфликтной ситуации в области систем видеонаблюдения, что позволило выявить начальные мероприятия, необходимые для последующего развития информационной безопасности систем видеонаблюдения.*

Ключевые слова: *киберпространство, информационно-технические воздействия, кибербезопасность, видеонаблюдение, угрозы, нарушитель, информационная безопасность.*

Введение

Сложившаяся военно-политическая обстановка привела к началу специальной военной операции (СВО) и, как следствие, к переформатированию мирового порядка. Одним из отличительных факторов данного военного конфликта является возросшая роль киберпространства при ведении военных действий. Резко возросло количество кибератак, осуществляемых противоборствующими сторонами (как открыто, так и посредством своих «прокси» группировок), появились новейшие вооружения, навигация и управление которыми осуществляется посредством киберпространства [1;2].

Киберпространство сформировалось в результате развития систем связи и их трансформации в информационно-коммуникационные системы с последующей интеграцией с навигационными, технологическими, экономическими и другими процессами в различных областях деятельности человечества. Произошла интеграция процессов генерации, сбора, передачи, обработки и распределения информационных ресурсов в автоматизированном и автоматическом режиме, что непрерывно порождает множество новых технологических процессов в различных областях деятельности человечества, в том числе в управлении отдельными индивидуумами, группами и обществом в целом [3–5].

В рамках статьи под киберпространством будем понимать искусственное неоднородное технологическое пространство с множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которого не предопределяется требованиями одной системы управления, а функционирует в интересах множества разнородных, в том числе антагонистических систем управления. При этом свойства киберпространства зависят как от характеристик собственных элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей [6–8].

Киберпространство обеспечивает функционирование множества систем различного назначения, в том числе систем наблюдения за общественным порядком, дорожным движением и т.д., которые в своей основе имеют систему видеонаблюдения, контролирующую дорожный трафик, пешеходные зоны городов, общественные места, метро, общественный транспорт и т.д. В своей совокупности эти системы создают своеобразные зоны покрытия страны видеонаблюдением с онлайн трансляцией видео и сохранением потока на центральных серверах.

В первые дни СВО эти системы продолжали свое функционирование, что позволяло вооруженным

1 Стародубцев Юрий Иванович, Заслуженный деятель науки РФ, Заслуженный изобретатель РФ, доктор военных наук, профессор, профессор кафедры, Военная академия связи, Санкт Петербург, Россия. e-mail: prof.starodubtsev@gmail.com, https://orcid.org/0000-0001-5140-4476

2 Закалкин Павел Владимирович, кандидат технических наук, Академия Федеральной Службы Охраны Российской Федерации, Орёл, Россия. e-mail: pzakalkin@mail.ru, https://orcid.org/0000-0003-2946-2586

3 Карасев Станислав Владимирович, Академия Федеральной Службы Охраны Российской Федерации, Орёл, Россия. -mail: ilmaglu@mail.ru

силам Украины (ВСУ) на своей территории в режиме реального времени наблюдать за передвижениями Вооруженных Сил Российской Федерации (ВС РФ) и, соответственно, планировать оборонительные действия, осуществлять ракетно-артиллеристские удары по движущимся колоннам техники, устраивать засады и т.д. В совокупности с системой распознавания лиц и OSINT возможно было определить личности конкретных военнослужащих и организационно-штатную принадлежность их подразделений [12–14].

В 2024 году при заходе на территорию Курской области ВСУ осуществили информационно-технические воздействия (ИТВ) на инфраструктуру РФ и получили доступ как к специализированным системам видеонаблюдения (например, систем наблюдения за общественным порядком, наблюдения за дорожным движением и т.п.), так и отдельных видеокамер частных лиц (web-камеры, установленные в частных домовладениях).

Полученные таким образом разведданные были использованы противником как для планирования боевых действий, так и для нанесения огневых ударов по объектам и подразделениям ВС РФ. В ряде случаев они способствовали вооруженным силам Украины в получении разведывательных данных о дислокации и перемещении подразделений и частей российской армии[4].

Аналогичные ИТВ, осуществляемые посредством киберпространства, приводили к компрометации критических систем на территории РФ. Так, по информации телеграмм-каналов[5] проект «Безопасный регион» был скомпрометирован из-за утечек и уязвимостей. Сотни незарегистрированных и не верифицированных пользователей получили доступ к системе. В результате в сети можно встретить множество видеозаписей с различными чрезвычайными происшествиями, которые были скачаны или пересняты из этой системы. По данным спецслужб ряд преступлений (в том числе резонансные) готовился и координировался по камерам Московской области.

Получается, что системы видеонаблюдения оказали влияние на ход боевых действий и на тактическом уровне значительно облегчали действия ВСУ, а также использовались криминальными элементами для планирования и осуществления противоправных действий.

Основными целями представляемого исследования является:

- рассмотрение обобщенного порядка осуществления информационно-технических воздействий на системы видеонаблюдения;
- рассмотрение существующих требований информационной безопасности к системам видеонаблюдения в РФ;
- формирование обобщенных предложений по обеспечению безопасности существующих систем видеонаблюдения в условиях преднамеренных информационно-технических воздействий.

Обобщенный порядок осуществления информационно-технических воздействий на системы видеонаблюдения

Комплексно обобщив представленную в отрытом доступе информацию[6], была сформирована обобщенная блок-схема порядка осуществления информационно-технических воздействий на системы видеонаблюдения (рисунок 1).

Рис. 1. Обобщенная блок-схема порядка осуществления информационно-технических воздействий на системы видеонаблюдения

Для обнаружения web-камер, подключенных к киберпространству на территории конкретного населенного пункта, используются IP-адреса. Из-за наличия большого количества устройств, подключенных к киберпространству (либо являющихся его ядром), все IP-адреса группируются в рамках заданных диапазонов. При этом, диапазон IP-адресов от региона к региону изменяется. Вся информация об IP-диапазонах является открытой и аккумулируется в базах данных, которыми пользуются в том числе и Интернет-провайдеры.

Выявленные IP-диапазоны анализируются с помощью специализированных поисковых сервисов. Среди наиболее часто используемых специализированных поисковых сервисов основными являются сервисы Shodan, Censys, Zomey. Данные сервисы позволяют обнаруживать, отслеживать и анализировать устройства, подключенные к киберпространству, либо являющиеся его ядром (например, магистральные маршрутизаторы операторов связи).

Информация, предоставляемая вышеописанными сервисами, достаточно подробна и позволяет получить доступ к обнаруженным web-камерам

4 Счет может идти на тысячи: ВСУ взламывают камеры наблюдения в России и шпионят за военными России [Электронный ресурс] URL: https://www.gazeta.ru/tech/2024/08/20/19602931.shtml

5 Телеграмм канал «ВЧК-ОГПУ» [Электронный ресурс] URL: t.me/vchkogpu

6 ИИ и взломанные камеры видеонаблюдения помогают ВСУ успешнее атаковать Россию [Электронный ресурс] URL: https://www.gazeta.ru/tech/news/2024/08/20/23733349.shtml.

(в бесплатных версиях к ограниченному количеству). Платные версии имеют расширенный функционал, позволяют осуществлять настройку фильтрации, а также предоставляют расширенный доступ к информации об обнаруженных устройствах (согласно правилам фильтрации).

Разумно предположить, что информация, предоставляемая данными сервисами (даже на максимальных тарифах), является весьма ограниченной. Максимально полный объем данных в первую очередь предоставляется иностранным спецслужбам и уже после дополнительной обработки и фильтрации по остаточному принципу идет в условно открытый доступ.

Получение доступа к web-камерам в подавляющем большинстве случаев заключается в эксплуатации уязвимостей в программном обеспечении (ПО) камер, либо в вводе установленных по умолчанию логина и пароля в панели администрирования (пароли, установленные производителями по умолчанию). При наличии времени и необходимых ресурсов осуществляется подбор пароля по словарю, либо с использованием специализированных средств подбора пароля.

Получение доступа к большому количеству web-камер дает доступ к видеопотоку большого объема, просмотр и сортировка (исключение – камеры, которые не информативны) которого вручную требует значительного количества времени и человеческих ресурсов. Соответственно, к моменту, когда будет выявлена необходимая информация, обнаружена корреляция между различными камерами (например, построен маршрут передвижения штурмовых групп, колонн техники и т.д.) полученная информация будет неактуальна.

Для повышения эффективности анализа получаемого видеопотока ВСУ использовали искусственный интеллект (ИИ), с помощью которого обрабатывалось полученное с web-камер изображение. Искусственный интеллект позволяет в режиме реального времени отсеивать ненужные записи, фиксировать на нужных материалах корреляции, которые человеком, вероятно, остались бы незамеченными, а также осуществлять в автоматическом режиме добавление вновь обнаруженных web-камер.

Таким образом, используя данный (относительно простой) подход, ВСУ при наступлении на территорию Курской области имели доступ к множеству web-камер, находящихся на территории РФ, и использовали исходящий от них видеопоток в своих интересах.

Исходя из этого задача обеспечения информационной безопасности распределенных систем видеонаблюдения является актуальной и требует тщательного рассмотрения. Исходя из сложившихся подходов к обеспечению информационной безопасности [7–9] прежде всего необходимо рассмотреть нормативно-правовые акты, распространяющие свое действие на системы видеонаблюдения.

Существующие нормативно-правовые акты, распространяющие свое действие на системы видеонаблюдения

Согласно ГОСТ[7] системы видеонаблюдения относятся к комплексным системам безопасности. Помимо этого, имеется ряд других документов и ГОСТ, в той или иной степени регулирующих построение и применение систем видеонаблюдения[8].

Существующие нормативные документы не предполагают унификацию требований для разных типов объектов, но позволяют выделить следующие группы требований к системам видеонаблюдения:

- функциональные требования;
- требования к видеоаналитике и системам хранения;
- требования к зонам наблюдения.

При этом, в явном виде требования по информационной безопасности к системам видеонаблюдения не предъявляются.

В РФ имеется два основных регулятора в области информационной безопасности (ИБ): ФСБ и ФСТЭК. Их задачи представлены в соответствующих руководящих документах[9].[1]

В рамках исследования рассматриваемый вопрос относится к ведению ФСТЭК. Исходя из этого далее будем использовать руководящие документы

7 ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования.

8 1) ГУВО МВД РФ Рекомендации по комплексному оборудованию банков, пунктов обмена валюты, оружейных и ювелирных магазинов, коммерческих и других фирм и организаций техническими средствами охраны, видеоконтроля и инженерной защиты. Типовые варианты Р 78.36.003-99.

2) ГУВО МВД РФ Выбор и применение телевизионных систем видеоконтроля. Рекомендации. Р 78.36.002-99

3) Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности».

4) Постановление Правительства РФ от 25.03.2015 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)».

5) Постановление Правительства РФ от 08.06.2023 № 944 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальных органов, а также подведомственных и относящихся к их сфере деятельности организаций».

6) Постановление Правительства РФ от 26 сентября 2016 г. № 969 «Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности» (с изменениями и дополнениями).

7) Распоряжение Правительства Москвы от 20 июля 2007 г. № 1529-РП «О Концепции по повышению безопасности и антитеррористической защищенности гостиничных предприятий города Москвы».

9 1) Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности».

2) Указ Президента РФ от 16.08.2004 № 1085 (ред. от 08.11.2023) «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).

ФСТЭК. Также в рамках статьи будем рассматривать типовую распределенную систему видеонаблюдения критической инфраструктуры РФ[10] (не путать с критической информационной инфраструктурой). В первую очередь это обусловлено ограниченностью объема статьи (дополнительное рассмотрение web-камер во дворах частных домовладений значительно увеличит объем статьи), а также несоизмеримостью затрачиваемого ресурса на добывание информации из частного домовладения и ее ценностью в оперативных масштабах (в условиях ограниченности временного ресурса).

В то же время получение доступа к многофункциональной интеллектуальной системе контроля дорожного движения в заданном регионе даст практически неограниченный разведывательный ресурс без необходимости физического присутствия на территории противника.

Система видеонаблюдения, являясь элементом комплексной системы безопасности, позволяет в режиме реального времени осуществлять визуальный контроль охраняемого объекта и своевременно реагировать на инциденты. Получаемая от web-камер информация в режиме реального времени отражает состояние охраняемого объекта (либо объектов), за которыми ведется наблюдение (автомобильные дороги, железнодорожные пути и другие объекты критической инфраструктуры).

Сама по себе информация, передаваемая с каждой из web-камер по отдельности в явном виде, не относится ни к одному из видов информации, определенных нормативными документами в РФ:

1. Общедоступная информация[11].
2. Информация ограниченного доступа:
   - информация, содержащая сведения, составляющие государственную тайну[12];
   - конфиденциальная информация (служебная тайна, персональные данные)[13].

Получаемая с web-камер информация (например, с камер торгового центра, камер контроля дорожного движения, камер, установленных в общественном транспорте, в метро и т.д.) в явном виде не является общедоступной, в то же время она не относится к информации, содержащей сведения, составляющие государственную тайну, и не относится к конфиденциальной информации[14].

Таким образом, циркулирующая в системах видеонаблюдения информация, в явном виде не относится к первым двум категориям, но при этом вся ее совокупность относится к защищаемой информации. Циркулирующая информация однозначно является информацией ограниченного доступа, но в то же время согласно руководящим документам эта информация не относится ни к одному виду информации, которая подлежит защите.

В данном случае сам процесс отнесения информации к защищаемой требует от регулятора четких рекомендаций, определяющих порядок:

- классификации подобной информации и отнесения ее либо к существующим видам информации, либо создания нового класса информации (например: «информация, циркулирующая в комплексных системах безопасности») для комплексных систем безопасности;
- обеспечения информационной безопасности для комплексных систем безопасности (а в частности, для систем видеонаблюдения на объектах критической инфраструктуры).

Основные угрозы для типовых систем видеонаблюдения. Предлагаемые меры безопасности

На основе открытых источников, включающих в себя руководства администраторов, инструкции по монтажу и эксплуатации и т.п. различных коммерческих структур, предлагающих готовые решения для систем видеонаблюдения (в том числе контроля трафика, пропускного режима и контроля транспорта на объектах) была сформирована типовая структура территориально распределенной системы видеонаблюдения (рис. 2).

Исходя из типовой структуры территориально распределенной системы видеонаблюдения далее сформируем перечень угроз и актуальных мер защиты от них. Для решения задач этого типа ФСТЭК России создал специализированный онлайн инструмент[15], в данный момент проходящий этап опытной эксплуатации. Дальнейшее исследование проводилось с использованием этого инструментария.

На первоначальном этапе формирования перечня угроз и актуальных мер защиты ФСТЭК предполагает определение негативных последствий, которые могут возникнуть в результате нарушения функционирования системы видеонаблюдения. Из предлагаемого ФСТЭК перечня негативных последствий (52 негативных последствия), напрямую с системами видеонаблюдения связано 24 последствия. Также к негативным были отнесены не явные на первый взгляд последствия. Например: «Н.1 Угроза жизни или здоровью», «Н.31 Причинение ущерба жизни

10 Что такое критическая инфраструктура [Электронный ресурс] URL: https://esg.kaspersky.com/ru/future-tech/what-is-critical-infrastructure

11 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

12 Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1.

13 Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

14 Перечень нормативных актов, относящих сведения к категории ограниченного доступа (Материал подготовлен специалистами КонсультантПлюс) [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_93980/

15 Банк данных угроз безопасности информации [Электронный ресурс] URL: https://bdu.fstec.ru/threat-section/potential

Рис. 2. Типовая структура территориально распределенной системы видеонаблюдения

и здоровью людей», были выбраны как негативные последствия, т.к. с помощью систем видеонаблюдения ВСУ осуществляли контроль за перемещением штурмовых групп, отдельных подразделений ВС РФ и т.д., наносили ракетно-артиллеристские удары и т.п.

В качестве основных актуальных угроз (ФСТЭК выделяет 11 угроз) для систем видеонаблюдения были выбраны:

- УБИ.1 – Угроза утечки информации.
- УБИ.2 – Угроза несанкционированного доступа.
- УБИ.5 – Угроза удаления информационных ресурсов.
- УБИ.6 – Угроза отказа в обслуживании.
- УБИ.7 – Угроза ненадлежащего (нецелевого) использования.
- УБИ.8 – Угроза нарушения функционирования (работоспособности).
- УБИ.9 – Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника.
- УБИ.11 – Угроза несанкционированного массового сбора информации.

Угрозы УБИ.3 (угроза несанкционированной модификации (искажения)), УБИ.4 (угроза несанкционированной подмены) и УБИ.10 (угроза распространения противоправной информации) теоретически возможны, но их реализация достаточно сложна и ресурсозатратна, в связи с чем эти угрозы не рассматривались.

На этапе выбора объекта воздействия были отобраны следующие объекты, свойственные для распределенных систем видеонаблюдения:

- 0.1 – Автоматизированное рабочее место;
- 0.2 – Сервер;
- 0.3 – Периферийное оборудование;
- 0.4 – Устройство хранения данных;
- 0.5 – Устройство интернета-вещей;
- 0.6 – Активное сетевое оборудование;
- 0.11 – Информация (данные), содержащаяся в системах и сетях;
- 0.12 – Физические линии связи.

Объекты воздействия 0.7 Обеспечивающие системы, 0.8 Телефония (VoIP, GSM), 0.9 Средства защиты информации, 0.10 Мобильное устройство – вынесены в ограничения, т.к. не являются обязательными для систем видеонаблюдения.

На следующем шаге было осуществлено уточнение компонент объектов воздействия и определен тип нарушителей. Согласно руководящим документам, ФСТЭК выделяет 4 уровня возможностей нарушителя[16] (рис. 3).

В рассматриваемой нами ситуации нарушителями являются специальные службы иностранных государств, т.е. согласно рис. 3 – нарушитель, обладающий высокими возможностями. Однако, как правило, для защиты от специальных служб иностранных

16 Банк данных угроз безопасности информации [Электронный ресурс] URL: https://bdu.fstec.ru/threat-section/potential

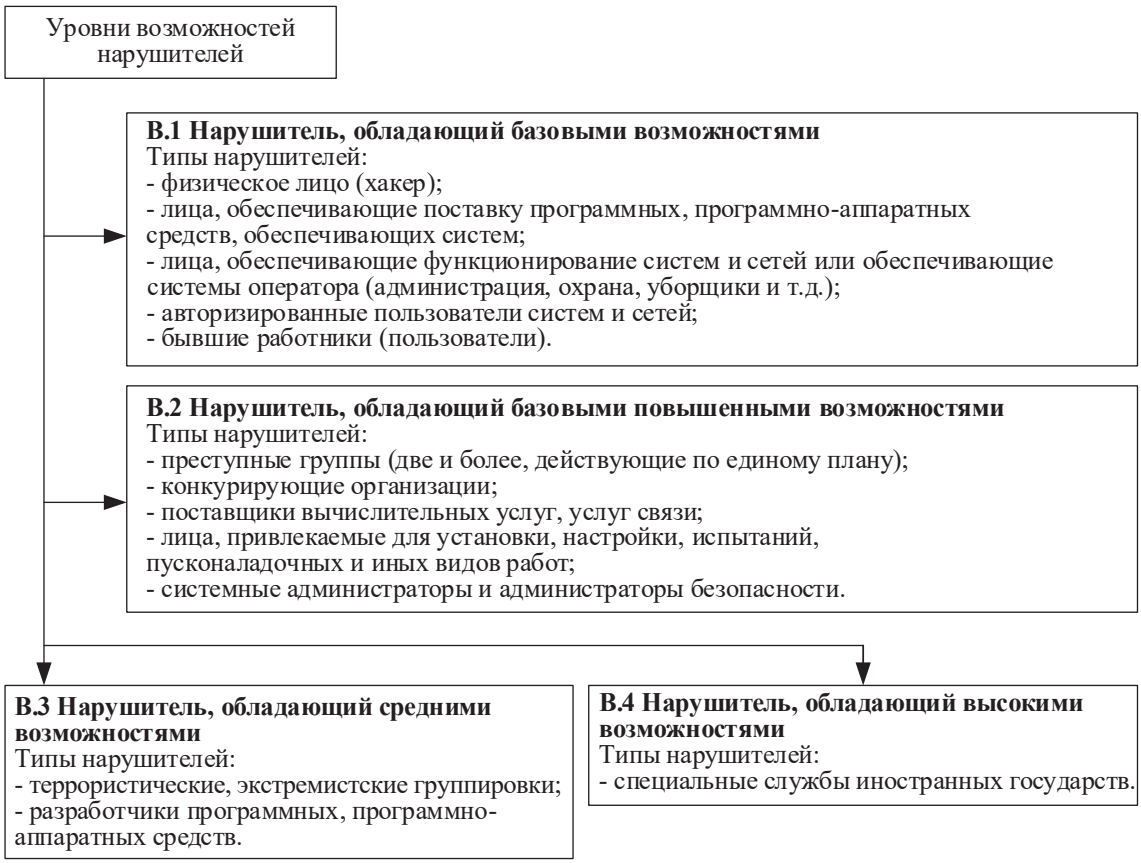


Рис. 3. Уровни возможностей нарушителей (согласно ФСТЭК)

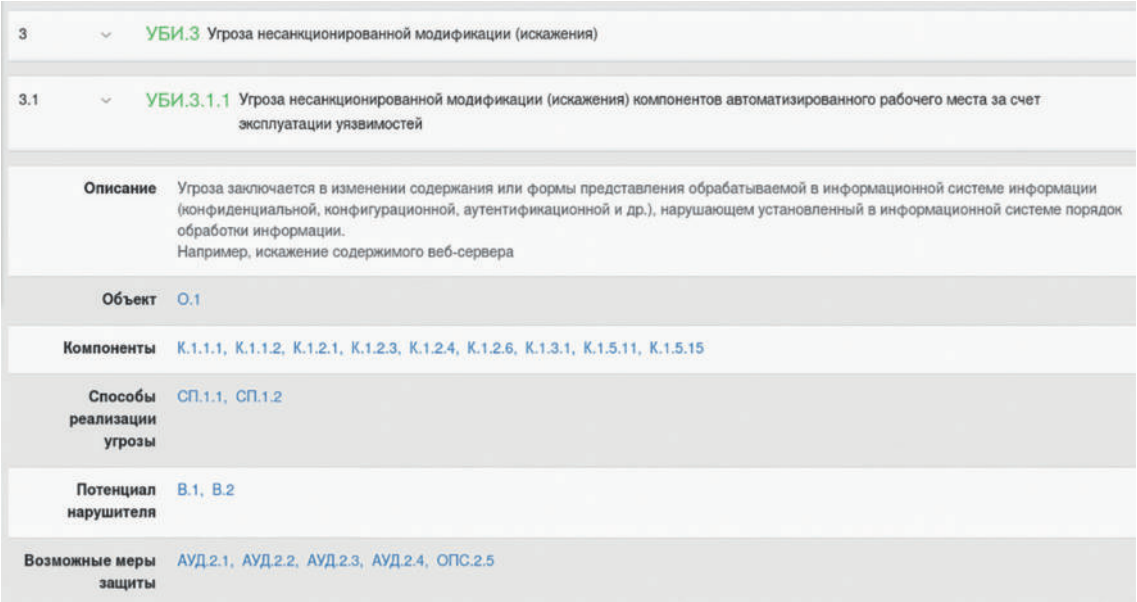


Рис. 4. Пример описания угроз безопасности информации

государств необходимо реализовать обширный перечень требований информационной безопасности с соответствующими значительными финансовыми вложениями. Также для иностранных спецслужб интерес представляет ограниченное число систем видеонаблюдения, которое существенно меньше общего количества существующих систем. Исходя из этого нарушитель В.4 был вынесен в ограничения. Далее в качестве нарушителей будем рассматривать нарушителей В.1, В.2 и В.3.

Исходя из описанных выше исходных данных, программным средством ФСТЭК был сформирован

перечень возможных угроз безопасности информации. Пример описания угрозы представлен на рис. 4.

Полученные результаты были сохранены в файл формата *.JSON и посредством специально разработанного для этой задачи парсера были преобразованы в 39 страничный документ формата *.pdf . Учитывая ограниченный объем статьи, далее будут представлены основные результаты исследования.

Согласно руководящим документам ФСТЭК с учетом описанных выше исходных данных, для распределенных систем видеонаблюдения актуальными угрозами являются угрозы, представленные в Таблице 1.

Таблица 1.

Актуальные угрозы безопасности

Угроза	Номер угрозы
Угроза утечки информации	УБИ.1.1.1[17], УБИ.1.1.2, УБИ.1.1.3, УБИ.1.1.4, УБИ.1.1.5, УБИ.1.1.7, УБИ.1.1.8, УБИ.1.1.9, УБИ.1.1.10, УБИ.1.1.11, УБИ.1.1.12, УБИ.1.1.13, УБИ.1.1.16, УБИ.1.1.18, УБИ.1.1.24, УБИ.1.1.25, УБИ.1.2.1, УБИ.1.2.2, УБИ.1.2.3, УБИ.1.2.4, УБИ.1.2.5, УБИ.1.2.7, УБИ.1.2.8, УБИ.1.2.9, УБИ.1.2.10, УБИ.1.2.11, УБИ.1.2.12, УБИ.1.2.13, УБИ.1.2.16, УБИ.1.2.18, УБИ.1.2.25, УБИ.1.3.1, УБИ.1.3.2, УБИ.1.3.3, УБИ.1.3.4, УБИ.1.3.5, УБИ.1.3.10, УБИ.1.3.18, УБИ.1.4.1, УБИ.1.4.2, УБИ.1.4.3, УБИ.1.4.4, УБИ.1.4.5, УБИ.1.4.10, УБИ.1.4.18, УБИ.1.5.1, УБИ.1.5.2, УБИ.1.5.3, УБИ.1.5.4, УБИ.1.5.5, УБИ.1.5.10, УБИ.1.5.18, УБИ.1.6.1, УБИ.1.6.2, УБИ.1.6.3, УБИ.1.6.4, УБИ.1.6.5, УБИ.1.6.7, УБИ.1.6.10, УБИ.1.6.11, УБИ.1.6.16, УБИ.1.6.18, УБИ.1.6.25, УБИ.1.12.3, УБИ.1.12.7, УБИ.1.12.10, УБИ.1.12.11, УБИ.1.12.16, УБИ.11.1.1, УБИ.11.1.2, УБИ.11.1.3, УБИ.11.1.4, УБИ.11.1.5, УБИ.11.1.7, УБИ.11.1.8, УБИ.11.1.9, УБИ.11.1.13, УБИ.11.1.18, УБИ.11.1.25, УБИ.11.2.1, УБИ.11.2.2, УБИ.11.2.3, УБИ.11.2.4, УБИ.11.2.5, УБИ.11.2.7, УБИ.11.2.8, УБИ.11.2.9, УБИ.11.2.13, УБИ.11.2.18, УБИ.11.2.25, УБИ.11.3.1, УБИ.11.3.2, УБИ.11.3.3, УБИ.11.3.4, УБИ.11.3.5, УБИ.11.3.9, УБИ.11.3.18, УБИ.11.5.1, УБИ.11.5.2, УБИ.11.5.3, УБИ.11.5.4, УБИ.11.5.5, УБИ.11.5.9, УБИ.11.5.18, УБИ.11.6.1, УБИ.11.6.2, УБИ.11.6.3, УБИ.11.6.4, УБИ.11.6.5, УБИ.11.6.7, УБИ.11.6.9, УБИ.11.6.18, УБИ.11.6.25
Угроза несанкционированного доступа	УБИ.2.1.1, УБИ.2.1.2, УБИ.2.1.3, УБИ.2.1.4, УБИ.2.1.5, УБИ.2.1.7, УБИ.2.1.10, УБИ.2.1.13, УБИ.2.1.16, УБИ.2.1.17, УБИ.2.1.18, УБИ.2.1.19, УБИ.2.1.23, УБИ.2.1.24, УБИ.2.1.25, УБИ.2.2.1, УБИ.2.2.2, УБИ.2.2.3, УБИ.2.2.4, УБИ.2.2.5, УБИ.2.2.7, УБИ.2.2.10, УБИ.2.2.13, УБИ.2.2.16, УБИ.2.2.17, УБИ.2.2.18, УБИ.2.2.19, УБИ.2.2.23, УБИ.2.2.25, УБИ.2.3.1, УБИ.2.3.2, УБИ.2.3.3, УБИ.2.3.4, УБИ.2.3.5, УБИ.2.3.10, УБИ.2.3.17, УБИ.2.3.18, УБИ.2.3.23, УБИ.2.4.1, УБИ.2.4.2, УБИ.2.4.3, УБИ.2.4.4, УБИ.2.4.5, УБИ.2.4.10, УБИ.2.4.17, УБИ.2.4.18, УБИ.2.4.23, УБИ.2.5.1, УБИ.2.5.2, УБИ.2.5.3,УБИ.2.5.4, УБИ.2.5.5, УБИ.2.5.10, УБИ.2.5.17, УБИ.2.5.18, УБИ.2.5.23, УБИ.2.6.1, УБИ.2.6.2, УБИ.2.6.3, УБИ.2.6.4, УБИ.2.6.5, УБИ.2.6.7, УБИ.2.6.10, УБИ.2.6.16, УБИ.2.6.17, УБИ.2.6.18, УБИ.2.6.23, УБИ.2.6.25, УБИ.2.12.3, УБИ.2.12.7, УБИ.2.12.10, УБИ.2.12.16, УБИ.2.12.17.
Угроза удаления информационных ресурсов	УБИ.5.1.1, УБИ.5.1.2, УБИ.5.1.3, УБИ.5.1.4, УБИ.5.1.5, УБИ.5.1.10, УБИ.5.1.13, УБИ.5.1.14, УБИ.5.1.15, УБИ.5.1.16, УБИ.5.1.18, УБИ.5.1.19, УБИ.5.1.21, УБИ.5.1.23, УБИ.5.1.24, УБИ.5.1.25, УБИ.5.2.1, УБИ.5.2.2, УБИ.5.2.3, УБИ.5.2.4, УБИ.5.2.5, УБИ.5.2.10, УБИ.5.2.13, УБИ.5.2.14, УБИ.5.2.15, УБИ.5.2.16, УБИ.5.2.18, УБИ.5.2.19, УБИ.5.2.21, УБИ.5.2.23, УБИ.5.2.25, УБИ.5.4.1, УБИ.5.4.2, УБИ.5.4.3, УБИ.5.4.4, УБИ.5.4.5, УБИ.5.4.10, УБИ.5.4.18, УБИ.5.4.23, УБИ.5.6.1, УБИ.5.6.2, УБИ.5.6.3, УБИ.5.6.4, УБИ.5.6.5, УБИ.5.6.10, УБИ.5.6.14, УБИ.5.6.16, УБИ.5.6.18, УБИ.5.6.23, УБИ.5.6.25, УБИ.5.12.3, УБИ.5.12.10, УБИ.5.12.14, УБИ.5.12.16

17 УБИ – угроза безопасности информации, 1.1.1 – номер угрозы в банке угроз информационной безопасности ФСТЭК

Угроза	Номер угрозы
Угроза отказа в обслуживании	УБИ.6.1.1, УБИ.6.1.2, УБИ.6.1.4, УБИ.6.1.5, УБИ.6.1.14, УБИ.6.1.15, УБИ.6.1.19, УБИ.6.1.21, УБИ.6.1.23, УБИ.6.1.24, УБИ.6.1.25, УБИ.6.2.1, УБИ.6.2.2, УБИ.6.2.4, УБИ.6.2.5, УБИ.6.2.14, УБИ.6.2.15, УБИ.6.2.19, УБИ.6.2.21, УБИ.6.2.23, УБИ.6.2.25, УБИ.6.3.1, УБИ.6.3.2, УБИ.6.3.4, УБИ.6.3.5, УБИ.6.3.14, УБИ.6.3.23, УБИ.6.4.1, УБИ.6.4.2, УБИ.6.4.4, УБИ.6.4.5, УБИ.6.4.14, УБИ.6.4.23, УБИ.6.5.1, УБИ.6.5.2, УБИ.6.5.4, УБИ.6.5.5, УБИ.6.5.14, УБИ.6.5.23, УБИ.6.6.1, УБИ.6.6.2, УБИ.6.6.4, УБИ.6.6.5, УБИ.6.6.7, УБИ.6.6.14, УБИ.6.6.23, УБИ.6.6.25, УБИ.6.12.7, УБИ.6.12.14
Угроза ненадлежащего (нецелевого) использования	УБИ.7.1.1, УБИ.7.1.2, УБИ.7.1.4, УБИ.7.1.5, УБИ.7.1.11, УБИ.7.1.18, УБИ.7.1.19, УБИ.7.1.23, УБИ.7.1.24, УБИ.7.1.25, УБИ.7.2.1, УБИ.7.2.2, УБИ.7.2.4, УБИ.7.2.5, УБИ.7.2.11, УБИ.7.2.18, УБИ.7.2.19, УБИ.7.2.23, УБИ.7.2.25, УБИ.7.4.1, УБИ.7.4.2, УБИ.7.4.4, УБИ.7.4.5, УБИ.7.4.18, УБИ.7.4.23, УБИ.7.5.1, УБИ.7.5.2, УБИ.7.5.4, УБИ.7.5.5, УБИ.7.5.18, УБИ.7.5.23, УБИ.7.6.1, УБИ.7.6.2, УБИ.7.6.4, УБИ.7.6.5, УБИ.7.6.11, УБИ.7.6.18, УБИ.7.6.23, УБИ.7.6.25
Угроза нарушения функционирования (работоспособности)	УБИ.8.1.1, УБИ.8.1.2, УБИ.8.1.4, УБИ.8.1.5, УБИ.8.1.13, УБИ.8.1.14, УБИ.8.1.15, УБИ.8.1.16, УБИ.8.1.18, УБИ.8.1.19, УБИ.8.1.21, УБИ.8.1.23, УБИ.8.1.24, УБИ.8.1.25, УБИ.8.2.1, УБИ.8.2.2, УБИ.8.2.4, УБИ.8.2.5, УБИ.8.2.13, УБИ.8.2.14, УБИ.8.2.15, УБИ.8.2.16, УБИ.8.2.18, УБИ.8.2.19, УБИ.8.2.21, УБИ.8.2.23, УБИ.8.2.25, УБИ.8.3.1, УБИ.8.3.2, УБИ.8.3.4, УБИ.8.3.5, УБИ.8.3.18, УБИ.8.3.23, УБИ.8.4.1, УБИ.8.4.2, УБИ.8.4.4, УБИ.8.4.5, УБИ.8.4.18, УБИ.8.4.23, УБИ.8.5.1, УБИ.8.5.2, УБИ.8.5.4, УБИ.8.5.5, УБИ.8.5.18, УБИ.8.5.23, УБИ.8.6.1, УБИ.8.6.2, УБИ.8.6.4, УБИ.8.6.5, УБИ.8.6.7, УБИ.8.6.16, УБИ.8.6.18, УБИ.8.6.23, УБИ.8.6.25, УБИ.8.7.1, УБИ.8.7.2, УБИ.8.7.4, УБИ.8.7.5, УБИ.8.7.18, УБИ.8.7.23, УБИ.8.12.7, УБИ.8.12.16
Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника	УБИ.9.11.2, УБИ.9.11.4, УБИ.9.11.5, УБИ.9.11.13, УБИ.9.11.25
Угроза несанкционированного массового сбора информации	УБИ.11.1.1, УБИ.11.1.2, УБИ.11.1.3, УБИ.11.1.4, УБИ.11.1.5, УБИ.11.1.7, УБИ.11.1.8, УБИ.11.1.9, УБИ.11.1.13, УБИ.11.1.18, УБИ.11.1.25, УБИ.11.2.1, УБИ.11.2.2, УБИ.11.2.3, УБИ.11.2.4, УБИ.11.2.5, УБИ.11.2.7, УБИ.11.2.8, УБИ.11.2.9, УБИ.11.2.13, УБИ.11.2.18, УБИ.11.2.25, УБИ.11.3.1, УБИ.11.3.2, УБИ.11.3.3, УБИ.11.3.4, УБИ.11.3.5, УБИ.11.3.9, УБИ.11.3.18, УБИ.11.5.1, УБИ.11.5.2, УБИ.11.5.3, УБИ.11.5.4, УБИ.11.5.5, УБИ.11.5.9, УБИ.11.5.18, УБИ.11.6.1, УБИ.11.6.2, УБИ.11.6.3, УБИ.11.6.4, УБИ.11.6.5, УБИ.11.6.7, УБИ.11.6.9, УБИ.11.6.18, УБИ.11.6.25

Актуальными способами реализации угроз являются:

1. Эксплуатация уязвимостей (СП.1.1[18], СП.1.2).
2. Атака типа «человек посередине» (СП.10.1, СП.10.2, СП.10.4, СП.10.7).
3. Применение скрытых каналов (СП.11.1).
4. Считывание вводимой и выводимой информации (СП.12.1, СП.12.3, СП.12.6, СП.12.9).
5. Реализация социальной инженерии (СП.13.1, СП.13.2, СП.13.3, СП.13.4, СП.13.5, СП.13.6, СП.13.7, СП.13.8).
6. Атака типа «отказ в обслуживании» (СП.14.1, СП.14.10, СП.14.2, СП.14.3, СП.14.4, СП.14.5, СП.14.6, СП.14.7, СП.14.8).
7. Шифрование данных (СП.15.1, СП.15.2).
8. Нарушение изоляции (СП.16.2, СП.16.3).
9. Подбор (восстановление) аутентификационной информации (СП.17.1, СП.17.10, СП.17.11, СП.17.2, СП.17.3, СП.17.8, СП.17.9).

18 СП – способ реализации угрозы, 1.1 – номер угрозы в банке угроз информационной безопасности ФСТЭК

10. Использование недостатков механизмов разграничения доступа (СП.18.1, СП.18.2).
11. Модификация ОС (подмена системных файлов, внедрение вредоносного кода в системные процессы и ядро ОС) (СП.19.1, СП.19.2, СП.19.3, СП.19.4).
12. Использование недостатков конфигурации (СП.2.1, СП.2.10, СП.2.11, СП.2.2, СП.2.3, СП.2.4, СП.2.6, СП.2.7, СП.2.8, СП.2.9).
13. Повреждение данных (СП.21.2, СП.21.3).
14. Модификация (подмена) прошивки (микропрограммы) (СП.23.1, СП.23.2).
15. Физическое воздействие (СП.24.2, СП.24.3).
16. Использование недостатков архитектуры (СП.3.1).
17. Внедрение вредоносного программного обеспечения (СП.4.1, СП.4.10, СП.4.12, СП.4.2, СП.4.3, СП.4.4, СП.4.5, СП.4.6, СП.4.8, СП.4.9).
18. Внедрение программных и аппаратных закладок (СП.5.1, СП.5.2, СП.5.3, СП.5.4, СП.5.5, СП.5.7).
19. Прослушивание (захват) сетевого трафика (СП.7.1, СП.7.2, СП.7.3, СП.7.4, СП.7.5, СП.7.6, СП.7.7).
20. Сканирование сетевой инфраструктуры (СП.8.1, СП.8.2, СП.8.4, СП.8.5, СП.8.6).
21. Изучение информации о системе (СП.9.1, СП.9.2, СП.9.3, СП.9.4, СП.9.5, СП.9.6, СП.9.7).

С учетом актуальных угроз и способов их реализации программным средством ФСТЭК был сформирован перечень актуальных мер защиты в количестве 221 меры.

Представленное исследование показывает, что обеспечение информационной безопасности систем видеонаблюдения не является тривиальной задачей, а требует большого количества мер защиты и как следствие значительных финансовых вложений. Но даже при наличии финансовой составляющей имеются объективные причины, не позволяющие одномоментно обеспечить информационную безопасность систем видеонаблюдения. Среди основных причин можно выделить:

- отсутствие нормативной базы, однозначно определяющей порядок обеспечения информационной безопасности комплексных систем безопасности;
- необходимость подготовки (доподготовки) специалистов, обладающих соответствующими компетенциями в области обеспечения информационной безопасности систем комплексной безопасности.

Выводы

Результаты исследования показывают, что для защиты систем видеонаблюдения необходимо реализовать достаточно обширный список мероприятий. Однако необходимо учитывать, что исследование ориентировано на нарушителя В.3, и для нарушителей В.1 и В.2 перечень мероприятий будет существенно уменьшен.

Тем не менее одномоментное введение требований по информационной безопасности (описанных в результатах исследования) для систем видеонаблюдения по объективным причинам для большинства систем будет сложно реализуемо. В связи с чем, необходим переходной этап с пошаговым усилением требований ИБ и постепенной тестовой эксплуатацией систем с функционирующей на них системой информационной безопасности.

Касательно нормативной базы применительно к системам видеонаблюдения необходима разработка:

- нормативных документов, определяющих требования информационной безопасности к системам видеонаблюдения;
- типовых моделей угроз и нарушителя для систем видеонаблюдения;
- методических документов, позволяющих осуществлять классификацию информации, циркулирующей в системах видеонаблюдения и отнесения ее либо к существующим видам информации, либо к созданию нового класса информации (например: «информация, циркулирующая в комплексных системах безопасности») для комплексных систем безопасности;
- методических рекомендаций, регулирующих порядок обеспечения информационной безопасности для комплексных систем безопасности (а в частности, для систем видеонаблюдения на объектах критической инфраструктуры);
- методических рекомендаций, регулирующих порядок проведения тематических исследований программного обеспечения используемого в системах видеонаблюдения на отсутствие недекларированных возможностей.

Литература

1. *Стародубцев Ю. И., Закалкин П. В. Структурно-функциональный анализ конфликтной ситуации между государственной системой обеспечения информационной безопасности и иностранной системой деструктивных воздействий // Вопросы кибербезопасности. 2024. №4(62). С.82–91. DOI: 10.21681/2311-3456-2024-4-82-91.*
2. *Иванов С. А. Трансформация роли единой сети электросвязи Российской Федерации в системе военного управления в результате реализации процессов цифровой трансформации и глобализации // Вопросы радиоэлектроники. Серия: Техника телевидения. 2021. №3. С.17–23.*
3. *Иванов С. А. Устойчивость сетей связи общего пользования в условиях глобализации // Известия Тульского государственного университета. Технические науки. 2021. № 9. С. 86–90. DOI: 10.24412/2071-6168-2021-9-86-90.*

4. Коцыняк М.А., Лаута О.С., Нечепуренко А.П. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного противоборства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 1–2 (127-128). С. 58–62.
5. Бречко А.А., Сазыкин А.М. Проблема управления параметрами киберпространства в интересах субъектов критической информационной инфраструктуры Российской Федерации // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2022. № 5–6 (167-168). С. 36–43.
6. Закалкин П.В. Аспекты использования киберпространства в интересах корпоративных систем управления // Труды Научно-исследовательского института радио. 2021. № 4. С. 23–32. DOI: 10.34832/NIIR.2021.7.4.003.
7. Starodubtsev Y.I., Balenko E.G., Zakalkin P.V., Fedorov V.H. Change dynamics for forms and opportunities of centers of power under globalization // В сборнике: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. 2020. С. 9271172. DOI: 10.1109/FarEastCon50210.2020.9271172
8. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Многовекторный конфликт в киберпространстве как предпосылка формирования нового вида вооруженных сил // Военная мысль. 2021. №12. С. 126–135.
9. Hwang Y.-W., Lee I.-Y., Kim H., Lee H., Kim D. Current status and security trend of OSINT // Wireless Communications and Mobile Computing. 2022. Т. 2022. С. 1290129. DOI: 10.1155/2022/1290129.
10. Махнин В.Л. О законах и формах войны // Вестник академии военных наук. 2024. №2(87). С.45–53.
11. Гаврилов А.Д., Грудинин И.В., Майбуров Д.Г., Новиков В.А. Два года специальной военной операции: некоторые итоги, вероятные перспективы // Вестник академии военных наук. 2024. №2(87). С. 54–64.
12. Белов А.С., Добрышин М.М., Шугуров Д.Е. Научно-методический подход к оцениванию качества систем обеспечения информационной безопасности // Приборы и системы. Управление, контроль, диагностика. 2022. № 11. С. 34–40. DOI: 10.25791/pribor.11.2022.1373.
13. Добрышин М.М. Выбор структуры и механизмов адаптивного управления системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки. 2022. № 2. С. 214–223. DOI: 10.24412/2071-6168-2022-2-214-223.
14. Толстой А.И. Системотехника обеспечения безопасности объектов в информационной сфере // Вопросы кибербезопасности. 2024. № 5 (63). С. 47–57 DOI: 10.21681/2311-3456-2024-5-47-57.

CYBERSECURITY OF VIDEO SURVEILLANCE SYSTEMS IN THE CONTEXT OF INFORMATION TECHNOLOGY IMPACTS

Starodubtsev Yu. I.[19], Zakalkin P. V.[20], Karasev S. V.[21]

Keywords: *cyberspace, information technology impacts, cybersecurity, video surveillance, threats, intruder, information security.*

The purpose of the study: *to consider the procedure for the implementation of information technology impacts on video surveillance systems; to assess the existing information security requirements for video surveillance systems in the Russian Federation; to form generalized proposals to ensure the information security of existing video surveillance systems in conditions of deliberate information technology impacts.*

The results obtained: *a generalized scheme of the procedure for the implementation of information technology impacts on video surveillance systems has been formed; generalized proposals for ensuring the information security of existing video surveillance systems have been formulated; proposals for the development of regulatory documentation by regulators (in the field of information security) have been formulated.*

Scientific novelty: *the analysis of the conflict situation in the field of video surveillance systems has been carried out, which made it possible to identify the initial measures necessary for the subsequent development of information security of video surveillance systems.*

Research methods: *system analysis, classification, comparative analysis.*

References

1. Starodubcev Yu. I., Zakalkin P. V. Strukturno-funkcional'nyj analiz konfliktnoj situacii mezhdu gosudarstvennoj sistemoj obespecheniya informacionnoj bezopasnosti i inostrannoj sistemoj destruktivnyh vozdejstvij // Voprosy kiberbezopasnosti. 2024. №4(62). S. 82–91. DOI: 10.21681/2311-3456-2024-4-82-91.
2. Ivanov S. A. Transformaciya roli edinoj seti elektrosvyazi Rossijskoj Federacii v sisteme voennogo upravleniya v rezul'tate realizacii processov cifrovoj transformacii i globalizacii // Voprosy radioelektroniki. Seriya: Tekhnika televideniya. 2021. №3. S. 17–23.

19 Yuri Starodubtsev, Honored Scientist of the Russian Federation, Honored Inventor of the Russian Federation, Doctor of Military Sciences, Professor, Professor of the Department, Military Academy of Communications, Saint Petersburg, Russia. E-mail: prof.starodubtsev@gmail.com, https://orcid.org/0000-0001-5140-4476
20 Pavel Zakalkin, Ph.D., Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: pzakalkin@mail.ru, https://orcid.org/0000-0003-2946-2586
21 Stas Karasev, Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: llmaglu@mail.ru

3. *Ivanov S.A. Ustojchivost' setej svyazi obshchego pol'zovaniya v usloviyah globalizacii // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2021. № 9. S. 86–90. DOI: 10.24412/2071-6168-2021-9-86-90.*
4. *Kocynyak M.A., Lauta O.S., Nechepurenko A.P. Metodika ocenki ustojchivosti informacionno-telekommunikacionnoj seti v usloviyah informacionnogo protivoborstva // Voprosy oboronnoj tekhniki. Seriya 16: Tekhnicheskie sredstva protivodejstviya terrorizmu. 2019. № 1-2 (127-128). S. 58–62.*
5. *Brechko A.A., Sazykin A.M. Problema upravleniya parametrami kiberprostranstva v interesah sub"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii // Voprosy oboronnoj tekhniki. Seriya 16: Tekhnicheskie sredstva protivodejstviya terrorizmu. 2022. № 5-6 (167-168). S. 36–43.*
6. *Zakalkin P.V. Aspekty ispol'zovaniya kiberprostranstva v interesah korporativnyh sistem upravleniya // Trudy Nauchno-issledovatel'skogo instituta radio. 2021. № 4. S. 23–32. DOI: 10.34832/NIIR.2021.7.4.003.*
7. *Starodubtsev Y.I., Balenko E.G., Zakalkin P.V., Fedorov V.H. Change dynamics for forms and opportunities of centers of power under globalization // V sbornike: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. 2020. S. 9271172. DOI: 10.1109/FarEastCon50210.2020.9271172.*
8. *Starodubcev Yu.I., Zakalkin P.V., Ivanov S.A. Mnogovektornyj konflikt v kiberprostranstve kak predposylka formirovaniya novogo vida vooruzhennyh sil // Voennaya mysl'. 2021. №12. S. 126–135.*
9. *Hwang Y.-W., Lee I.-Y., Kim H., Lee H., Kim D. Current status and security trend of OSINT // Wireless Communications and Mobile Computing. 2022. T. 2022. S. 1290129. DOI: 10.1155/2022/1290129.*
10. *Mahnin V.L. O zakonah i formah vojny // Vestnik akademii voennyh nauk. 2024. №2(87). C. 45–53.*
11. *Gavrilov A.D., Grudinin I.V., Majburov D.G., Novikov V.A. Dva goda special'noj voennoj operacii: nekotorye itogi, veroyatnye perspektivy // Vestnik akademii voennyh nauk. 2024. №2(87). C. 54–64.*
12. *Belov A.S., Dobryshin M.M., SHugurov D.E. Nauchno-metodicheskij podhod k ocenivaniyu kachestva sistem obespecheniya informacionnoj bezopasnosti // Pribory i sistemy. Upravlenie, kontrol', diagnostika. 2022. № 11. S. 34–40. DOI: 10.25791/pribor.11.2022.1373.*
13. *Dobryshin M.M. Vybor struktury i mekhanizmov adaptivnogo upravleniya sistemy obespecheniya informacionnoj bezopasnosti // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2022. № 2. S. 214–223. DOI: 10.24412/2071-6168-2022-2-214-223.*
14. *Tolstoj A.I. Sistemotekhnika obespecheniya bezopasnosti ob"ektov v informacionnoj sfere // Voprosy kiberbezopasnosti. 2024. № 5 (63). S. 47–57 DOI: 10.21681/2311-3456-2024-5-47-57.*

О ПЕРВОЙ РОССИЙСКОЙ ПРОФЕССИОНАЛЬНОЙ СЕРТИФИКАЦИИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ «СЕРТИФИЦИРОВАННЫЙ СПЕЦИАЛИСТ ПО КИБЕРБЕЗОПАСНОСТИ»

Дорофеев А. В.[1]

DOI: 10.21681/2311-3456-2025-1-147-149

Введение

Специалистам по информационной безопасности, как и другим ИТ-профессионалам, часто требуется подтверждение своих знаний в различных ситуациях: на собеседованиях, при переходе на новую работу или в борьбе за выгодный контракт. Наличие широко признаваемого сертификата может значительно упростить решение данных задач [1–4].

В мировой практике существует более десятка сертификаций для специалистов нашего профиля, каждая из которых имеет свою направленность. Самые известные из них: Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), CompTIA Security+ и Offensive Security Certified Professional (OSCP).

К примеру, общее количество сертифицированных специалистов CISSP составляет более 156 000 человек. Данная независимая сертификация всячески поддерживается государством, например, прохождение ее рекомендуется для ряда категорий служащих США, в том числе в Министерстве обороны.

Требования Министерства обороны США по наличию сертификатов у персонала

Вид сертификата		
IAM Level I	IAM Level II	IAM Level III
CAP, CND, Cloud+, GSLC, Security+ CE, H CISPP	CAP, CASP+ CE, CISM, CISSP (или Associate CISSP), GSLC, CCISO, HCISPP	CISM, CISSP (или Associate CISSP), GSLC, CCISO
IASAE I	IASAE II	IASAE III
CASP+ CE, CISSP (или Associate CISSP), CSSLP	CASP+ CE, CISSP (или Associate CISSP), CSSLP	CISSP-ISSAP, CISSP-ISSEP, CCSP

Рис. 1. Требования к специалистам по директиве US DoD 8570

Что касается нашей страны, то обычной практикой является включение требований по наличию сертифицированных специалистов CISSP в условиях контрактов на выполнение работ в ИТ-области. Это является объективным фактором востребованности сертификации специалистов.

Однако после 2022 года доступ для российских специалистов к получению этих международных сертификатов значительно затруднился.

Для заполнения этого пробела авторы данной статьи предложили создание российского аналога для CISSP и CISM — сертификацию ССК (Сертифицированный специалист по кибербезопасности). Были организованы подготовительные курсы, а также сдача сертификационных экзаменов.

Ниже мы поделимся своим опытом создания системы профессиональной сертификации.

Обзор доменов

Основным элементом любой системы профессиональной сертификации является набор доменов, на основе которых формулируются вопросы экзамена [5–10]. В системе сертификации мы выбрали следующие восемь ключевых доменов:

1. Менеджмент информационной безопасности;
2. Законодательство в области информационной безопасности;
3. Безопасный доступ;
4. Сетевая безопасность;
5. Криптография;
6. Обеспечение непрерывности и восстановления;
7. Контроль и мониторинг информационной безопасности;
8. Разработка безопасного программного обеспечения.

Эти домены охватывают основные аспекты профессиональных знаний в области кибербезопасности, и их понимание позволяет специалистам решать актуальные задачи в своих организациях.

«Менеджмент информационной безопасности» является ключевым доменом, так как основная задача специалистов по кибербезопасности — защитить организацию, которая их наняла. Для этого важно не только уметь применять современные технологии информационной безопасности, но и управлять процессами информационной безопасности в организации. Ведь в конечном итоге информационная безопасность в организации зависит от каждого, кто имеет доступ к защищаемой информации.

В ходе подготовительных курсов в рамках данного домена мы рассматриваем основные понятия информационной безопасности: активы, угрозы, меры безопасности, риски и СМИБ (система менеджмента

1 Дорофеев Александр Владимирович, CISSP, CISA, CISM, директор Учебного центра «Эшелон». Россия. Москва. E-mail: ad@cnpo.ru

информационной безопасности). Подробно разбираем цикл Деминга (PDCA) и ГОСТ Р ИСО/МЭК ИСО 27001. Отдельное внимание уделяется формированию в организации понятной системы организационно-распорядительной документации, а также проведению внутреннего аудита СМИБ.

Одной из ключевых целей информационной безопасности в организации является выполнение нормативных требований. Эти требования существуют не только для самой организации и её конкретных процессов, но и для информационных систем, используемых для поддержки этих процессов, а также для средств защиты информации.

Специалист по кибербезопасности должен хорошо ориентироваться в требованиях законодательства в области информационной безопасности, так как они служат основой для формирования внутренних документов организации по информационной безопасности и являются критериями для проведения различных проверок со стороны регулирующих органов.

Домен «Безопасный доступ» посвящен ряду важных тем, связанных с управлением доступом к данным. Основными темами домена являются различные типы моделей управления доступом, технологии аутентификации и идентификации и современные атаки на данные системы.

Другим ключевым доменом является «Сетевая безопасность». Специалист по кибербезопасности должен понимать, как функционируют сети, хорошо ориентироваться в угрозах, которые могут быть реализованы на различных уровнях семиуровневой модели ISO/OSI, а также уметь применять ключевые технологии сетевой безопасности: IDS/IPS, межсетевое экранирование и т.п.

Домен «Криптография» посвящён криптографической защите информации при ее хранении и передаче. Домен включает в себя темы, посвященные алгоритмам шифрования с секретным/открытым ключом, хеш-функциям, протоколам безопасности. В ходе подготовительных курсов по этому домену рассматриваются как российские, так и зарубежные стандарты.

Обеспечение доступности информационных систем и данных является ключевой задачей обеспечения информационной безопасности. Поэтому в системе сертификации специалиста по кибербезопасности нельзя не включить домен, посвященный обеспечению непрерывности бизнеса и восстановлению организации после разрушений, бедствий, критических ситуаций или аварий. Хорошее знание этого домена позволит подготовить организацию к оперативному реагированию на различные негативные события, а также обеспечить ее непрерывное функционирование.

Специалист по кибербезопасности должен быть максимально компетентен в таких аспектах, как выявление киберугроз, попыток вторжения злоумышленников, а также реагирования на инциденты информационной безопасности. Именно этим вопросам посвящен домен «Контроль и мониторинг информационной безопасности».

Уязвимое программное обеспечение представляет значительный риск для безопасности любой организации. Чтобы минимизировать уязвимости, компании-производители программного обеспечения внедряют процессы безопасной разработки, предусматривающие различные меры на всех стадиях цикла создания программного обеспечения. В этом контексте мы добавили отдельный домен, посвящённый разработке безопасного программного обеспечения. В ходе подготовительных курсов мы подробно рассматриваем положения ГОСТ Р 56939, активное участие в создании которого принимали участие эксперты нашей испытательной лаборатории.

Форматы экзаменов

Система сертификации предусматривает два вида экзаменов: экзамен на статус кандидата и на статус специалиста (рис. 2). Первый экзамен проводится в онлайн формате и является бесплатным, что позволяет попробовать свои силы неограниченному кругу российских специалистов. Второй экзамен доступен пока только в оффлайн формате, в рамках которого не допускается возможность списывания. Длительность кандитатского экзамена – 2 часа, в ходе которых нужно ответить на 100 вопросов, а экзамена на статус специалиста – 4 часа, и количество вопросов уже – 200. Проходной балл – 70 % правильных ответов.

Каждый вопрос содержит четыре варианта ответа, и испытуемому необходимо выбрать наилучший.

Для подготовки к экзаменам имеются онлайн и оффлайн курсы, которые проводятся экспертами группы компаний «Эшелон». Причём доступен бесплатный онлайн курс, к которому можно присоединиться, пройдя регистрацию по ссылке https://etecs.ru/ssc/. Видео с прошлого курса выложено на наших каналах в YouTube https://www.youtube.com/playlist?list=PLAs36PQnfDQ0-U7iGV2Z6_1v-s9RXktHc и RuTube https://rutube.ru/plst/429175/. Для общения слушателей курса и разбора вопросов в Telegram организованы канал https://t.me/sskquestions и группа https://t.me/cybersecspec. Также в настоящее время идет работа по написанию учебного пособия.

Отдельно стоит обратить внимание, что статус «Сертифицированный специалист по кибербезопасности» присваивается специалистам, которые успешно сдали оффлайн-экзамен, а также подтвердили наличие опыта по нескольким доменам экзамена не менее 5 лет. В случае наличия высшего образования в области информационной безопасности необходимо подтвердить опыт не менее 4 лет.

Рис. 2. Сертификаты специалистов

Первые итоги

Первый эксперимент показал, что созданная система сертификации вызвала большую заинтересованность у российских специалистов в области информационной безопасности. На онлайн курсы по подготовке к экзамену «Сертифицированный специалист по кибербезопасности» (ССК) от учебного центра «Эшелон» получено уже более 3 тыс. регистраций. По итогам первого курса, проведенного в 2024-м году, 269 участников участвовало в сдаче онлайн-экзамена, из которых 163 набрали более 70 баллов из 100 возможных и стали кандидатами ССК. Среди слушателей специалисты из России, Узбекистана, Казахстана и других стран СНГ. Размер группы слушателей в Telegram уже более 760 подписчиков.

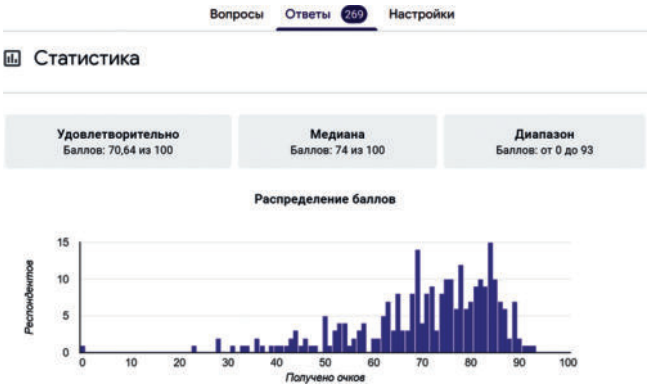


Рис.3. Распределение результатов онлайн теста ССК

В результате проведения оффлайн-экзамена, а также акции выдачи сертификата российским специалистам, обладающим действующими сертификатами CISSP и CISM, количество обладателей статуса ССК уже превысило 30 человек.

Заключение

Учебный центр «Эшелон» провел указанный эксперимент с целью демонстрации возможности альтернативной (негосударственной) независимой сертификации специалистов в нашей стране с привлечением всех заинтересованных лиц от ведущих компаний и ВУЗов страны. Возможно, данная идея покажется привлекательной специалистам Союзного государства и ОДКБ [11].

В планах активистов ССК в настоящее время стоят следующие задачи:

- расширение списка организаций-партнеров, отвечающих за создание и развитие базы вопросов сертификационного экзамена;
- расширение списка учебных заведений, проводящих подготовительные курсы и прием экзамена.

Литература

1. *Дорофеев А. В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С. 65–68.*
2. *Лившиц И. И. Проблемы подготовки специалистов в области информационной безопасности // Вестник ДГТУ. Технические науки. 2024. Т. 51. № 1. С. 123–131. DOI: 10.21822/2073-6185-2024-51-1-123-131.*
3. *Чванова М. С., Киселева И. А., Анурьева М. С. Зарубежный опыт подготовки специалистов для наукоемких технологий // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2021. Т. 26. № 190. С. 7–24. DOI: 10.20310/1810-0201-2021-26-190-7-24.*
4. *Seidakhmetova F., Pasekova M., Sarygulova R., Sholpanbayeva K. Training of Specialists in the Field of Information Security // Statistics, Accounting and Audit. 2023. № 2 (89). С. 40–46. DOI:10.31992/0869-3617-2022-31-2-82-93.*
5. *Барабанов А. В., Дорофеев А. В., Марков А. С., Цирлов В. Л. Семь безопасных информационных технологий / Под. ред. А. С. Маркова. М.: ДМК Пресс, 2017. 221 с.*
6. *Дорофеев А. В., Марков А. С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67–73.*
7. *Дорофеев А. В., Марков А. С. Планирование обеспечения непрерывности бизнеса и восстановления // Вопросы кибербезопасности. 2015. № 3 (11). С. 68–73.*
8. *Марков А. С., Цирлов В. Л. Безопасность доступа: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 2 (10). С. 60–68.*
9. *Марков А. С., Цирлов В. Л. Основы криптографии: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 1 (9). С. 65–73.*
10. *Петренко Ю. А., Петренко С. А. Лучшая практика управления непрерывностью бизнеса // Защита информации. Инсайд. 2010. № 5 (35). С. 12–21.*
11. *Марков А. С. Проблемные вопросы международной сертификации специалистов по информационной безопасности // В сб. трудов XVIII Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». М.: НАМИБ, 2024. С. 82–85.*

CYBERSECURITY ISSUES

SCIENTIFIC PEER-REVIEWED JOURNAL

2025, № 1 (65)

Cybersecurity Issues is a research periodical scientific and practical publication specializing in information security.
Published six times a year

https://cyberrus.info

The journal is being published from 2013
(Registration Certificate PI No. FS 77-75239).
CrossRef number (DOI): 10.21681/2311-3456

The journal is included in the Russian list of peer-reviewed academic publications of the Higher Attestation Commission (VAK), it is registered in the Russian Science Citation Index (RSCI/RINTs) on the Web of Science (WoS) platform and holds the 1st place in its cyber security rating. The journal's articles are available in full text

Founder and publisher
JSC «NPO «Echelon»
Postal address: Elektrozavodskaya str., 24, bld. 1, 107023, Moscow, Russia
E-mail: editor@cyberrus.info

CONTENTS

1-3 апреля, 2025
Астана, МВЦ EXPO

Kazakhstan
Security Systems

Kazakhstan Security Systems

kss-expo.kz

1 день

4 конференции

90+ спикеров

1000+ участников

ТЕРРИТОРИЯ БЕЗОПАСНОСТИ 2025: ВСЕ PRO ИБ

3 Апреля

www.comnews-conferences.ru/ru/conference/tb2025/

CYBERSECURITY ISSUES
VOPROSY KIBERBEZOPASNOSTI

№1 2025

DOI: 10.21681/2311-3456

- Multi-level vulnerabilities
- Asset Management
- Cybersecurity of video surveillance systems

www.cyberrus.info
editor@cyberrus.info