ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

№6 2023 (58)

DOI: 10.21681/2311-3456

Риск-ориентированный подход

Обнаружение вторжений

Международная безопасность

ФСТЭК России – 50 лет!

История создания и деятельности нынешней Федеральной службы по техническому и экспортному контролю началась 18 ноября 1973 года.

Все глобальные изменения, произошедшие в нашей стране после 1973 года по настоящее время, отразились и в названиях этой важной и нужной государственной структуры, обеспечивающей национальную безопасность государства в области защиты информации.

Постановлением ЦК КПСС и Совета Министров СССР от 18 декабря 1973 г. № 903—303 «О противодействии иностранной технической разведке» была создана Государственная комиссия СССР по противодействию иностранным техническим разведкам (Гостехкомисия СССР).

Указом Президента СССР от 22 мая 1991 г. № УП-2003 «Об образовании Государственной технической комиссии СССР по противодействию иностранным техническим разведкам» Гостехкомисия СССР была подчинена Президенту СССР.

Указом Президента Российской Федерации от 5 января 1992 г. № 9 «О создании Государственной технической комиссии при Президенте Российской Федерации» создана Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России).

В соответствии с Указом Президента Российской Федерации от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» вместо существовавшей Государственной технической комиссии при Президенте Российской Федерации был создан (преобразован) федеральный орган исполнительной власти — Федеральная служба по техническому и экспортному контролю Российской Федерации.

Положение о Федеральной службе по техническому и экспортному контролю (ФСТЭК России) утверждено Указом Президента РФ от 16 августа 2004 г. № 1085.

В соответствии с Положением, ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

Полвека сотрудники Гостехкомиссии СССР- ФСТЭК России стоят на страже нашей Отчизны и в наше сложное время делают все возможное для обеспечения обороноспособности Государства Российского!

Честь и слава сотрудникам ФСТЭК России!

С Юбилеем!

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ

№6 (58) 2023 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 перечень научных изданий, в которых должны быть опубликованы основные результаты исследований соискателей учёных степеней кандидата и/или доктора наук, а также в российский индекс научного цитирования RSCI на международной платформе научных публикаций Web of Science (WoS)

Учредитель и издатель

АО «Научно-производственное объединение «Эшелон»

Над номером работали:

Г.И. Макаренко – *шеф-редактор* И.Ю.Шахалов – *отв. секретарь*

И.М. Ануфриев – *дизайн*

Подписано к печати 20.11.2023 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

О ВЕРОЯТНОСТНОМ ПРОГНОЗИРОВАНИИ РИСКОВ В ИНФОРМАЦИОННОЙ ВОЙНЕ. ЧАСТЬ 1. АНАЛИЗ СТРАТЕГИЙ ОПЕРАЦИЙ И КОНТРОПЕРАЦИЙ ДЛЯ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

Манойло А.В.[1], Костогрызов А.И.[2]

Цель 1-й части работы: *на основе анализа основных стратегий операций и контроопераций в информационной войне (ИВ) сформировать общие положения подхода к математическому моделированию с тем, чтобы во 2-й заключительной части предложить модель и методы для вероятностного прогнозирования частных и интегрального рисков и с их помощью провести системный анализ выявленных возможностей по управлению рисками в ИВ.*

Результат работы: *на основе результатов анализа стратегий операций и контроопераций (в 1-й части статьи) предложены модель и методы для вероятностного прогнозирования частных и интегрального рисков в ИВ. На основе их применения разработаны примеры, иллюстрирующие работоспособность предложенного подхода. Для отдельных ретроспективных данных проведен системный анализ выявленных возможностей по управлению рисками в ИВ (во 2-й заключительной части статьи).*

Научная новизна: *сегодня воздействие разнородных угроз при ведении ИВ в международном публичном медиапространстве выражается в целенаправленных компрометирующих выдумках резонансного характера (лжефактах, лженамерениях), способствующих опорочиванию и дискредитации репутации государства, его руководства и иных представителей власти. Эта лицевая сторона ИВ видна всем потребителям информации, но без адекватной дифференциации «истина» — «ложь». Изучению этой лицевой стороны посвящены политологические исследования. В отличии от этих исследований в настоящей работе предложена математическая основа для системного анализа развития информационных операций и возможных способов противодействия им. Результаты математического моделирования операций и контроопераций ИВ представляются на количественном уровне вероятностных прогнозов рисков в терминах вероятностей «успеха» и «неудачи» в зависимости от конкретных исходных данных, формируемых по фактам или оцениваемых гипотетически. В работе изучены возможности по востребованным способам противодействия операциям в ИВ с указанием достижимых количественных оценок для управления рисками.*

Ключевые слова: *вероятность, репутация, модель, прогнозирование, риск, системный анализ, угроза.*

DOI: 10.21681/2311-3456-2023-6-2-19

1. Введение

В настоящей работе под информационной войной (ИВ) понимается особый вид гибридной войны, осуществляемый с применением информационных операций со стороны противника и мер противодействия (контроопераций) со стороны защищающейся стороны. ИВ охватывает управление психикой человека (его сознанием и подсознанием), и через это операции в ИВ направлены в итоге на дискредитацию репутации государства, его руководства и иных представителей власти в глазах мирового сообщества с последующим принуждением к подчинению неким «правилам» в интересах тех сторон, которые развязывают ИВ. Репутация государства, его руководства и иных представителей власти рассматривается как стихийно складыва-

1 Манойло Андрей Викторович, доктор политических наук, кандидат физико-математических наук, профессор МГУ им. М.В. Ломоносова, профессор факультета политологии МГУ им. М.В. Ломоносова. Москва, Россия. E-mail: Cyberhurricane@yandex.ru

2 Костогрызов Андрей Иванович, доктор технических наук, профессор, Федеральный исследовательский центр «Информатика и управление» Российской академии наук. Москва, Россия. E-mail: Akostogr@gmail.com

ющийся в массовом общественном сознании образ государства, его руководства и иных представителей власти, отражающий характер ожидаемых от них действий или поведения внутри государства и на международной политической арене. По сути репутация – это некий ценный виртуальный актив, используемый для поддержания конкурентоспособности и эффективного развития государства и подлежащий особому хранению и защите, в т. ч. в условиях ИВ.

Примечание. Несмотря на всю важность, в сферу настоящих исследований ИВ, сосредоточенных на управлении психикой человека, не вошли кибероперации, которые преимущественно направлены на технические системы[3].

Информационные операции, столь распространенные сегодня, несколько лет назад присутствовали практически исключительно в деятельности спецслужб и были элементами оперативных игр, разыгрываемых разведками. Ситуативность складывания сценария самих оперативных игр и преследуемые ими сугубо тактические цели, вызванные желанием чем-нибудь «зацепить» противника или на чем-нибудь его подловить, не давали возможности выйти информационным операциям на оперативный простор. В этом контексте сам термин «информационная война» на протяжении многих десятилетий не воспринимался серьезно: его считали ловкой находкой «газетчиков», пытающихся таким путем поднять тираж своих изданий. Похоже, серьезно к информационным операциям с самого начала отнеслись только военные США, уже в 1988 году внесшие термин «психологическая операция» в Полевой устав Армии FM 33.1-1.

Сами же информационные операции к 2014 году уже начинают складываться как самостоятельный вид деятельности, но в их планировании продолжают преобладать «ремесленный» подход. Каждая операция разрабатывается индивидуально, как уникальный образец, под нее подбирается такая же уникальная (и неповторимая, подготовленная под конкретные особенности конкретной оперативной остановки) схема организации, не похожая ни на одну из предыдущих.

Однако, в 2014 г. все существенно меняется: Крым добровольно входит в состав Российской Федерации. Для Запада это решение народа Крыма становится настоящим шоком, похоже, ни США, ни Турция такого от крымчан не ожидали. Возможность прямого военного вмешательства в форме, например, высадки десанта, в 2014 году у США и НАТО имелась, но была упущена. В этом плане у США остался только один весомый инструмент агрессивного ответа – информационные операции. Гибридизация современных войн вывела ИВ на новую ступень эволюции, в условиях разнородных факторов и неопределенностей, начинают использоваться разнообразные стратегии ведения ИВ. При этом в информационных операциях появляются новые инструменты – например, «фейки» (заведомо ложная информация провокационного и резонансного характера), сочетание которых с различными технологиями распространения информации сделало их абсолютным информационным оружием, угрожающим национальной безопасности государств [1-4]. Спайка фейков и вирусных технологий произошла в 2016 году в период президентской избирательной кампании в США [1, 5].

Сегодня создается устойчивое впечатление, что теория живет отдельно, практика (в виде «Скрипалей», «Аргентинского кокаинового дела», «Панамского досье» и др. — см. далее) – отдельно, и они не только не помогают друг другу, но и слабо пересекаются. В этом и заключается основная причина торможения развития отечественной научной школы исследования ИВ. Разрыв между теорией и практикой, в первую очередь на уровне научно обоснованных количественных прогнозов и управления рисками в условиях разнообразных неопределенностей, обусловливает актуальность настоящей работы.

В условиях разнородных неопределенностей для проведения научно-практических исследований ИВ остро востребовано математическое моделирование систем. При этом в качестве моделируемой системы предлагается рассматривать виртуальную репутацию государства, его руководства и иных представителей власти в условиях реализации разнородных угроз ИВ. Цель настоящей работы состоит в предложении востребованных модели и методов для вероятностного прогнозирования частных и интегрального рисков в ИВ и с их помощью на основе отдельных ретроспективных данных – в проведении прогнозного анализа выявленных возможностей по управлению рисками в ИВ.

Примечания. 1. Под системой понимается комбинация взаимодействующих элементов, организованная для достижения одной или нескольких поставленных целей (по ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем»).

2. Под риском понимается 1) мера опасности с ее последствиями (по ФЗ «О техническом регулиро-

3 В концепциях национальной безопасности США и РФ нанесение внезапного кибердара может быть приравнено к объявлению войны со всеми вытекающими последствиями, т.е. кибератаки могут спровоцировать прямой вооруженный конфликт даже между ядерными державами, что делает их чрезвычайно опасными и в мирное время.

вании», ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты», ГОСТ Р 51901.1-2002 «Менеджмент риска. Анализ риска технологических систем», ГОСТ Р 51897-2011 «Менеджмент риска. Термины и определения» и др.) или как более общее определение — 2) эффект неопределенности в целях и/или задачах (по ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство).

Работа состоит из двух частей.

В настоящей, 1-й части, проведен анализ основных стратегий ИВ, мер противодействия операциям ИВ (контроопераций), характера стратегических операций ИВ [1-9]. По результатам этого анализа разработаны общие положения математического моделирования для прогнозирования рисков и системного анализа выявленных возможностей по управлению рисками в ИВ. Развитие операций и контроопераций ИВ формализовано с использованием понятия моделируемой системы. Получаемые результаты математического моделирования операций и контроопераций ИВ для моделируемой системы используются в интерпретации к исходной системе, в интересах которой проводятся соответствующие расчеты. На основе рассмотренных ретроспективных данных определены некоторые правдоподобные диапазоны возможных значений исходных данных применительно к математическому моделированию и извлечению аналитических знаний для изучения возможностей по прогнозированию рисков (во 2-й части статьи).

Во 2-й заключительной части «Модель, методы, примеры» предложены модель и методы для вероятностного прогнозирования частных и интегрального рисков в ИВ. С их помощью на основе отдельных ретроспективных данных на примерах проиллюстрирована работоспособность модели и методов и проведен системный анализ выявленных возможностей по управлению рисками в ИВ.

2. Анализ основных стратегий

Ситуация с внезапным вхождением Крыма в состав Российской Федерации побудила специальные службы США реагировать на ходу, «с колес», поскольку времени на раскачку, как было замечено президентом России В. В. Путиным[4], у них уже не было. В этом плане прежние подходы к ведению ИВ, отличающиеся высокой избирательностью, не годились. В 2014 г. США остро нуждались именно в массовом проведении информационных операций. Это, в свою очередь, привело разведывательное сообщество США к идее перевода процессов планирования, организации и проведения информационных операций на промышленные рельсы. «Промышленный» подход, в свою очередь, привел к унификации организационно-технологических схем информационных операций, которые в итоге свелись в одну единственную универсальную базовую схему, появившуюся у американских спецслужб ориентировочно к лету 2015 г. Эта схема впервые получила свое «боевое крещение» в печально знаменитом скандале с «Панамским досье» 2016 г. В этом деле стандартная схема информационных операций, представляющая собой итерационную последовательность вбросов и технологических пауз («периодов тишины»), присутствует в чистом, незамутненном и абсолютно незамаскированном виде, ее легко можно разглядеть даже неспециалисту. Благодаря этой схеме «Панамский скандал», как известно, имел определенный успех. С этого самого момента все информационные операции спецслужб США становятся репликой «Панамского досье».

Новые стратегии ИВ и соответствующие технологические решения, выработанные США, дали возможность не только повысить частоту проведения самих операций (то есть, поставить их производство на конвейер), но и позволили испытывать на этой платформе различные оперативные сценарии и сюжеты, сделавшие современные информационные операции похожими на телевизионные сериалы. Так, в «Деле об отравлении Скрипалей» (совместной операции британских и американских спецслужб, продолжающейся еще и в настоящее время) только в течение одного 2018 г. были отработаны два сценария – «игра с пошаговым повышением ставок» и «ловля на живца» или приманку. В скандале с т.н. аргентинским кокаином – «ловля на приманку», в роли которой выступал сам кокаин, арестованный аргентинской полицией безопасности. «Дело Марии Бутиной» — это прием «ловли на живца», причем в роли «живца» выступила сама фигурантка дела, задержанная ФБР за создание в США «российской шпионской сети». История с перехватом в Генте в 2018 г. крупной партии кокаина, промаркированной символикой, похожей на символику «Единой России», — это «наклеивание ярлыков». «Выборы в Интерпол» (ноябрь 2018), завершившиеся срывом избрания российского кандидата А. Прокоп-

4 «Времени на раскачку нет» — одна из самых знаменитых цитат В. В. Путина. Например, в 2018 году на инаугурации: «Жизнь постоянно ставит перед нами новые вызовы, новые непростые задачи, и над их решением нам ещё предстоит напряженно работать. Времени на раскачку нет». См.: «Владимир Путин вступил в должность Президента России». http:// kremlin.ru, 7 мая 2018 г. URL: http://kremlin.ru/events/president/news/57416

чука, – это сценарий «скрытой угрозы», и т.д. [5]. Благодаря этим сценариям информационные операции превратились в тонкую многоходовую психологическую игру с привязкой ко временной оси.

В настоящей работе основные стратегии ИВ проанализированы на примере информационных операций против России. Анализ проведен в интересах разработки общих положений математического моделирования операций и контроопераций ИВ для прогнозирования рисков и системного анализа возможностей по управлению рисками в ИВ. Рассмотрены три основные стратегии: последовательного «удушения», «загонной охоты» и шантажа.

2.1. Стратегия «удушения» (так называемая «Петля Анаконды»)

Это — стратегия последовательно «удушения» конкретного политического лидера (как правило, президента страны) путем организации его травли сразу по нескольким независимым друг от друга направлениям, в определенный момент сходящимся в одном фокусе и дающим кумулятивный эффект.

Таким фокусом может стать выдвинутое в адрес лидера государства какое-либо особо тяжкое обвинение – например, в терроризме (радиационном, химическом, бактериологическом) и наркоторговле, на котором в определенный момент одновременно фокусируются все линии, отрабатываемые организаторами травли. Суммарный эффект от внезапной трансформации множества различных версий в один «окончательный» и «не подлежащий обжалованию» вердикт нередко лишает жертву травли не только «воздуха» (жертва начинает «задыхаться», утратив волю к сопротивлению), но и воли к самой жизни и к ее продолжению. В этой стратегии каждый новый этап реализации любой из линий травли (каждая новая операция или оперативная комбинация) должна еще сильнее сжимать «удавку», наброшенную на «шею» лидера, сжимая его грудь и легкие «на выдохе» — в тот самый момент, когда он в очередной раз среагирует на очередную провокацию и тем самым «откроется» перед противником — подставит себя под удар. Если он в таком положении «сделает выдох», обратно «набрать воздух в легкие» ему уже не дадут – «петля анаконды» на его груди и шее сожмется ровно настолько, насколько при выдохе сократилась его грудная клетка, и через некоторое время жертва просто погибнет от удушья.

Типичным примером применения «Петли Анаконды» на оперативном уровне (в рамках одной стратегической операции ИВ) являются:

- цепочка «Литвиненко – Скрипаль — Навальный», в которой обвинения в отравлениях с каждым этапом набирают обороты и становятся все более радикальными;
- цепочка «Бутина (обвиненная в создании разведывательно-диверсионно-террористической сети на территории США) – Аверьянов (обвиненный в создании диверсионно-террористической сети на территории ЕС) – «отравители Навального» (обвиненные в создании диверсионно-террористической сети на территории РФ»);
- линия «ядов» (полоний-новичок-вакцина);
- линия создания «террористических сетей и инфраструктуры» (одиночная группа «Петров-Боширов» в Солсбери – «в/ч 29155» и сеть баз в Европе – попытка создания такой же сети в США);
- явно вырисовывающаяся «кокаиновая» цепочка (поставок): «Аргентина (2017 г., 0,4 т.) – Бельгия (2018 г., 2 т.) – Кабо-Верде (2019 г., 9,5 т.).

При этом организаторы травли придерживаются следующего технологического приёма. Так, например, если в отношении лидера государства одновременно разворачиваются три кампании по его дискредитации по трем различным «основаниям» – по обвинению в политических убийствах (кампания №1), наркоторговле (№2) и покровительстве наемникам (№3), то ошибки, допущенные жертвой при попытке отразить удар, нанесенный по первой линии, сразу же используется для того, чтобы нанести удар с другого направления – по второй линии, а при попытке жертвы отразить и этот удар новая атака на нее приходит с направления №3. Так жертву травли, изматывая, «гоняют по кругу», и она вынуждена ради своего спасения хаотично метаться от одного источника угрозы к другому, пытаясь их нейтрализовать хотя бы на время.

Как именно действует стратегия «Петли Анаконды» в ИВ против России, показано на рис. 1. Для наглядной иллюстрации на рис. 2 показана последовательность информационных атак на РФ и ее лидера, выстроенная в хронологическом порядке.

2.2. Стратегия «загонной охоты»

Суть – в приклеивании на лидера ярлыка «международного преступника (террориста)» и организация его «международного уголовного преследования»): состоит в выдвижении прямых обвинений в терроризме и подведении конкретных представителей российского руководства под действие Freedom Act USA, допускающего внесудебную ликвидацию «главарей и пособников террористических группировок», или в

Рис. 1. «Петля анаконды» в ИВ против России. ©А.В. Манойло

Рис. 2. Хронологическая шкала информационных атак на РФ и ее лидера. ©А.В. Манойло

назначении за их головы конкретного денежного вознаграждения (как за Н. Мадуро и его сторонников в 2020 г.).

В рамках данной стратегии сходящимися линиями, например, могут быть «обвинения России в убийствах американских солдат в Афганистане» или «дело Навального» (идущее в развитии общей линии, заданной «делом Скрипалей»). Все это новейшие варианты стратегии «загонной охоты» 2020 года.

2.3. Стратегия прямого шантажа

«Венесуэльский прецедент» (2019) и попытка государственного переворота в Беларуссии (2020) показали, что на определенном этапе стратегической операций ее мишени – лидеру страны – может быть задан прямой вопрос: на что ты готов пойти ради того, чтобы сохранить свои активы за рубежом (если они есть) и даже жизнь?

Причем, если лидер страны не поймет сделанного ему намека, то его можно подвести под действие Freedom Act USA и затем ликвидировать без суда и следствия (как К. Сулеймани 03.01.2020 г.), или назначить за его голову цену, объявив особо опасным международным преступником (военным преступником или даже «наркотеррористом»), как это было сделано в отношении Н. Мадуро и его соратников в 2020 году.

Типичными примерами шантажа могут служить факты:

— 13 марта 2018г. Т. Мэй предъявила России ультиматум, согласно которому Россия в течение 24 часов должна «правдоподобно объясниться» по поводу инцидента в Солсбери (т. е. публично признать свою вину в отравлении С. и Ю. Скрипалей), иначе Великобритания будет рассматривать «химическую атаку в Солсбери» как акт военной агрессии[5];

— захват 32 российских граждан (и одного гражданина Республики Беларусь) в Белоруссии по обвинению в участии в т. н. «ЧВК Вагнера» и «подготовке терактов», угроза выдачи этих людей СБУ;

— ультиматум, выдвинутый США и группой стран по поводу избрания А. Прокопчука на выборах в Интерпол (2018).

При этом следует отметить, что, по мере нарастания накала информационной войны против РФ, шантаж со стороны США и их военно-политических союзников в отношениях с РФ становится все более грубым и используется все чаще.

На основе результатов проведенного анализа вышеизложенных стратегий и фактов для условий разнородных неопределенностей сделаны следующие выводы применительно к последующему математическому моделированию:

— основные стратегии ИВ формально могут быть описаны в терминах случайных событий, характеризующих возникновение и развитие во времени возможных угроз реализации операций ИВ для достижения цели дискредитации репутации государства, его руководства и иных представителей власти;

— для случая неприменения ответных мер противодействия информационным операциям или

5 Тереза Мэй выдвинула Москве ультиматум, согласно которому в течение 24 часов российская сторона должна правдоподобно объясниться по поводу инцидента. Срок ультиматума истек в 03:00 мск 14 марта 2018 г.». См.: Лондон официально обвинил Россию в отравлении Скрипаля. // Lenta.ru/ 2018, 13 мар. URL: https://lenta.ru/news/2018/03/14/skripal/

применения лишь пассивных мер, таких как отрицания или оправдания, указания на нестыковки в обвинениях и т. п. возникновение и развитие угроз может быть привязано к оси времени и охарактеризовано:

- возможной частотой возникновения конкретных угроз (несколько операций в год, по ретроспективным данным — в среднем около 6 операций в год);
- средним временем развития этих угроз до появления целевого негативного эффекта от реализации этих угроз (несколько месяцев, по ретроспективным данным — в среднем около 3-х месяцев);
- средним временем условно приемлемого восстановления репутации (несколько месяцев, по ретроспективным данным — в среднем около полугода).

3. Анализ мер противодействия информационным операциям

В настоящее время уже накоплен определенный опыт успешного противодействия информационным операциям США и их союзников – в том числе, в форме активных мероприятий (так называемых информационных контроопераций). В целом все применяемые меры противодействия операциям ИВ можно разделить на пять основных видов контроопераций:

1) перехват информационной повестки;
2) перехват оперативной инициативы;
3) отвлечение на негодный объект;
4) информационные прививки;
5) операции «возвратного типа» (класса «бумеранг»).

1) Перехват информационной повестки

Типичным примером такого рода мер противодействия операциям ИВ являются так называемые «Скрипальские чтения», перехватившие на 48 часов информационную повестку у западных (в основном, британских, американских и немецких) и российских СМИ с 3 по 4 марта 2019 г. – в первую годовщину инцидента в Солсбери.

2) Перехват оперативной инициативы
(или операции прямого действия).

Типичным примером такого рода мер противодействия операциям ИВ являются:

- т. н. «Дело Диосдадо Кабельо» (август 2019) – операция по разоблачению агента ЦРУ в ближайшем окружении президента Венесуэлы Н. Мадуро;
- «Русский информатор в ЦРУ», или оперативная игра в «поиск крота» с Р.О'Брайеном, помощником президента США по национальной безопасности (октябрь 2019);
- «Русская методичка» Сьюзан Райс (2020) – заявление Сьюзан Райс об использовании русскими специальной «методички» для политической дестабилизации США.

3) Отвлечение на негодный объект

Примером такого рода мер противодействия операциям ИВ стал т.н. «приезд Суркова и Манойло в Донецк» (в октябре 2019 г.) – наглядный пример того, как один информационный вброс может запустить информационное цунами.

4) Информационные прививки

Подобного рода меры предназначены для выработки у целевых аудиторий коллективного иммунитета на негативное информационное воздействие (ожидаемого содержания).

5) Операции «возвратного типа» (или операции класса «бумеранг»)

Это — информационные контроперации, рассчитанные на использование инерции, набранной операцией противника. Типичным примером такого рода операции может служить оперативная комбинация, разыгранная с США в марте 2020 г. – сразу после объявления Д. Трампа о начале «антинаркотеррористической операции» в Венесуэле. Данная операция получила название «Предупреждение Трампу: главное – не выйти на самого себя».

Далее с целью формирования множества правдоподобных исходных данных для последующего моделирования более подробно приведены результаты анализа первых двух мер (контроопераций).

В рамках анализа меры «Операции перехвата информационной повестки» необходимо отметить, что на данный момент «Скрипальские чтения» (рис. 3) уже довольно подробно описаны и разобраны как в публикациях СМИ[6], так и в различных научных источниках [5][7].

6 См.: Skripal Readings as an Example of a Special Operation to Intercept the Information Agenda. The Latest Practice of Modern Information Warfare and Psychological Operations. // Medium. 2020, Mar. 8. URL: https://medium.com/@andreimanoilo

7 См. в [5]: п. 5.1. «Скрипальские чтения» как пример специальной операции по перехвату информационной повестки.

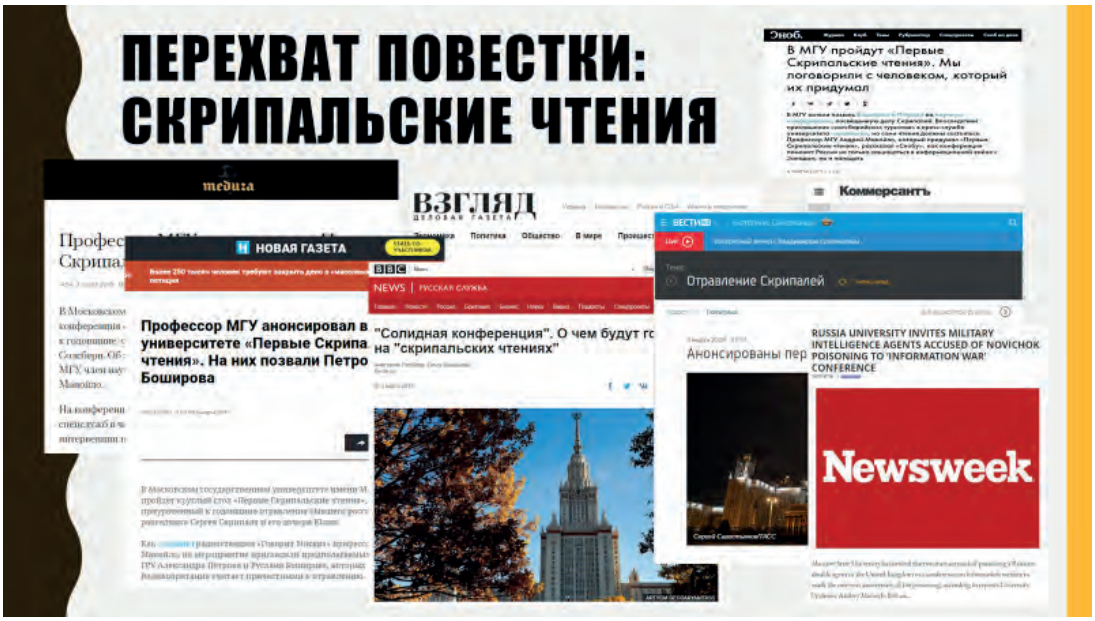

Рис. 3. «Скрипальские чтения» (3-4 марта 2019 г.): заголовки некоторых СМИ, ©А.В. Манойло

Рис. 4. «Скрипальские чтения» (3-4 марта 2019 г.): «вирусный эффект». ©А.В. Манойло

Рис. 5. «Скрипальские чтения» (3-4 марта 2019 г.): схема и результат операции. ©А.В. Манойло

Эта оперативная контроперация, проведенная 3-4 марта 2019 г. в Москве, на сегодняшний день продолжает оставаться одной из самых эффективных операций по перехвату информационной повестки – благодаря грамотно использованному тройному «вирусному эффекту» (см. рис. 4). О ее эффективности говорят статистические данные: так, за в период проведения операции (с 3 по 4 марта 2019 г.) только в одном Телеграмм-канале информационный повод захватил внимание аудитории в один миллион триста тысяч (1 304 640) человек. Совокупный же охват аудиторий в СМИ только за время проведения контроперации составил более 50 миллионов человек (опубликован 101 материал, см. рис. 5).

В рамках меры «Операция по перехвату оперативной инициативы» («операции прямого действия»), в отличие от остальных видов информационных контропераций, всегда присутствует нацеленность на нанесение противнику прямых потерь. Их результатом становятся выявленные и раскрытые тайные операции иностранных спецслужб, разоблачение их агентуры, чистки (после провалов), ведущие к потерям квалифицированных кадров, и утрата иностранными разведчиками веры в непогрешимость своего руководства и собственную неуязвимость и избранность. В то время как операции 1, 3, 4 и 5-го типов только создают условия для оказания разведывательного воздействия (перехватывают информационную повестку, отвлекают внимание противника на негодный объект и т.д.), операции прямого действия это разведывательное воздействие оказывают. Главным же итогом подобного рода операций становится перехват оперативной инициативы у противника и способность навязывать ему собственные правила игры. Но это далеко не все – как

следствие, дополнительно снижается частота возникновения разнородных угроз (т.к. необходимо время на проработку новых, еще не вскрытых идей в ведении ИВ) и растягивается среднее время развития угроз до появления целевого негативного эффекта (т.к. новые неапробированные идеи в ведении ИВ при их реализации сами наталкиваются на собственные недоработки и противодействия). Кроме того, более определенно может быть установлено реальное время восстановления на приемлемом уровне репутации государства, его руководства и иных представителей власти (которая в глазах международного сообщества может быть временно ухудшена после актов информационного воздействия со стороны противника).

Главный принцип операций прямого действия состоит в следующем: противника надо мотивировать только один раз. Все остальное он должен сделать сам, своими руками, без принуждения и лишних напоминаний, а именно: раскрыть собственную тайную операцию; выдать собственную агентуру, схемы и каналы связи; засветить кадровый состав разведчиков, участвующих в операции. И быть при этом твердо уверенным в том, что другого выхода у него нет.

В этом плане одним из важных примеров операций прямого действия является операция по разоблачению агента ЦРУ в ближайшем окружении Николаса Мадуро – так называемое «Дело Диосдадо Кабельо», проведенная в Венесуэле в августе 2019 года [7]. Эта операция, состоявшая всего из одного информационного вброса, опубликованного в венесуэльском издании «Medium» 17 августа 2019 г., вызвала настоящую панику в ЦРУ и, как следствие, привела к провалу одной из самых тщательно готовившихся и законспирированных тайных операций. Вероятно, именно из-за провала этой операции и раскрытия их агента влияния в ближайшем окружении Мадуро США временно приостановили свою работу по Венесуэле (поставили ее «на паузу» до выработки «Плана Б») вплоть до 26 марта 2020 г. – почти на семь месяцев. Схема и хронология операции подробно описана в [5][8]. Это – тот самый редкий случай, когда информационный вброс, сделанный 17 августа 2019 г., 21 августа добил до самого президента США Д. Трампа и вынудил его лично включиться в операцию по прикрытию своего агента, публично признав сам факт ведения тайных переговоров с «человеком из ближайшего окружения венесуэльского президента» (за спиной Н. Мадуро).

Другим примером операции прямого действия является оперативная игра, затеянная с новым помощником президента США по национальной безопасности Робертом О'Брайеном, сменившем в сентябре 2019 г. на этом посту Джона Болтона (уволенного 10 сентября 2019 г. президентом Д. Трампом из-за провала политики США в Венесуэле – сразу после завершения операции «Дело Диосдадо Кабельо») [5][9]. Бывший заместитель директора ЦРУ Роберт О'Брайен, придя в Белый Дом, сразу же стал выяснять, откуда «русские» узнали о контактах Д. Кабельо с ЦРУ. О'Брайен не без оснований решил, что о секретной операции русские могли узнать, только имея источник внутри разведсообщества США; значит, где-то там сидит «крот». Поиск «крота» привел людей О'Брайена к журналистам «Medium», причастным к размещению вброса о контактах Кобельо; к ним было сделано несколько разведподходов с целью выяснить, не проплатила ли эту публикацию «русская разведка».

7 октября 2019 года на сайте «Medium» появляется статья: «Andrei Manoilo: No es cierto que los rusos tengamos informantes internos en la CIA, al menos no por ahora» («Андрей Манойло: Неправда, что у русских есть свои информаторы в ЦРУ, по крайней мере, сейчас»[10], в которой Манойло, отвечая на прямой вопрос об источниках информации о связях Д. Кабельо с американской разведкой, категорически опровергает версию о том, что все материалы о Кабельо он получил от «собственного информатора в окружении директора ЦРУ или директора национальной разведки». Ответ Манойло вынесли в заголовок интервью. Когда статью увидели латиноамериканские журналисты и обозреватели, они перепечатали ее как сенсационное признание от первого лица, но тут же потеряли приставку «No»[11] (в самом начале заголовка, начинавшегося со слов «No es cierto...»). В результате категорическое отрицание превратилось в признание («у русских есть свой источник в ЦРУ»), которое, по-видимому, окончательно убедило американских разведчиков, что русский «крот» — не выдумка, он действительно существует. Опираясь на эти «сведения», Р. О'Брайен провел в структурах разведсообщества

8 См. [5]: Вирусные технологии и «эпидемии» каскадного типа на примере операции по разоблачению агента влияния ЦРУ, бывшего вице-президента Венесуэлы Диосдадо Кабельо 17-21/08/2019.

9 См. [5]: Продолжение «дела Диосдадо Кабельо»: поиск «крота».

10 См.: Andrei Manoilo (Andrey Manoylo): No es cierto que los rusos tengamos informantes internos en la CIA, al menos no por ahora. // Medium. 2019, Oct. 7 URL: https://vicentequintero.medium.com/andrei-manoilo-no-es-cierto-que-los-rusos-tengamos-informantes-internos-en-la-cia-y-la-casa-blanca-8b6c6b78bc85

11 Логический оператор «не» (логического отрицания) существует только в сознании человека; при трансляции информации из сознания в подсознание оператор «не» просто отбрасывается, и отрицание превращается в признание.

Рис. 6. «Поиск русского крота» в октябре 2019 года. ©А.В. Манойло

Рис. 7. Примеры оперативных игр (2020 г.). ©А.В. Манойло

грандиозную «чистку», в результате которой СНБ США, аппарат директора национальной разведки и оперативный директора ЦРУ покинуло несколько десятков сотрудников – в основном, специалистов по Латинской Америке и славистов (см. рис. 6). Был ли среди них русский «крот» — никто не знает.

Еще одним примером операции прямого действия является оперативная комбинация, связанная с находкой «русской методички» (по организации госпереворотов) для дестабилизации политической ситуации в США, о которой говорила Сьюзан Райс 31 мая 2020г. в эфире CNN, которую она видела своими глазами[12] (рис. 7).

В этом интервью С. Райс заявила, что «беспорядки, вызванные смертью в Миннеаполисе афроамериканца Джорджа Флойда, якобы могли быть организованы

12 См.: Экс-советник Обамы считает, что протесты в США организованы по «российской методичке». [Электронный документ] / ТАСС. Официальный сайт. 2020, 1 июня. URL: https://tass.ru/mezhdunarodnaya-panorama/8612639 (Дата обращения: 1 июня 2020 г.)

извне», подчеркнув, что уверена в российском следе в беспорядках в США: «их цель — не просто опозорить Соединенные Штаты, а разделить нас, сделать так, чтобы мы вступили в борьбу друг с другом». Свое скандальное заявление С. Райс сделала в связи с массовыми беспорядками и погромами, охватившими США в мае 2020 года.

Заявление, сделанное С. Райс, очевидно, не было случайной импровизацией. Напротив, оно было сделано намеренно, на пике роста массовых протестов в США, обеспечивших этому заявлению максимальный резонансный эффект. Теперь американцы наконец то нашли того, кто погрузил Соединенные Штаты в пучину цветной революции: этим врагом оказалась Россия. Все вместе это очень напоминало начало новой оперативной комбинации американских спецслужб, поставившей себе целью зацепить содержащимися в откровениях Райс обвинениями кого-нибудь из высокопоставленных российских чиновников (вывести их на ответную реакцию) и, тем самым, утвердить американское общество в мысли о том, что именно Россия несет главную ответственность за организацию массовых беспорядков и хаос, в который страна погрузилась после убийства Флойда. В этой комбинации вслед за первой порцией резонансных обвинений, озвученных устами С. Райс (первым информационным вбросом), обязательно должны были последовать другие, способные за несколько последовательных итераций довести российское руководство до «белого каления», заставив их «отрицать очевидное», изворачиваться или оправдываться. Заключительным этапом данной операции могло бы стать обвинение России в сознательном подрыве национальной безопасности Соединённых Штатов и в государственном терроризме. Расчет был на то, что российская сторона никогда не признает существование такой методички и будет все яростно отрицать, постепенно втягиваясь в ловушку, подготовленную для нее американской разведкой.

Однако этим планам американских разведчиков не суждено было сбыться: неожиданно для них и для самой С. Райс российские патриоты нашли ту самую «русскую методичку», которую видела Райс в свою бытность помощника президента Обамы и на которую она ссылалась в своем интервью телекомпании CNN. Этой «методичкой» оказалась монография «Color Revolutions: Techniques in Breaking Down Modern Political Regimes» (Цветные революции: техники взлома современных политических режимов), изданная А. Манойло и О. Карповичем в 2015 г. в США (рис. 7)[13]. Именно её С. Райс и видела, похоже, в Библиотеке Конгресса США (в каталоге библиотеки есть соответствующая отметка) в то самое время, когда она была помощником президента по национальной безопасности. В результате у организаторов оперативной игры произошел «разрыв программы»: они рассчитывали на совершенно иную линию поведения российской стороны. После того, как 7 июня 2020 года факт «обнаружения» «российской методички» был озвучен в открытом эфире телеканала «Звезда», операция американских спецслужб была «поставлена на паузу»; история с обвинениями России в организации цветной революции в США дальнейшего продолжения не получила.

Перечень конкретных фактов применения различных операций ИВ и мер противодействия операциям ИВ (контроопераций) можно было бы продолжить. Можно вспомнить историю с отравлением Навального, являющуюся точной копией «Дела об отравлении Скрипалей». Среди других операций специальных служб США и их союзников также можно выделить операции ИВ гибридного типа, такие, как:

— «антинаркотеррористическая операция» США против Венесуэлы, начатая 26 марта 2020 г., дополняющая сценарий информационной операции (в ходе которой за головы Мадуро и 14 его ближайших соратников объявляется награда в 10—15 млн. долл.) угрозой применения силы: угрозой морской блокады, угрозой похищения и ареста и, наконец, угрозой военного вторжения по сценарию вторжения в Панаму в 1989 году;
— операция ЦРУ по захвату (при содействии КГБ Белоруссии) 32 российских граждан, следовавших транзитом в одну из стран Ближнего Востока (в которых США подозревали сотрудников ЧВК Вагнера), и попытка переправить их на Украину для развертывания на базе этой оперативной комбинации массированной информационной кампании с перспективой реализацией стратегий «загонной охоты» и прямого шантажа.

Тем не менее для целей настоящей статьи приведенных фактов предостаточно.

На основе результатов проведенного анализа вышеизложенных контроопераций ИВ, рассматривае-

13 В аннотации к данному изданию сказано: «The monograph is devoted to the analysis of the problems associated with the dismantling of the political regimes in modern states (both authoritarian and democratic type) and with the role of technology in the process of color revolutions».

мых как активные меры противодействия угрозам, и ретроспективных фактов для условий разнородных неопределенностей сделаны следующие выводы применительно к последующему математическому моделированию:

— основные меры противодействия операциям ИВ формально могут быть описаны в терминах случайных величин, характеризующих замедление развития во времени возможных угроз (вплоть до отмены операции ИВ в ее изначальном виде) и тем самым воспрепятствование достижению цели дискредитации репутации государства, его руководства и иных представителей власти;
— меры противодействия операциям ИВ, а также диагностика наличия угроз в информационном пространстве могут быть привязаны к оси времени и конкретным реализуемым угрозам. С формальной точки зрения успешные меры противодействия операциям ИВ, в т.ч. в упреждающем режиме, ведут к снижению частоты возникновения конкретных угроз (т.к. необходимо время на проработку новых, еще не вскрытых идей в ведении ИВ – например, снижение с 6 до 4-х операций в год) и растягиванию среднего времени развития этих угроз до появления целевого негативного эффекта (т.к. новые неапробированные идеи для ведения ИВ при их реализации сами наталкиваются на собственные недоработки и противодействия – например, с 3-х до 7 месяцев и более), а также в случае состоявшихся актов информационного воздействия — к более адекватному пониманию того времени, которое потребуется для восстановления на приемлемом уровне репутации государства, его руководства и иных представителей власти (которая в глазах международного сообщества может быть временно ухудшена после актов информационного воздействия – например, восстановление репутации за 1 месяц в сравнении с 6 месяцами для пассивных мер противодействия угрозам).

Отдельные операции ИВ и контроперации могут оказаться составными элементами в проведении стратегических операций, анализ характера которых проведен ниже.

4. Анализ характера стратегических операций

В отличие от оперативных игр, стратегические операции в ИВ, как правило, имеют и генеральный план, и четко обозначенные цели на ближнесрочную, среднесрочную и долгосрочную перспективы. Главным критерием их эффективности является гарантированное достижение стратегически значимого результата, причем не вообще (как в оперативных играх), а именно того, ради которого эта операция разработана. Классическим примером операций такого типа является так называемое «Дело об отравлении Скрипалей» (начавшаяся в 2018 году, см. рис. 8).

Операция американских и британских спецслужб в Солсбери (Великобритания), более известная как «Дело об отравлении Сергея и Юлии Скрипалей», на сегодняшний день остается самой успешной стратегической операцией, проведенной противником. В основе всех ее каскадных реакций лежит один единственный резонансный инцидент: попытка отравления бывшего агента МИ-6 Сергея Скрипаля (являвшегося, одновременно, бывшим офицером ГРУ) и его дочери Юлии. Как бы мы не относиться с нравственной стороны дела к этой операции, приходится признать, что первые два этапа этой операции (весна и осень 2018 года) были выполнены совершенно; все цели, поставленные организаторами этой операции, были достигнуты; все ловушки сработали; все «приманки» и «крючки» были «проглочены» противником, которые большую часть работы сделал за британских разведчиков, даже не подозревая об этом. Наконец, в скандальное дело был вовлечен президент РФ, фактически лично поручившийся за Петрова и Боширова (на Восточном экономическом форуме), что стало для МИ-6 полной неожиданностью. Подробный разбор схемы и хода данной операции представлен в [8].

При рассмотрении данной операции может сложиться впечатление, что сама операция началась и полностью завершилась в 2018 году; при этом сами Скрипали исчезли (по некоторым сведениям, в 2020 году их переправили в Новую Зеландию). Однако это впечатление обманчиво: операция ЦРУ и МИ-6 не прекращалась ни на минуту. Только в одном 2019 г. в рамках этой операции британской и американской разведками (в тесном содружестве с Der Spiegel) было отработано пять эпизодов:

— восьмого февраля 2019 г. британские таблоиды Daily Mail и Daily Telegraph одновременно сообщили, что в Лондон Петров и Боширов прилетали не одни; тем же рейсом с ними прилетел третий член «солсберецкой группировки» — Федотов (он же, по данным британских журналистов, Сергеев), кадровый сотрудник ГРУ и, возможно, начальник Петрова и Боширова.

Рис. 8. «Дело Скрипалей» (2018-н.вр.) как классический пример стратегической операции. © А.В. Манойло

После «осечки» с устранением Скрипалей, Федотов остался в Солсбери – наблюдать за тем, как будут развиваться события (хотя должен был улететь тем же рейсом Аэрофлота, что и его подчиненные). При этом свидетельства источников Daily Mail и Daily Telegraph о дальнейшей судьбе Федотова (Сергеева) в финальной части статей расходятся: Daily Mail, опираясь на источники в британской криминальной полиции, утверждает, что Федотов, убедившись, что Скрипали выжили и их теперь не достать, покинул Великобританию; Daily Telegraph, опираясь на показания источников из национальной разведки (МИ-6), напротив, отметила, что у разведки Великобритании нет достоверных доказательств того, что Федотов вообще покидал территорию Соединенного Королевства. Тем самым два печатных издания создали «вилку», опубликовав две почти идентичные версии, диаметрально расходящиеся на финальной стадии, и, тем самым, дали понять, что Федотов, возможно, и есть тот самый «крот» в руководстве ГРУ (ставший перебежчиком), от которого МИ-6 и получила упреждающую информацию о готовящемся визите Петрова и Боширова в Солсбери (для проведения задушевной беседы)[14];

— восьмого ноября 2019 г. The New York Times, ссылаясь на источники в спецслужбах четырех различных западных стран, публикует информацию о существовании в структуре российской военной разведки (которую они по привычке продолжают называть ГРУ) сверхсекретной воинской части №29155, специализирующейся на организации государственных переворотов и «внесудебных ликвидациях»; в статье указывается, что это та самая воинская часть, в которой служат Петров и Боширов; раскрывается имя генерала ГРУ, руководящего данной частью[15]. Им оказывается генерал-майор Аверьянов, в отношении которого «информационный партнер» МИ-6 Der Spiegel публикует полные установочные данные, полученные, предположительно, кадровыми разведчиками ЦРУ/МИ-6 и их агентурой в ходе оперативной установки личности «подозреваемого»; попутно выдвигается версия о том, что в Европе действует целая сеть «ликвидаторов», управляемых из единого центра и функционирующая по такому же принципу, что и террористические сети ИГИЛ и Аль-Кайды, запрещенных в РФ)[16];

14 См.: Britain will take ‘every possible step’ to extradite Novichok trio from Russia, warns Priti Patel after Scotland Yard named third GRU spy wanted over Salisbury attack on double-agent Sergei Skripal and daughter Yulia. // Daily Mail. 2019, Feb 8. URL: https://www.dailymail.co.uk/news/article-10012043/THIRD-Russian-spy-wanted-Salisbury-poisoning.html (Дата обращения: 10 февраля 2021)

15 См.: Schwirtz, Michael. Top Secret Russian Unit Seeks to Destabilize Europe, Security Officials Say. [Электронный документ] // New York Times. 2019, 8 oct. URL: https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html (Дата обращения: 15 ноября 2020)

16 См.: Рассекречено подразделение, которое отвечает за дестабилизацию Европы. // Экспресс-Газета. 2019, 18 ноя. URL: https://www.eg.ru/politics/806825-rassekrecheno-podrazdelenie-kotoroe-otvechaet-za-destabilizaciyu-evropy-079957/

— 23 ноября 2019 г. сразу два издания Der Spiegel и The Insider – публикуют личные (установочные) данные восьми сотрудников той самой «сверхсекретной» воинской части ГРУ №29155, о которой немецкая газета писала 8 ноября; личные данные на каждого подобраны в виде развернутой анкеты и напоминают результаты оперативной установки, осуществленной британской и американской разведками (на журналистское расследование это вообще не похоже) и легализованные через их агентуру в окружении главреда Der Spiegel (а, может быть, благодаря прямой договоренности с немецкой разведкой, сделавшей нужный звонок в редакцию немецкого издания)[17]; при этом Der Spiegel и The Insider прозрачно намекают, что располагают подробной установочной информацией на всех (или почти всех) военнослужащих указанной воинской части, а публикация всего лишь восьми анкет связана исключительно с тем, что «газета не резиновая» и большее число разоблачений просто бы не поместилось на газетной странице; тем самым британская (и, возможно, американская) разведка наглядно продемонстрировала, что она может персонально установить личность каждого сотрудника секретного подразделения ГРУ №29155, вплоть до последнего клерка;
— 24 августа 2019 г. в Берлине неизвестным был убит Зелимхан Хангошвили, бывший чеченский боевик, воевавший против федеральных войск и участвовавший в организации терактов; западные издания Bellingcat, The Insider, Dossier Center и Der Spiegel, заявляют, что убийство – политическое и организовано российской военной разведкой[18]. Немецкая криминальная полиция и контрразведка первоначально занимают осторожную позицию, но к концу ноября 2019 года (почти синхронно с сенсационным «разоблачением» в/ч №29155 журналистами-расследователями Der Spiegel) их тон меняется на обвинительный и, в результате разразившегося дипломатического скандала, 4 декабря 2019 г. два российских дипломата признаются персонами нон-грата и вынуждены покинуть страну[19];
— 5 декабря 2019 г. французская газета Le Monde публикует статью о том, что на территории Франции, во французских Альпах, обнаружена «секретная база диверсантов ГРУ»[20]; отмечается, что эта база служила местом сбора и отдыха для диверсионных групп, забрасываемых в различные точки Европы; что на этой базе «восстанавливали силы» (после удачно проведенных операций) Петров, Боширов и многие из тех восьми сотрудников в/ч №29155, личные данные которых опубликовали расследователи Der Spiegel. Завершается статья французских журналистов выводом о том, что в Европе у «террористов» ГРУ, похоже, есть опорные базы и лагеря, и база в Альпах, скорее всего, не единственная.

Все пять эпизодов готовились самостоятельно, внешне – независимо друг от друга; так, чтобы создавалось впечатление того, что журналисты-расследователи из разных изданий практически одновременно вышли на след диверсантов из ГРУ и отработали этот «след» на отлично, документально подтвердив предположения, которые западные разведки очень осторожно высказывали в 2018 и начале 2019 г. После того, как все пять эпизодов были отработаны в СМИ, стало ясно, что эти сюжеты имеют много точек пересечения, и остается только сделать последний шаг – связать их все вместе в одну историю, в которой ГРУ потребуют признать террористической организацией, такой же, как ИГИЛ[21].

Такой «точкой сборки» в самом конце июня 2020 года должна была стать «сенсационная новость», опубликованная The New York Nimes: 26 июня её обозреватели, опираясь на сведения собственных источ-

17 См.: Bulgarien — Geheimdienstanschlag in Sofia: GRU-Killerteam aus Russland. [Электронный документ] // Der Spiegel. 2019, 23 ноября. URL: https://www.spiegel.de/politik/ausland/bulgarien-geheimdienstanschlag-in-sofia-gru-killerteam-aus-russland-a-1297753.html (Дата обращения 4 января 2020 г.)

18 См.: Russischer Geheimdienst womöglich in Mord an Exil-Georgier verwickelt. [Электронный документ] // Der Spiegel. 2019, 30 авг. URL: https://www.spiegel.de/politik/ausland/berlin-mord-in-moabit-hinweis-auf-russischen-geheimdienst-a-1284400.html (Дата обращения 4 января 2020 г.)

19 См.: Германия высылает двух сотрудников посольства РФ из-за убийства в Берлине. [Электронный документ] //DW. 2019, 4 дек. URL:

https://www.dw.com/ru/germanija-vysylaet-dvuh-diplomatov-rf-iz-za-ubijstva-v-parke-tirgarten/a-60133996 (Дата обращения 4 января 2020 г.)

20 См.: La Haute-Savoie, camp de base d'espions russes spécialisés dans les assassinats ciblés. [Электронный документ] // Le Mond. 2019, 5 дек. URL: https://www.lemonde.fr/international/article/2019/12/04/la-haute-savoie-camp-de-base-d-espions-russes_6021648_3210.html; Russian spies used French Alps as 'base camp' for hits on Britain and other countries. [Электронный документ] // The Telegraph. 2019, 5 дек. URL: https://www.telegraph.co.uk/news/2019/12/05/russian-spies-used-french-alps-base-camp-hits-britain-countries/ (Дата обращения 04 января 2020 г.)

21 Запрещена в РФ.

ников из разведки США, сообщили, что российская военная разведка платила талибам и их пособникам (в Афганистане) за убийства американских солдат. В статье «Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says» («[Американская] разведка сообщает, что Россия тайно платила афганским боевикам за убийства американских солдат [в Афганистане]») утверждалось, что ради убийства американских солдат в контакт с талибами вступили военнослужащие той самой воинской части 29155, в которой проходят службу Петров и Боширов; те, в свою очередь, исправно уничтожали американских военнослужащих «за деньги, передаваемые им агентами ГРУ»[22]. В качестве мотива совершения преступления было названо желание отомстить американцам за преследование сотрудников ГРУ за инцидент в Солсбери[23].

Трудно сказать, почему этот план, весьма реальный и очень хорошо просчитанный, так и не был реализован: в самый последний момент его «поставили на паузу», решив, что еще не время. Возможно, на реализацию этого плана повлияла набиравшая обороты президентская избирательная кампания, переключившая внимание Трампа на борьбу с внутренними противниками и не оставившая ему времени для интриг против России. Не случайно источники NYT из разведсообщества США отмечали, что информация об операциях ГРУ в Афганистане была получена еще в начале февраля 2020 года, но, однако, все это время она оставалась «без движения», поскольку президент США Дональд Трамп «не знал, что с ней делать»[24].

На основе результатов проведенного анализа характера стратегических операций для условий разнородных неопределенностей сделаны следующие выводы применительно к последующему математическому моделированию:

— стратегические операции в ИВ формально могут быть формализованы в виде сложной структуры с привязкой к генеральному плану и обозначением целей на ближнесрочную, среднесрочную и долгосрочную перспективы во времени. Каждый из составных формализованных элементов этой структуры (реально разнесенных в пространстве и времени) связан с другими элементами логическими условиями и реализует конкретный фрагмент стратегии и набор операций ИВ для достижения интегральной цели дискредитации репутации государства, его руководства и иных представителей власти. Математически выполнение плана стратегической операции может быть описано в терминах случайных событий, характеризующих развитие во времени возможных угроз для элементов этой структуры, связь элементов характеризуется логическими условиями «И», «ИЛИ» для достижения целей в ИВ;
— по каждому составному элементу меры противодействия операциям ИВ, а также диагностика наличия угроз в информационном пространстве могут быть привязаны к оси времени и конкретным реализуемым угрозам. С формальной точки зрения успешность мер противодействия операциям ИВ полностью аналогична успешности, определенной выше.

С точки зрения влияния на репутацию государства, его руководства и иных представителей власти все вышеизложенное характеризуется множеством факторов, доступное воздействие на которые позволит управлять возникающими частными и интегральным рисками (для каждого из факторов учитываются принципиальная возможность, целесообразность и осуществимость воздействия на них). Каковы пределы достигаемой эффективности от управления рисками? – На этот вопрос возможно ответить только в результате математического моделирования операций и контроопераций в условиях реализации разнородных угроз при ведении ИВ.

5. Общие положения предлагаемого подхода к математическому моделированию

За основу предлагаемого подхода к математическому моделированию принят подход, изложенный в разные годы в приложении к различным системам [10-15] и доведенный до реализации на уровне ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы», ГОСТ Р 59991 «Системная инженерия. Системный анализ процесса управления рисками для

22 Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says. By Charlie Savage, Eric Schmitt and Michael Schwirtz. [Электронный документ] // The New York Times. 2020. June 26. URL: https://www.nytimes.com/2020/06/26/us/politics/russia-afghanistan-bounties.html

23 Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says. By Charlie Savage, Eric Schmitt and Michael Schwirtz. [Электронный документ] // The New York Times. 2020. June 26. URL: https://www.nytimes.com/2020/06/26/us/politics/russia-afghanistan-bounties.html

24 «The Trump administration has been deliberating for months about what to do about a stunning intelligence assessment». См.: Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says. By Charlie Savage, Eric Schmitt and Michael Schwirtz. [Электронный документ] // The New York Times. 2020. June 26. URL: https://www.nytimes.com/2020/06/26/us/politics/russia-afghanistan-bounties.html

системы». Развитие операций и контроопераций ИВ формализовано с использованием понятия моделируемой системы. Получаемые результаты математического моделирования операций и контроопераций ИВ для моделируемой системы используются в интерпретации к исходной системе, в интересах которой проводятся соответствующие расчеты. В качестве исходной системы выступает оцениваемая реальная репутация государства, его руководства и иных представителей власти в условиях ИВ.

Под моделируемой системой понимается система, для которой решение задач системного анализа осуществляется с использованием ее формализованной модели и, при необходимости, формализованных моделей учитываемых сущностей, объединенных целевым назначением в задаваемых условиях (по ГОСТ Р 59341). В свою очередь под целостностью моделируемой системы понимается такое ее состояние, которое отвечает целевому назначению модели системы.

В качестве моделируемой системы, используемой для вероятностного прогноза расчетных показателей рисков на задаваемый период времени, выступает моделируемая система в элементарном состоянии «целостность моделируемой системы обеспечена». Элементарные состояния, формально определенные как «целостность моделируемой системы обеспечена» и «целостность моделируемой системы нарушена», при проведении исследований должны быть конкретизированы с учетом специфики реальной системы, целей и требований к сохранению ее функциональности и эффективности. Например, если в качестве моделируемой системы выступает репутация государства, под состоянием «целостность моделируемой системы нарушена» может пониматься достижение целей противником при проведении тех или иных операций ИВ, направленных против руководства страны, против которого направлены информационные операции, под состоянием «целостность моделируемой системы нарушена» может пониматься неспособность руководства этой страны принимать адекватные решения и осуществлять их эффективную реализацию (по мнению общественности, на которую нацелены операции ИВ, например, по мнению электората).

Соответственно на определенном выше пространстве элементарных событий предлагаемая (в части 2 статьи) модель позволяет рассчитать показатели вероятности обеспечения целостности и вероятности нарушения целостности моделируемой системы в течение задаваемого периода прогноза. С учетом последствий последний показатель может быть интерпретирован как риск нарушения целостности моделируемой системы в течение задаваемого периода прогноза.

Моделируемая система простой структуры представляет собой систему из единственного элемента или множества элементов, логически объединенных для системного анализа как один элемент. Анализ моделируемой системы простой структуры осуществляют по принципу «черного ящика», когда известны входы и выходы, но неизвестны внутренние детали функционирования системы.

В качестве исходных данных для моделирования «черного ящика» выступают:

- частота возникновения источников угроз;
- среднее время развития возникшей угрозы до ее реализации в виде нарушения целостности моделируемой системы;
- время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;
- длительность диагностики моделируемой системы;
- среднее время восстановления нарушенной целостности моделируемой системы;
- длительность периода прогноза.

Моделируемая система сложной структуры представляется как совокупность взаимодействующих элементов, каждый из которых представляется в виде «черного ящика», функционирующего в условиях неопределенности. Причем элементы связаны логическими условиями «И», «ИЛИ» для достижения целей моделируемой системы.

Выводы

1. Для математического моделирования различных способов ведения ИВ проведен анализ основных стратегий операций «удушения», «загонной охоты», прямого шантажа. В интересах аналитических исследований рассмотрены такие меры противодействия информационным операциям (меры контроопераций), как перехват информационной повестки и оперативной инициативы, отвлечение на негодный объект, информационные прививки и контроперации возвратного типа. Проведен анализ характера стратегических операций в современной ИВ. Сформулированы общие положения и определены исходные данные для математического моделирования.

2. На основе результатов анализа сделаны следующие обобщенные выводы применительно к последующему математическому моделированию (в следующей публикации 2-й части статьи):

— основные стратегии ИВ формально могут быть описаны в терминах случайных событий, характеризующих возникновение и развитие во времени возможных угроз реализации операций и контроопераций в ИВ;
— для случаев применения активных и пассивных мер противодействия угрозам. возникновение и развитие угроз может быть привязано к оси времени и охарактеризовано:
— возможной частотой возникновения конкретных угроз (несколько операций в год, по ретроспективным данным — в среднем около 4-6 операций в год);
— средним временем развития этих угроз до появления целевого негативного эффекта от реализации этих угроз (несколько месяцев, по ретроспективным данным — в среднем около 3–7 месяцев);
— средним временем условно приемлемого восстановления репутации (по ретроспективным данным — в среднем от одного месяца до полугода);
— стратегические операции в ИВ формально могут быть формализованы в виде сложной структуры с привязкой к генеральному плану и обозначением целей на ближнесрочную, среднесрочную и долгосрочную перспективы во времени. Каждый из составных формализованных элементов этой структуры (реально разнесенных в пространстве и времени) связан с другими элементами логическими условиями и реализует конкретный фрагмент стратегии и набор операций ИВ для достижения интегральной цели дискредитации репутации государства, его руководства и иных представителей власти. Математически выполнение плана стратегической операции может быть описано в терминах случайных событий, характеризующих развитие во времени возможных угроз для элементов этой структуры, связь элементов характеризуется логическими условиями «И», «ИЛИ» для достижения целей в ИВ.

(Продолжение следует)

Литература

1. Манойло А.В. Фейковые новости как угроза национальной безопасности и инструмент информационного управления // Вестник Московского университета. Серия 12: Политические науки. — 2019. — № 2. — С. 41–42.
2. Трубецкой А. Ю. Психология репутации. — М.: Наука, 2005. — 291 с.
3. Устинова Н. В. Политическая репутация: сущность, особенности, технологии формирования: дис. канд. полит. наук. — Екатеринбург: УГУ, 2005. — 166 с.
4. Шишканова А. Ю. Репутация политического лидера: особенности и технологии формирования // Огарёв-Online. 2016. №7(72). С. 2.
5. Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. 4-е изд., перераб. и доп. — Горячая линия-Телеком Москва, 2020. — 636 с.
6. Манойло А.В. Современная практика информационных войн и психологических операций. Вирусные технологии и «эпидемии» каскадного типа на примере операции по разоблачению агента влияния ЦРУ, бывшего вице-президента Венесуэлы Диосдадо Кабельо 17-21/08/2019. // Национална сигурност (Nacionalna sigurnost). 2019. Выпуск №3. С. 3–8.URL: https://nacionalna-sigurnost.bg/broi-3/
7. Манойло А.В. Дело Скрипалей как операция информационной войны // Вестник Московского государственного областного университета. — 2019. — № 1.
8. Манойло А.В. Цепные реакции каскадного типа в современных технологиях вирусного распространения фейковых новостей // Вестник Московского государственного областного университета (Электронный журнал). — 2020. — № 3.
9. Климов С. М. Модели анализа и оценки угроз информационно-психологических воздействий с элементами искусственного интеллекта. / Сборник докладов и выступлений научно-деловой программы Международного военно-технического форума «Армия-2018». 2018. С. 273-277.
10. Костогрызов А. И. Прогнозирование рисков по данным мониторинга для систем искусственного интеллекта / БИТ. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н. Э. Баумана, 2019, с. 220–229.
11. Kostogryzov A., Nistratov A., Nistratov G. (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352-364. https://www.springer.com/gp/book/9783030468941
12. Kostogryzov A, Nistratov A. Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In “Safety and Reliability of Systems and Processes”, Gdynia Maritime University, 2020. pp. 153-174. DOI: 10.26408/srsp-2020
13. Костогрызов А. И. Подход к вероятностному прогнозированию защищенности репутации политических деятелей от «фейковых» угроз в публичном информационном пространстве // Вопросы кибербезопасности. 2023, №3. С. 114–133. DOI:1021681/2311-3456-2023-3-114-133
14. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments (Вероятностное упреждающее моделирование для оценок рисков в сложных системах). Time Series Analysis — New Insights. IntechOpen, 2023, pp. 73-105. http://mts.intechopen.com/articles/show/title/probabilistic-predictive-modelling-for-complex-system-risk-assessments
15. Костогрызов А. И., Нистратов А.А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом // Вопросы кибербезопасности. 2023, №5. DOI:1021681/2311-3456-2023-5-9-24, с. 9–24.

ON PROBABILISTIC FORECASTING OF RISKS IN INFORMATION WARFARE. PART 1. ANALYSIS OF OPERATIONS AND COUNTEROPERATIONS STRATEGIES FOR MATHEMATICAL MODELING

Manoilo A.V.[25], Kostogryzov A.I.[26]

The purpose of the 1st *part of the work: on the basis of the analysis of the main strategies of operations and counteroperations in information warfare (IW), to form general provisions of the approach to mathematical modeling in order to propose a model and methods for probabilistic forecasting of particular and integral risks in the 2nd and final part, and with their help to conduct a systematic analysis of the identified opportunities for risk management in IW.*

Result of research: *based on the results of the analysis of strategies of operations and counteroperations (in the 1st part of the article), a model and methods for probabilistic forecasting of particular and integral risks in IW are proposed. Based on their application, examples have been developed to illustrate the efficiency of the proposed approach. For some retrospective data, a systematic analysis of the identified opportunities for risk management in IW was carried out (in the 2nd final part) articles).*

Scientific novelty: *today the impact of heterogeneous threats in the conduct of IW in the international public media space is expressed in purposeful compromising fabrications of a resonant nature (false facts, false intentions) that contribute to the discrediting and discrediting of the reputation of the state, its leadership and other representatives of the authorities. This front side of IoT is visible to all consumers of information, but without an adequate differentiation between "true" and "false". The study of this on the front side, political science studies are devoted. In contrast to these studies, this paper proposes a mathematical basis for a system analysis of the development of information operations and possible ways to counteract them depending on specific initial data, formed on the basis of facts or estimated hypothetically. The paper examines the possibilities for popular methods of countering operations in IoT with the indication of achievable quantitative estimates for risk management.*

Keywords: *probability, reputation, model, forecasting, risk, system analysis, threat.*

References

1. Manojlo A.V. Fejkovye novosti kak ugroza nacional'noj bezopasnosti i instrument informacionnogo upravlenija // Vestnik Moskovskogo universiteta. Serija 12: Politicheskie nauki. — 2019. — № 2. — S. 41–42.
2. Trubeckoj A. Ju. Psihologija reputacii. — M.: Nauka, 2005. — 291 s.
3. Ustinova N. V. Politicheskaja reputacija: sushhnost', osobennosti, tehnologii formirovanija: dis. kand. polit. nauk. — Ekaterinburg: UGU, 2005. — 166 s.
4. Shishkanova A. Ju. Reputacija politicheskogo lidera: osobennosti i tehnologii formirovanija // Ogarjov-Online. 2016. №7(72). S. 2.
5. Manojlo A. V., Petrenko A. I., Frolov D. B. Gosudarstvennaja informacionnaja politika v uslovijah informacionno-psihologicheskoj vojny. 4-e izd., pererab. i dop. — Gorjachaja linija-Telekom Moskva, 2020. — 636 s.
6. Manojlo A.V. Sovremennaja praktika informacionnyh vojn i psihologicheskih operacij. Virusnye tehnologii i «jepidemii» kaskadnogo tipa na primere operacii po razoblacheniju agenta vlijanija CRU, byvshego vice-prezidenta Venesujely Diosdado Kabel'o 17-21/08/2019. // Nacionalna sigurnost (Nacionalna sigurnost). 2019. Vypusk №3. S. 3-8. URL: https://nacionalna-sigurnost.bg/broi-3/
7. Manojlo A.V. Delo Skripalej kak operacija informacionnoj vojny // Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. — 2019. — № 1.

25 Andrey V. Manoilo, Dr.Sc. (Political Science), Ph.D. (Physics & Mathematics), Professor of Lomonosov Moscow State University, Professor of the Faculty of Political Science of Lomonosov Moscow State University. Moscow, Russia. E-mail: Cyberhurricane@yandex.ru

26 Andrey I. Kostogryzov, Dr.Sc. (Technology), Professor, Federal Research Center "Informatics and Control" of the Russian Academy of Sciences. Moscow, Russia. E-mail: Akostogr@gmail.com

8. Manojlo A.V. Cepnye reakcii kaskadnogo tipa v sovremennyh tehnologijah virusnogo rasprostranenija fejkovyh novostej // Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta (Jelektronnyj zhurnal). — 2020. — № 3.
9. Klimov S. M. Modeli analiza i ocenki ugroz informacionno-psihologicheskih vozdejstvij s jelementami iskusstvennogo intellekta. / Sbornik dokladov i vystuplenij nauchno-delovoj programmy Mezhdunarodnogo voenno-tehnicheskogo foruma «Armija-2018». 2018. S. 273-277.
10. Kostogryzov A. I. Prognozirovanie riskov po dannym monitoringa dlja sistem iskusstvennogo intellekta / BIT. Sbornik trudov Desjatoj mezhdunarodnoj nauchno-tehnicheskoj konferencii – M.: MGTU im. N.Je. Baumana, 2019, ss. 220-229
11. Kostogryzov A., Nistratov A., Nistratov G. (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352-364. https://www.springer.com/gp/book/9783030468941
12. Kostogryzov A, Nistratov A. Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In “Safety and Reliability of Systems and Processes”, Gdynia Maritime University, 2020. pp. 153-174. DOI: 10.26408/srsp-2020
13. Kostogryzov A.I. Podhod k verojatnostnomu prognozirovaniju zashhishhennosti reputacii politicheskih dejatelej ot «fejkovyh» ugroz v publichnom informacionnom prostranstve // Voprosy kiberbezopasnosti. 2023, №3. S. 114–133. DOI:1021681/2311-3456-2023-3-114-133
14. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments (Verojatnostnoe uprezhdajushhee modelirovanie dlja ocenok riskov v slozhnyh sistemah). Time Series Analysis — New Insights. IntechOpen, 2023, pp. 73-105. http://mts.intechopen.com/articles/show/title/probabilistic-predictive-modelling-for-complex-system-risk-assessments
15. Kostogryzov A.I.. Nistratov A.A. Analiz ugroz zloumyshlennoj modifikacii modeli mashinnogo obuchenija dlja sistem s iskusstvennym intellektom // Voprosy kiberbezopasnosti. 2023, №5. DOI:1021681/2311-3456-2023-5-9-24, s. 9–24.

ПРИМЕНЕНИЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ЧАСТЬ 3)

Калашников А.О.[1], Бугайский К.А.[2], Аникина Е.В.[3], Перескоков И.С.[4], Петров Андрей О.[5], Петров Александр О.[6], Храмченкова Е.С.[7], Молотов А.А.[8]

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, теории категорий, 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. Показано, что состояние отношений агента может быть получено на основе соответствующих оценок состояний на уровне информационных ресурсов и информационных потоков из состава агента. Разработана схема признаков для представления событий с точки зрения информационной безопасности и предложен способ единообразного представления событий и сообщений поступающих из разных источников . Доказано, что состояние отношения на уровне информационного ресурса или информационного потока определяется как результат соотнесения текущего и эталонного наборов событий. Доказано, что события и их наборы могут быть представлены как многоместные отношения признаков. Доказано, что каждое отношение признаков для события может быть поименовано первым элементом схемы признаков. Разработана матрица свертки признаков, содержащая только разрешенные сочетания параметров признаков для наборов событий, описывающих состояние отношений. Доказано, что применение матрицы свертки дает линейную зависимость от размерности наборов событий. Даны формальные определения базовых действий Защитника и Нарушителя на агенте. Обоснована необходимость внесения изменений в состав и способы регистрации событий информационной безопасности информационных ресурсов и информационных потоков.*

Научная новизна: *рассмотрение вопросов защиты информации с использованием аппарата математических и логических отношений, а также теории категорий. Разработка матрицы свертки событий на основе категорного подхода для определения состояния отношений агента. Доказательство линейной зависимости операций сравнения текущего и эталонного наборов событий при использовании матрицы свертки событий. Разработка формальных определений базовых операций агента для Защитника и Нарушителя. Сформулированы две гипотезы, описывающие возможности агента в области защиты информации.*

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. разработали модель многоместных отношений при описании наборов событий, разработали доказательство утверждения 4, а также сформулировали гипотезы и определения базовых операций агентов. Перескоков И.С и Петров Андрей О. разработали доказательство утверждения 1. Петров Александр О. и Храмченкова Е.С. разработали доказательство утверждения 3, Молотов А.А. разработал доказательство утверждения 2.*

1 Калашников Андрей Олегович, доктор технических наук, главный научный сотрудник лаборатории «Сложных сетей» ФГБУН Институт проблем управления им. В.А. Трапезникова РАН. г. Москва, Россия. E-mail: aokalash@ipu.ru

2 Бугайский Константин Алексеевич, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН. E-mail: kabuga@ipu.ru

3 Аникина Евгения Владимировна, научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН. e-mail: ajanet@ipu.ru

4 Перескоков Илья Сергеевич, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН. E-mail: pereskokov@phystech.edu

5 Петров Андрей Олегович, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН. E-mail: petrovaojob@gmail.com

6 Петров Александр Олегович, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН, E-mail: petrovalexandr@ipu.ru

7 Храмченкова Екатерина Сергеевна, младший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН. E-mail: hramchenkovaes@yandex.ru

8 Молотов Александр Анатольевич, инженер-программист, Институт проблем управления им. В.А. Трапезникова РАН. E-mail: alpha.sphere@ya.ru

Ключевые слова: *модель информационной безопасности, оценка сложных систем, логико-вероятностный метод, теория категорий, системный анализ, многоагентная система.*

DOI: 10.21681/2311-3456-2023-6-20-34

Введение

Данная статья является третьей из серии публикаций, посвященных исследованию вопроса применения логико-вероятностного метода при изучении вопросов защиты информации. Метод был разработан Рябининым И.А. [1, см. литературу там же]. Метод получил высокую популярность при проведении исследований, связанных с анализом и оценкой сложных систем. Прежде всего для решения вопросов надежности работы систем и 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 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 объектов. Логико-вероятностный метод также находит свое применение 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 задач в области информационной безопасности (далее – ИБ).

Постановка задачи

Современные информационные системы (далее – ИС) [12, 13] отличаются большим разнообразием обрабатываемой информации, сложными типами связей между аппаратными и программными компонентами, распределенным характером обработки и управления информацией и компонентами ИС. Что с большой вероятностью влечет за собой проблему экспоненциального взрыва при непосредственном использования для описания структурно-логических схем ИС функций алгебры логики в рамках логико-вероятностного метода.

Для обеспечения достижения общей цели исследования (адаптации логико-вероятностного метода для решения задач ИБ) в настоящей статье разработаны формально-логические основы для предотвращения экспоненциального взрыва. Для решения этой задачи выделяется системный уровень ИС, состоящий из функций расчета состояния отношений агентов информационной безопасности.

Формализация исходных данных

Обозначим множество агентов в составе ИС как *AG*, отдельного агента как $\beta \in AG$, а множество агентов, взаимодействующих с данным и обозначаемых далее как респондентов – как *AV*, то есть имеем $AV \subset AG, \gamma \in AV, \beta \in AG, \beta \neq \gamma$.

Положения и выводы изложенные в [14, 15] показывают, что выбор тех или иных действий по защите информации для конкретного агента зависит от определения намерений каждого из респондентов, которые предложено оценивать как состояние отношения $\beta[R]_i, i = \{1, \dots, n\}, n = |AV|$ между агентом β и респондентом γ. Состояния отношений определены как $R = \{Lr, Dr, Ir, Ur\}$ или *R*={*Лояльное, Нелояльное, Неопределенное и Безразличное*} соответственно. Таким образом, интегральное состояние агента представляет собой вектор состояний отношений данного агента со всеми его респондентами

$$Q_\beta = [\beta[R]_1, \dots, \beta[R]_n], n = |AV| \quad (1)$$

При этом определение состояния отношений агент может выполнить только на основании сбора и анализа событий и сообщений, формируемых информационными потоками (далее – ИП) и информационными ресурсами (далее – ИР) из состава данного агента.

На основании [13, 16, 17, 18] можно полагать, что данные события и сообщения генерируются программным путем (автоматически) и независимо каждым ИП и ИР как результат внешних воздействий или взаимодействия собственных ИП и ИР, но опять же вызванных внешними воздействиям. Обозначим множество ИП в составе агента как *QS*, а множество ИР – как *QR*. Для реализации выражения (1) необходимо обеспечить разделение событий и сообщений, как по функциональному признаку, так и по респондентам. Поскольку взаимодействие агентов основано на обмене сообщениями, то обозначим MS^{β} как исходящие сообщения агента, MS^{γ} – как входящие сообщения агента. Работу агента можно представить в виде схемы $MS^{\gamma} \to (QS, QR) \to MS^{\beta}$. Соответственно, формируемые в процессе работы агента события и сообщения можно разделить по типам:

— внешние воздействия (*in*), позволяющие идентифицировать респондента и его воздействие;
— события и сообщения (*out*) от ИП и ИР, являющиеся откликом агента на внешние воздействия.

Совокупность этих типов событий и сообщений, автоматически формируемых агентом в процессе его функционирования, обозначим как $ME = \{ME^{in}, ME^{out}\}$.

Сделаем следующие допущения.

D1. В каждый конкретный момент времени формирование *ME* агента вызывает один респондент.

D2. Один и тот же респондент может воздействовать на агента разными способами, то есть оказывать воздействие на различные ИП и ИР агента.

D3. Отдельное воздействие респондента вызывает формирование событий и сообщений только частью ИП и ИР агента.

D4. Отдельное воздействие респондента вызывает формирование алгоритмически обусловленного набора событий и сообщений со стороны каждого из участвующих ИП и ИР агента.

Эти допущения дают возможность установить отображение $ME^{in} \to ME^{out}$ в виде функций воздействия $\delta: MS^{\gamma} \to ME^{in}$ и отклика $\varepsilon: ME^{out} \to MS^{\beta}$.

Таким образом, общем виде агент может быть представлен как автомат

$$\beta = \langle ME, QS, QR, \delta, \varepsilon, Q_{\beta} \rangle \qquad (2)$$

Множество *ME*, а также функции δ, ε для любых *QS* или *QR* агента входящие в выражение (2) алгоритмически предопределены на этапе разработки соответствующих ИП и ИР, а также агента в целом. Отсюда следует вывод, что реакция агента на любое внешнее воздействие со стороны респондента γ представляет собой фиксированный по составу и содержанию конечный набор событий и сообщений QM_{γ}. При этом, одни и те же комбинации событий (или отдельное событие) могут входить в подмножества *QM* описывающих разных респондентов.

$$QM_{\gamma} = ME_{\gamma}^{in} \cup ME_{\gamma}^{out},\ QM_i \cap QM_j \neq \emptyset, \qquad (3)$$

$$QM_i, QM_j \in ME,\ i, j \in AV$$

Таким образом, функционирование агента с точки зрения информационной безопасности (далее – ИБ) может быть представлена целевой функцией

$$FT: \bigcup_{\gamma \in AV} QM_{\gamma} \to Q_{\beta} \qquad (4)$$

Исходя из алгоритмической предопределенности множества *ME* любое его подмножество *QM* может быть разделено на следующие функциональные подмножества:

M^{α} – события и сообщения, позволяющие идентифицировать респондента, то есть отвечающие на вопросы «кто, где, когда»;

M^{Q} – события и сообщения, позволяющие идентифицировать состояние отношения агент-респондент, то есть отвечающие на вопрос «что делает».

В итоге имеем $QM = \{M^{\alpha}, M^{Q}\}$. При этом согласно (3) действуют следующие ограничения $\sum_{\gamma \in AV} |QM_{\gamma}| > |ME|$ и $|M_i^{\alpha}| + |M_i^{Q}| > QM_i$, $i \in AV$, которые говорят о том, что все подмножества формируемые из общего множества *ME* агента являются «неопределенными». В данном случае не используется типичный для подобных ситуаций термин «нечеткое множество» поскольку для реализации (3) и (4) факт вхождения события или сообщения в то или иное подмножества должен трактоваться однозначно, но при этом подмножества не имеют четких границ, позволяющих утверждать отсутствие пересечения этих подмножеств. Соответственно, агент должен на алгоритмическом уровне реализовывать соответствующие функции отнесения отдельных событий и сообщений к тому или иному целевому подмножеству.

Функцию выделения событий и сообщений, обеспечивающих идентификацию респондента представим в виде

$$F^{\alpha}(m): \delta(MS^{\gamma}) \to (m \in M_{\gamma}^{\alpha}) \qquad (5)$$

Результатом работы функции является набор правил $BA = \{b_i, \dots, b_n\}$, $b_i = \{0,1\}$. Значение «1» для элемента будет означать отнесение отдельного события или сообщения *m* из множества MS^{γ} к набору событий и сообщений, позволяющие идентифицировать конкретного респондента.

Это дает функцию распределения событий и сообщений – откликов агента на внешние воздействия – по взаимодействующим респондентам

$$FA(m): (ME \wedge BA) \rightarrow (m \in QM_{\gamma}) \quad (6)$$

Возникающая рекурсия между выражениями (5) и (6) заслуживает отдельного исследования.

Здесь необходимо обратить внимание на следующие условия.

Y1. Принципы построения современных вычислительных средств позволяют представить каждый из ИП и ИР агента как единый набор API и алгоритмов для всех взаимодействующих респондентов.

Y2. Регистрация событий и сообщений в процессе функционирования ИП и ИР агента реализуется разработчиком, что означает уникальность допустимых наборов событий и сообщений *M* для каждого ИП и ИР, то есть $ME = \bigcup_{i \in N} M_i$, $M_i \cap M_j = \emptyset$, $i, j \in N$,

$$M = \{M^{in}, M^{out}\}, \quad M_i^{in} \in ME^{in}, \quad M_i^{out} \in ME^{out},$$

где $N = |QS| + |QR|$ – общее число ИП и ИР в составе агента.

Y3. Не все ИП и ИР агента могут принимать участие в определении состояния отношения с конкретным респондентом.

На основании условий *Y1-Y3* можно определить функцию отнесения сообщений из множества QM_{γ} к множеству QP_i, $i \in N$

$$FM(m): (QM_{\gamma} \wedge BM) \rightarrow (m \in QP_i) \quad (7),$$

где *BM* – набор правил $BM = \{b_i, \dots, b_n\}, b_i = \{0,1\}$. Значение «1» для элемента будет означать отнесение отдельного события или сообщения *m* из множества QM_{γ} к набору событий и сообщений, описывающих реакцию агента на воздействия конкретного респондента.

Выражение (7) определяет, что множество QP содержит все события и сообщения из *QM* для отдельного ИП или ИР агента, относящиеся к определенному респонденту $QP = \{M^{\alpha}, M^{Q}\}$. При этом наличие в *QP* подмножества M^{α} обеспечивает сквозную идентификацию респондента в данном отношении для всех ИП и ИР агента. Это позволяет рассматривать *QP* как паттерн (схему) описывающую реакцию агента на внешнее воздействие посредством фиксированных наборов событий и сообщений для отдельных ИП и ИР.

Выражения (4) – (7) позволяют представить отношение агент-респондент в виде декартового произведения множеств

$$\beta[R]^{*} = QP_1 \times \cdots \times QP_i \times \cdots \times QP_N \quad (8)$$

Символ * в выражении (8) означает необходимость выбора конкретного состояния отношений. То есть, каждому состоянию отношений агента $R = \{Lr, Dr, Ir, Ur\}$ должен соответствовать определенный набор событий и сообщений M^{Q} отдельного ИП или ИР. Это позволяет представить функцию выделения событий и сообщений, обеспечивающих идентификацию состояния отношений агента с отдельным респондентом на уровне отдельного ИП или ИР в виде

$$F^{Q}(m): (\mathrm{QP} \wedge BP) \rightarrow (m \in M_r^{Q}), \; r \in R \quad (9),$$

где *BP* – набор правил $BP = \{b_i, \dots, b_n\}, b_i = \{0,1\}$. Значение «1» для элемента будет означать отнесение отдельного события или сообщения *m* из множества *QP* к набору событий и сообщений, идентифицирующих конкретное состояние отношений агента на уровне ИП и ИР. Таким образом применительно к определению состояния отношения получаем $QP = \bigcup_{r \in R} M_r^{Q}$, при этом $\sum_{r \in R} \left| M_r^{Q} \right| > |QP|$.

В итоге целевая функцию агента с точки зрения категорного подхода должна содержать

$$FT = Ref\left(\psi(m) \circ F^{Q}(m)\right) \circ FM(m) \circ \circ FA(m) \circ F^{\alpha}(m) \quad (10),$$

где:

$F_k = F^{Q}(m) \circ FM(m) \circ FA(m) \circ F^{\alpha}(m)$ – целевая функция отбора событий объекта;

$\psi(*)$ – решающая функция, которая реализует отношение между набором событий и сообщений и состоянием отношений $\psi: M_r^{Q} \rightarrow R$.

Поскольку функции $\psi(m)$ и $F^{Q}(m)$ относятся к отдельным ИП и ИР агента, то необходима также функция *Ref(*),* которая обеспечивает интегральную оценку состояния отношения $\beta R\gamma$ агента с отдельным респондентом на основании исходных данных на уровне ИП или ИР.

Вопросы создания правил и реализации функций указанных в выражениях (5, 6, 7, 9), (применительно к множествам *ME*, *QM, QP)* давно и успешно исследуются [19, 20, см. литературу там же], поэтому в данной статье вопросы реализации указанных выражений рассматривать не будем.

Вместе с тем отметим, что в самом общем виде события и сообщения из состава множества ME и всех его подмножеств:

- Представляют собой алгоритмически определенные семантические структуры, причем для различных ИП и ИР состав и содержание этих структур может значительно различаться.
- В качестве своего источника имеют не только различные ИП и ИР, но и фиксируются (с предварительной обработкой) в нескольких журналах регистрации как в рамках собственно ИП или ИР, так и в рамках агента в целом.
- В процесс реализации целевой функции агента (10) подразумевают внесение изменений структуры и значений содержащейся в событии и сообщении информации.
- Предполагают наличие различных трактовок со стороны различных экспертов как по содержанию, так и по значению событий и сообщений.

Отсюда возникает необходимость в приведении событий и сообщений к единообразному с точки зрения ИБ виду или к их ортогонализации.

Будем использовать общепринятое определение признака как наличие определенных черт, характеристик или свойств дающих основание отнести событие или сообщение к тому или иному типу или классу.

Под ортогонализацией событий и сообщений агента будем понимать формирование единообразных для всех событий и сообщений агента шкал признаков, которые так или иначе содержатся в семантической структуре событий и сообщений. Формирование шкал признаков будем проводить на основе следующего правила:

L1. Признак определяет характер воздействия на носитель данных имеющий определенный уровень последствий

Компоненты этого правила соответствуют следующим морфизмам, определенным во второй части статьи, которые описывают формирование событий и сообщений в агенте.

Компоненте *Характер воздействия* соответствует морфизм $AC \to ME$, описывающий регистрацию действий выполняемых в рамках аккаунта. В соответствии с принятыми в ИБ подходами, компоненте соответствуют операции типа Запись, Чтение, вызывающие изменения Конфиденциальности, Целостности, Доступности для носителя информации. Таким образом можно сформировать шкалу из шести значений для признака *SI* (scale impact).

Компоненте *Носитель данных* соответствует морфизм $Conf \to ME$, описывающий регистрацию фактов выполнения операций с теми или иными носителями данных (включая сюда и программы представленные в виде блоков данных в памяти или на дисках). В современных вычислительных системах, построенных на принципах открытых систем, можно выделить следующие базовые носители данных: Регистры процессора, Оперативная память, Долговременная память, Сетевые адаптеры и Устройства ввода-вывода. Таким образом можно сформировать шкалу из пяти значений для признака *SC* (scale carrier).

Компоненте *Уровень последствий* соответствует морфизм $Prog \to ME$, описывающий статус и режимы выполняемых операций. Поскольку речь идет о событиях и сообщениях, формируемых в агенте как отклик на внешние воздействия, то для перечисления уровней воздействия целесообразно использовать типовые уровни журналирования: fatal, error, warning, info. Таким образом можно сформировать шкалу из четырех значений для признака *SL* (scale level).

Значения шкал признаков можно рассматривать как множества, что дает основание представить любое событие или сообщение как комбинацию значений признаков, то есть как многоместное отношение $SI \times SC \times SL$. Многоместное отношение, описывающее событие или сообщение можно представить в виде схемы признаков $\langle SI, SD, SL \rangle$, поэтому дальше будем использовать только термин «событие». Каждый элемент схемы может содержать наборы значений соответствующих шкал признаков, например, $\{a, b, c\}$, $a, b, c \in SI$ [21, см. литературу там же]. Для демонстрации в дальнейшем необходимых по ходу изложения примеров, определим признаки со следующим составом параметров $SI = \{\theta_1, \theta_2, \theta_3\}$, $SD = \{\lambda_1, \lambda_2, \lambda_3\}$, $SL = \{\mu_1, \mu_2, \mu_3\}$. Равномощность множеств носит исключительно демонстрационный характер.

Необходимо отметить, что согласно правилу *L1*, для каждой операции всегда есть носитель и уровень воздействия, то есть $SI \wedge SD \wedge SL$. Следовательно, выполнение правила *L1*, влечет необходимость выполнения еще двух правил, обеспечивающих полноту описания события и порядок перечисления значений признаков.

L2. Любое событие или сообщение должно соответствовать схеме

$$\exists m: \langle SI, SD, SL \rangle \Rightarrow \exists(\theta_i \in SI) \wedge \exists(\lambda_i \in SD) \wedge \exists(\mu_i \in SL)$$

L3. Порядок перечисления значений признаков при описании события определяется по шкале SI

$$\forall m: \langle SI, SD, SL \rangle, \theta_i \in SI, \lambda_j \in SD, \mu_n \in SL \Rightarrow$$
$$\Rightarrow n = j = i$$

Будем полагать, что шкалы признаков имеют преимущественно качественные значения. В дальнейшем значения шкал признаков будем определять как «параметры». Для соответствия признаков целевой функции (10) применяется следующее условие.

Y4. Число шкал признаков и число параметров для каждой шкалы могут быть различными, но должны быть конечными.

Экспертно формируемые признаки и параметры должны быть единообразны для всех событий объекта. Правило *L1*, и условие *Y4* подразумевают (на основании положений алгебры кортежей) возможность описания одного и того же события несколькими параметрами для каждого из признаков. Например, можно получить кортеж вида

$$m = \langle \{\theta_1, \theta_2\}\{\lambda_3\}\{\mu_1, \mu_3\} \rangle \quad (11)$$

Здесь и далее указание, что конкретные переменные в приводимых выражениях даны для примера, даваться не будет. Отметим, что выражение (11) эквивалентно следующим сочетаниям параметров: $(\theta_1\lambda_3\mu_1)$, $(\theta_1\lambda_3\mu_3)$, $(\theta_2\lambda_2\mu_1)$, $(\theta_2\lambda_3\mu_3)$. Аналогичным (11) образом может быть представлен и некоторый набор событий.

Но представляется очевидным, что подобное определение для наборов событий является недостоверным в силу неизбежного наличия в этом случае ошибочных комбинаций параметров признаков. Например, при рассмотрении кортежа (11) как набора событий, возникающее в процессе его разложения сочетание параметров для отдельного события $m_i = (\theta_2\lambda_3\mu_3)$ может соответствовать несуществующему событию.

Если учесть, что множество событий как агента в целом, так и отдельных ИП или ИР алгоритмически предопределено разработчиками, а наборы правил являются в общем случае результатом экспертных заключений, то выражение (9) позволяет двояко трактовать множество M_r^Q. С одной стороны, для полного набора событий заданного для ИП или ИР, множество M_r^Q представляет из себя эталонные наборы S^r событий для каждого из возможных состояний отношений агента. С другой стороны, регистрируемый в процессе функционирования ИП и ИР набор событий будет отличаться от эталонного набора, который обозначим как текущий набор M^C.

Понятия эталонного и текущего наборов событий также можно описать с помощью предикатов «Событие входит в правило» – $Pr1(m)$, «Событие произошло» – $Pr2(m)$ и «Событие зарегистрировано» – $Pr3(m)$. Эталонный набор событий должен определяться только тавтологией $Pr1(m) \wedge Pr2(m) \wedge Pr3(m)$, в то время как текущий набор событий может быть представлен следующим образом:

$Pr1(m) \wedge Pr2(m) \wedge Pr3(m)$ – событие произошло и зарегистрировано,

$Pr1(m) \wedge Pr2(m) \wedge \overline{Pr3(m)}$ – событие произошло, но не зарегистрировано,

$Pr1(m) \wedge \overline{Pr2(m)} \wedge Pr3(m)$ – событие не произошло, но есть регистрация,

$Pr1(m) \wedge \overline{Pr2(m)} \wedge \overline{Pr3(m)}$ – событие не произошло и не зарегистрировано.

Данные высказывания позволяют говорить, что $M_r^Q \Leftrightarrow S^r \vee M^C$, при этом в силу истинности $Pr1(m)$ во всех высказываниях, на данном этапе исследования можно полагать $|S^r| \geq |M^C|$.

Свертка событий и сообщений

Проведенная в предыдущем разделе ортогонализация событий и сообщений для ИП и ИР агента позволяют упростить терминологию следующим образом: «события и сообщения» далее будем именовать как «события», эталонные наборы событий как «шаблоны», а ИП и ИР, рассматривая их как носители сообщений – как «объекты». Соответственно, введем следующие обозначения:

K – множество объектов в составе агента и $k \in K$ – отдельный объект;

R_k – множество возможных состояния объекта $R_k \subseteq R$ и $r_k \subseteq R_k$ – текущее состояния объекта;

M_k – полный набор событий алгоритмически реализованный на объекте;

F_k – целевая функция отбора событий объекта, как следует из (10);

S_k^r – формируемый экспертно для каждого состояния $r \in R$ и для каждого объекта $k \in K$ шаблон событий, $S_k^r \subseteq M_k$;

C_k – текущий набор событий отдельного объекта $k \in K$, формируемый алгоритмически на дискретный момент времени, $C_k \subseteq M_k$;

$V_k^r = \{S_k^r | r \in R, k = const\}$, $V_k^r \subseteq M_k$ – вариант, когда отдельное состояние объекта (или группы объектов) описывается несколькими шаблонами событий.

Также сформулируем дополнительные условия.

Y5. Одно и тоже событие может входить в разные шаблоны для разных состояний $\sum_{k \in K} |S_k^r| \geq |M_k|$.

Y6. Для каждого состояния и для каждого объекта существует не менее одного шаблона событий $\forall r \forall k \; \exists S_k^r$.

Отметим, что шаблоны состояний S_k^r для каждого объекта относительно постоянны: они могут изменяться только при внесении разработчиками изменений в их состав. В то время как расчеты состояний объекта выполняются в дискретные моменты времени. Вопросы формирования текущих наборов и влияние дискретов времени на оценку состояния отношений требуют отдельного исследования.

Сделаем следующее утверждение

Утверждение 1. Состояние объекта определяется соотнесением текущего набора событий и эталонного набора $r_k = \varphi(C_k, S_k^r)$.

Доказательство будем проводить по необходимости и достаточности.

Необходимость. Если представлять взаимосвязи между состоянием r_k, формулой F_k и шаблоном S_k^r с точки зрения необходимости, то получим следующее правило. Для определения состояния необходима формула, а для расчета формулы необходим соответствующий шаблон событий. Что через отношение необходимости можно записать как $(r_k \leftarrow F_k) \wedge (F_k \leftarrow S_k^r)$. В силу правила цепного заключения получаем формулирование состояния на основе эталонного набора событий $r_k \leftarrow S_k^r$.

Достаточность. Если представлять взаимосвязи между состоянием r_k, формулой F_k и текущим набором C_k с точки зрения достаточности, то получим следующее правило. Из заданности r_k и F_k следует, что для определения текущего состояния достаточно формулы, а для расчета формулы достаточно соответствующего набора событий. Что через отношение достаточности можно записать как $(C_k \rightarrow F_k) \wedge (F_k \rightarrow r_k)$. Опять же в силу правила цепного заключения имеем определение состояния на основе текущего набора событий $C_k \rightarrow r_k$.

В итоге получаем $C_k \rightarrow r_k \leftarrow S_k^r$. С точки зрения теории категорий, речь можно вести о коммутационной диаграмме уравнителя, изображенной на рисунке 1.

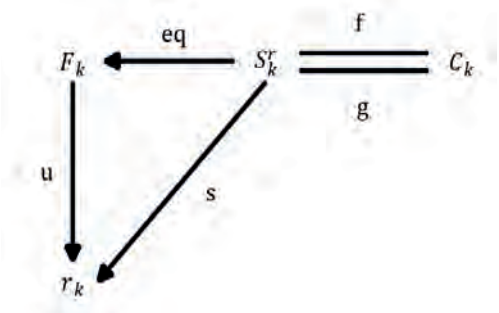

Рис. 1. Коммутационная диаграмма уравнителя

Морфизм *eq* следует из (10). Морфизм *m* следует из *Y6*. На основании этих же условий можно записать $r_k = F_k(M_k)$, что определяет морфизм *u*. При этом вследствие условий необходимости и достаточности выполняется требование $eq \circ u = s$ для уравнителя. В результате получаем $f \circ s = g \circ s$. Следовательно, подлежащим определению остается именно результат соотнесения текущего и эталонного наборов событий. Что и требовалось доказать.

Назовем функцию $\varphi(C_k, S_k^r)$ функцией вхождения. Как следует из диаграммы рисунка 1, результатом работы функция вхождения фактически является двоичный вектор, формируемый по следующему правилу

$$\varphi(x, y) = \begin{cases} 1, \exists (f \vee g) \\ 0, \nexists (f \vee g) \end{cases} \quad (12)$$

где: $x \in C_k$ и $y \in S_k^r$.

Морфизмы *f* и *g* на рисунке 1 можно трактовать с точки зрения направления сравнения текущего и эталонного наборов событий в зависимости от их мощности. Если состав эталонного набора событий по смыслу формируется разработчиком объекта , то состав текущего набора событий полностью зависит от дискретов времени в течение которого он формируется. Как уже отмечалось ранее, вопрос зависимости результатов сравнения наборов событий от дискретов времени заслуживает отдельного исследования.

Таким образом, в следствие *Утверждения 1*, задачу определения состояния объекта агента по текущему набору событий следует рассматривать как определения факта наличия совпадения (12) текущего набора событий со всеми возможными для данного объекта и данного состояния шаблонами, то есть вариантами.

$$\varphi(C_k, S_k^r) : C_k \bigcap\nolimits_{r \in R} V_k^r \neq \emptyset \quad (13)$$

Наличие морфизмов *f* и *g* на рисунке 1 кроме того является причиной возможного комбинаторного взрыва, поскольку показывает необходимость проведения сравнения событий текущего и эталонных наборов по принципу «каждый с каждым».

Но с учетом условия *Y4* и правила *L2* (как было показано на примере (11)), каждое событие представляет из себя однозначно *определенное* сочетание строго *определенных* морфизмов между множествами параметров именно *различных* признаков. Что дает основание сделать следующее утверждение.

Утверждение 2. Параметры признаков могут использоваться как обозначения координат морфизмов.

Доказательство основано на определении морфизма $f: X \rightarrow Y$, где именование начала и окончание морфизма как ребра направленного графа $dom(f) = X$ и $cod(f) = Y$. Правила *L1* и *L2* и пример (11) позволяют рассматривать собы-

тие как многоместное отношение между признаками с морфизмами $f: SI \to SD$ и $g: SD \to SL$, то есть для f – $dom(f) = SI$, $cod(f) = SD$ и для g – $dom(g) = SD$, $cod(g) = SL$. Следовательно, можем представить событие как $m \Leftrightarrow g(\theta,\lambda) \bowtie f(\lambda,\psi)$, где через $\bowtie$ обозначим сцепку морфизмов для соответствующих параметров признаков. Введение операции сцепки определяется в общем случае необходимостью соблюдения порядка следования признаков, определяемого правилом *L1*. Соответственно, все возможные сочетания морфизмов по признакам для объекта можно записать как $M_k = Hom(SI, SD) \times Hom(SD, SL)$. Обозначим через $H = \sum_{r \in R} |S_k^r|$ общее число всех событий, образующих шаблоны всех состояний объекта, а сочетания морфизмов для таких событий, как $W_k = \bigcup_{i \in H} (g_i(\theta,\lambda) \bowtie f_i(\lambda,\psi))$. Тогда в соответствии с коммутационной диаграммой классификатора представленной на рисунке 2, морфизм $M_k \to \{0,1\}$ представляет собой характеристическую функцию, принимающую значение 1 на подмножестве W_k, что дает основания говорить о вытекающей из (10) функции отбора F_k.

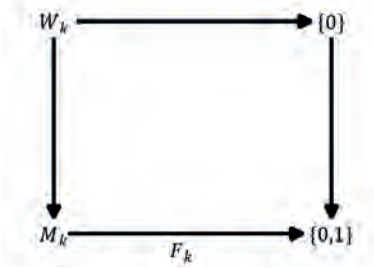

Рис. 2. Коммутационная диаграмма классификатора

Таким образом, F_k есть функция отбора событий для формирования шаблонов состояний объекта именно на основе сцепки морфизмов $g(\theta,\lambda) \bowtie f(\lambda,\psi)$. Доказательство закончено.

По индукции любой набор событий объекта для отдельного состояния при произвольном, но конечном числе признаков (например, $\{A, \cdots, Z\}$) может быть представлен как

$$M_k, C_k, S_k^r, V_k^r \Leftrightarrow Hom(A,B) \times_{F_k} \cdots \quad (14)$$
$$\cdots \times_{F_k} Hom(Y,Z)$$

Утверждение 3. Параметр первого признака в схеме события может использоваться для именования сцепки морфизмов соответствующей определенному событию.

Доказательство. Доказательство будем проводить используя обозначения принятые в примере (11). Пусть $\mathbf{A}$ – множество шкал признаков, $\mathbf{B}$ – это произведение $SD \times_A SL$ над $\mathbf{A}$ вместе с морфизмами $b_1: SD \to \lambda_m$ и $b_2: SL \to \mu_m$ определяющими параметры для конкретного события m. Морфизмы a_1 и a_2 дают декартов квадрат такой, что $B = \{(\lambda_m, \mu_m) \in SD \times SL: a_1(\lambda_m) = a_2(\mu_m)\}$.

То есть, морфизмы a_1 и a_2 определяют выбор конкретных параметров признаков. Далее, в силу правила *L2* и выражения (11), мы можем ввести шкалу признака SI и морфизмы $q_1: SI \to SD$ и $q_2: SI \to SL$ сохраняя коммутативность диаграммы как показано на рисунке 3.

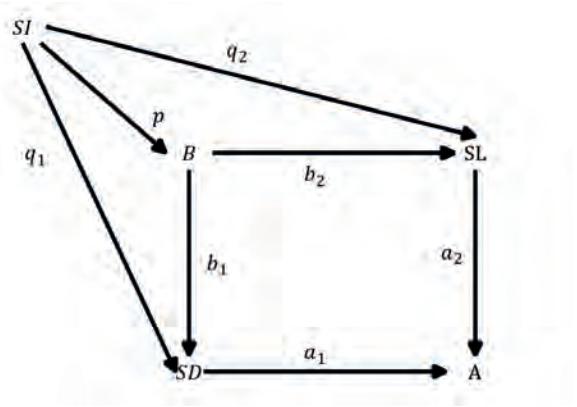

Рис. 3. Коммутативная диаграмма именования

Соответственно, имеет место единственный морфизм $p: SI \to B$, который и является именованием сцепки морфизмов, соответствующих определенному событию, что и требовалось доказать. Доказательство утверждения 3 для числа признаков больше трех проводится по индукции.

Приведенные рассуждения позволяют сконструировать свертку событий в виде матрицы, где:

- строки поименованы параметрами шкалы SD,
- столбцы поименованы параметрами шкалы SL,
- ячейки матрицы содержат параметры шкалы SI для каждого события в свертке.

При этом:

- согласно правилу *L1*, для каждой операции всегда есть носитель и уровень воздействия, то есть отношения между признаками сюрьективны $SI \mapsto SD \mapsto SL$, что влечет за собой их упорядоченность;
- порядок следования параметров признаков по столбцам и строкам матрицы может быть произвольный, но фиксированный все время применения свертки;
- для функции вхождения порядок следования событий может быть произвольным.

Применение свертки событий

Пример 1. Примерный вид матрицы в соответствии с приведенным ранее примером (11) как набора событий и исключением из него $m_i = (\theta_2 \lambda_3 \mu_3)$ через параметры признаков приведен ниже.

	λ_1	λ_2	λ_3
μ_1			θ_2, θ_1
μ_2			
μ_3			θ_1

Пример 2. Пусть набор событий состоит из $m_1 = (\theta_1 \lambda_1 \mu_1)$ $m_2 = (\theta_2 \lambda_2 \mu_2)$ $m_3 = (\theta_3 \lambda_3 \mu_3)$. Кортеж набора имеет вид $\langle\{\theta_1, \theta_2, \theta_3\}\{\lambda_1, \lambda_2, \lambda_3\}\{\mu_1, \mu_2, \mu_3\}\rangle$ и при его разложении даст ложные определения событий. В то время как матрица таких ошибок не дает

	λ_1	λ_2	λ_3
μ_1	θ_1		
μ_2		θ_2	
μ_3			θ_3

Пример 3. Пусть набор событий состоит из $m_1 = (\theta_1 \lambda_1 \mu_1)$ $m_2 = (\theta_2 \lambda_2 \mu_2)$ $m_3 = (\theta_3 \lambda_3 \mu_3)$ $m_4 = (\theta_2 \lambda_1 \mu_1)$. Кортеж набора имеет вид $\langle\{\theta_1, \theta_2, \theta_3\}\{\lambda_1, \lambda_2, \lambda_3\}\{\mu_1, \mu_2, \mu_3\}\rangle$ при его разложении даст ложные определения событий. Матрица свертки для такого набора событий имеет вид

	λ_1	λ_2	λ_3
μ_1	θ_1, θ_2		
μ_2		θ_2	
μ_3			θ_3

Использование матрицы свертки событий рассмотрим на следующем примере.

Пример 4. Пусть отдельное состояние объекта описывается вариантом из двух шаблонов событий, которые образуют С-систему алгебры кортежей, являющуюся аналогом ДНФ системы.

$$A1 = \begin{bmatrix} \{a,b\} & \{f,e\} & \{g,h\} \\ \{a,c\} & \{d,e\} & \{h,j\} \end{bmatrix}$$

Отметим, что для такого представления варианта состояния объекта, события должны быть упорядочены по их источникам, то есть иметь схему $\langle Log1 Log2 Log3\rangle$. Пусть также задан текущий набор событий $A2 = [\{b,c\} \quad \{d,f\} \quad \{g,j\}]$. Алгебра кортежей позволяет выполнить операцию проверки включения кортежа *A2* в систему *A1*, что соответствует определению функции вхождения (13). В общем виде проверка включения основана на разбиении A1 и A2 на элементарные кортежи вида $A1' = \{(afg), \cdots, (beh), (adh), \cdots, (cej)\}$ и $A2' = \{(bdg), \cdots, (cfj)\}$ и их попарном пересечении $A2' \cap A1' = (bdg) \cap (afg), \cdots, (cfj) \cap (beh), (bdg) \cap (adh), \cdots, (cfj) \cap (cej)$

Результат проверки включения требует дальнейшей интерпретации, но представляет интерес определение числа операций пересечения, поскольку алгебра кортежей представляется общепризнанным инструментом работы с множествами. Данное число можно определить как $\sum_{i \in v}(|A2'| \times |A_i'|)$, где *v* – число наборов в варианте шаблонов *A1*, то есть речь идет о полиноминальной зависимости от размеров текущего и эталонного наборов событий. Разработанные алгоритмы снижения числа пересечений не отменяют полиноминальной зависимости от размерности.

При использовании матрицы свертки событий справедливо следующее утверждение.

Утверждение 4. Проверка вхождения текущего набора событий в эталонный имеет линейный характер зависимости от размерности сравниваемых компонент.

Доказательство. При использовании для определения состояния отношения объекта матрицы свертки, С-система А1 представляет из себя матрицу эталонного набора событий, а кортеж А2 – множество событий текущего набора.

Построение матрицы свертки проводится аналогично предыдущим примерам и рассматриваться не будет. Отметим только, что в ее основе лежит схема размерности $SI = \{\theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6\}$, $SD = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5\}$, $SL = \{\mu_1, \mu_2, \mu_3, \mu_4\}$, что дает возможность классифицировать события с точки зрения ИБ по 120 типам.

В соответствии с определением события $m_i = (\theta_i \lambda_i \mu_i)$, примем λ_i и μ_i в качестве координат текущего или эталонного события, а θ_i – как сравниваемые величины. Обозначим координаты матрицы свертки *A1* (наименование строк и столбцов) как λ_i и μ_i а для каждого события из *A2* как λ_i', μ_i'. соответственно. Координаты текущего и эталонного событий идентичны, поскольку являются *i-м* элементом множеств SD и SL с одинаковым индексом. Следовательно, применение λ_i', μ_i' текущего события к матрице свертки дает содержимое соответствующей ячейки матрицы.

Введем функции:

— ρ (m), возвращающую координаты конкретного события $(x, y) = \rho(m)$;

— $\pi(\rho(m),A1)$, возвращающую содержимое ячейки матрицы $\Theta_{x,y} = \pi((x, y), A1)$.

Будем полагать, что величина θ_i' получается автоматически из определения события. В итоге получаем выражение, дающее подмножество содержащее $\emptyset$ или θ_i' для событий текущего набора $m_i' \in A2 \Rightarrow z_i = \theta_i' \cap \Theta_{x,y}$

Тогда, при начальном значении $Z = \emptyset$ выражение (13) можно записать как

$$\varphi(C_k, S_k^r): \forall m_i \in C_k, Z \coprod_{i \in |C_k|} (z_i, i) \mid z_i \neq \emptyset \quad (15)$$

Анализ выражения (15) с учетом определения функции $\pi(\rho(m),A1)$ показывает, что количество операций, необходимых для получения результата вхождения C_k в S_k^r линейно зависит от размера текущего набора событий. Что и требовалось доказать.

Получаемое в результате вычисления $Z = \varphi(C_k, S_k^r)$ множество позволяет определить количественные характеристики вхождения C_k в S_k^r:

— мощность множества Z характеризует уровень совпадения текущего и эталонного наборов событий;

— набор параметров θ из C_k, позволяющий при необходимости ввести дополнительные оценки совпадения текущего и эталонного наборов событий с точки зрения конфиденциальности, целостности и доступности.

Положим, что матрица свертки событий создана для всех возможных вариантов состояний отношений. Тогда решающая функция $\psi: M_r^Q \to R$ из (10) может быть определена следующим образом $M_r^Q = \{C_k, V_k^1, \cdots, V_k^n\}$, где $n = |R|$. С учетом (15) получаем результат работы решающей функции $Q_k = \forall r \in R \ \varphi(C_k, V_k^r) = [Z_k^1, \cdots, Z_k^n]$ – вектор оценок каждого из состояний для конкретного объекта.

Функцию определения интегральной оценки состояния отношения $\beta R \gamma$ агента с отдельным респондентом на основании исходных данных на уровне ИП или ИР $Ref(Q_k)$ рассмотрим в следующей статье цикла.

Типизация агента

Из выражения (4) и последующих рассуждений, дающих выражения (5) – (10), можно положить, что в самом общем виде состояние агента можно рассматривать с двух точек зрения: что он знает о себе (внутренняя оценка) и что агент знает о своем окружении (внешняя оценка). Соответственно, множество *ME* может быть разделено на следующие целевые подмножества: M^β – события и сообщения доступные агенту и M^γ – события и сообщения доступные респонденту.

Представление агента в виде автомата (2) позволяет представить эти подмножества в следующем виде: $M^\beta = \{MS^\beta, QM_\gamma, MS^\gamma\}$ и $M^\gamma = \{MS^\gamma, MS^\beta, QM_\gamma\}$

Напомним, что QM_γ – алгоритмически определенный по составу и содержанию конечный набор событий и сообщений, определяющий реакцию агента на внешние воздействия, MS^β – исходящие сообщения агента, MS^γ – входящие сообщения агента

Результаты предыдущих разделов статьи позволяют доопределить функции автомата (2) следующим образом: функция воздействия $\delta: MS^\gamma \to QM_\gamma$ и функция отклика $\pi: QM_\gamma \to MS^\beta$. То есть, множества M^β и M^γ следует рассматривать как видимость результатов работы функций воздействия и отклика. Представляется целесообразным под видимостью понимать мощность множеств MS^γ, MS^β, QM_γ доступных со стороны агента и респондента. Для этого введем функцию видимости $F^*: |X| \xrightarrow{\Omega} |Y|$, осуществляющую фильтрацию множеств MS^γ, MS^β, QM_γ в M^β и M^γ.

Тогда должно выполняться условие $|Y| \leq |X|$, что соответствует выражению $|Y| = |X|/\Omega$. Аналогично с M^β и M^γ функции видимости будем обозначать как $F^\beta(X, \Omega)$ и $F^\gamma(X, \Omega)$.

Определения и выводы первой части статьи позволяют представить Защитника и Нарушителя в качестве агентов. Положим, что респондентом является Нарушитель (*H*), а агентом - Защитник (*D*). Отсюда следует, что множества M^β и M^γ и соответствующие функции видимости имеют двойственную природу: каждый из субъектов (представленный как агент) воспринимает другую сторону взаимодействия как респондента. Для уточнения принадлежности функций введем следующие обозначения:

$F^\beta\lfloor_D(*)$ – функция обеспечивающая видимость сообщений Защитником своих собственных сообщений;

$F^\gamma\lfloor_D(*)$ – функция обеспечивающая видимость сообщений Защитника со стороны Нарушителя;

$F^\gamma\lfloor_H(*)$ – функция обеспечивающая видимость сообщений Нарушителя со стороны Защитника;

$F^\beta\lfloor_H(*)$ – функция обеспечивающая видимость сообщений Нарушителем своих собственных сообщений.

Тогда базовые действия Защитника, применимые для всех агентов из состава ИС, можно сформулировать следующим образом

$$SA_{QM}(D) = \arg\max_{\Omega} F^{\beta}\lfloor_{D}(QM_{\gamma},\Omega) \wedge \wedge \arg\min_{\Omega} F^{\gamma}\lfloor_{D}(QM_{\gamma},\Omega) \quad (16)$$

Выражение (16) означает наибольшую видимость внутренних сообщений агента со стороны Защитника и наименьшую видимость таких сообщений для Нарушителя.

$$SA_{MS^{\beta}}(D) = \arg\min_{\Omega} F^{\gamma}\lfloor_{D}(MS^{\beta},\Omega) \quad (17)$$

Выражение (17) означает минимизацию для Нарушителя видимости исходящих сообщений Защитника или иначе – ограничение для Нарушителя возможности видеть результаты его деятельности.

$$SA_{MS^{\gamma}}(D) = \arg\min_{\Omega} F^{\gamma}\lfloor_{D}(MS^{\gamma},\Omega) \quad (18)$$

Выражение (18) означает минимизацию видимости со стороны Нарушителя входящих сообщений Защитника или иначе – ограничение возможности Нарушителя воздействовать на Защитника.

В целом, на основании (16) – (18) действия Защитника могут быть сформулированы как $SA(D) = SA_{QM}(D) \wedge SA_{MS^{\beta}}(D) \wedge SA_{MS^{\gamma}}(D)$, что соответствует стремлению Защитника иметь возможно более полную информацию о состоянии ИП и ИР агента, а также в наибольшей степени ограничить возможности Нарушителя по получению такой информации и воздействию на ИП и ИР агента.

Для Нарушителя базовые действия формулируются аналогично.

$$SA_{QM}(H) = \arg\max_{\Omega} F^{\gamma}\lfloor_{D}(QM_{\gamma},\Omega) \wedge \wedge \arg\max_{\Omega} F^{\beta}\lfloor_{H}(QM_{\gamma},\Omega) \wedge \wedge \arg\min_{\Omega} F^{\gamma}\lfloor_{H}(QM_{\gamma},\Omega) \quad (19)$$

Выражение (19) означает стремление Нарушителя обеспечить наибольшую видимость внутренних сообщений своего агента и атакуемого респондента (Защитника) и в то же время обеспечить наименьшую видимость своих сообщений для Защитника или иначе – максимально скрыть от Защитника свою деятельность.

$$SA_{MS^{\beta}}(H) = \arg\max_{\Omega} F^{\beta}\lfloor_{H}(MS^{\beta},\Omega) \wedge \wedge \arg\min_{\Omega} F^{\gamma}\lfloor_{H}(MS^{\beta},\Omega) \quad (20)$$

Выражение (20) означает стремление обеспечить наибольшую видимость своих исходящих сообщений со стороны Нарушителя и минимизировать их видимость для Защитника или иначе – максимально скрыть свои атакующие действия.

$$SA_{MS^{\gamma}}(H) = \arg\max_{\Omega} F^{\beta}\lfloor_{H}(MS^{\gamma},\Omega) \wedge \wedge \arg\min_{\Omega} F^{\gamma}\lfloor_{H}(MS^{\gamma},\Omega) \quad (21)$$

Выражение (21) означает стремление Нарушителя иметь максимальную видимость для входящих сообщений от Защитника и при этом обеспечить их минимальную видимость для Защитника или иначе – скрыть свою осведомленность.

В целом, на основании (19) – (21) действия Нарушителя могут быть сформулированы как $SA(H) = SA_{QM}(H) \wedge SA_{MS^{\beta}}(H) \wedge SA_{MS^{\gamma}}(H)$, что соответствует стремлению Нарушителя иметь максимально полную информацию о состоянии ИП и ИР респондента (атакуемого агента) и возможность воздействовать на них, а также в наибольшей степени скрыть события и сообщения описывающие его действия с ИП и ИР респондента.

В качестве промежуточного итога отметим.

1. Защитник не может ограничить действие $lim(SA_{MS^{\gamma}}(D)) \to 0$ и $lim(SA_{MS^{\beta}}(D)) \to 0$ в силу необходимости обеспечения доступности ИР и ИП агента, что означает невозможность исключения деструктивных действий Нарушителя.в отношении агента.

2. В выражении (16) присутствует требование $F^{\beta}(QM_{\gamma},\Omega) > F^{\gamma}(QM_{\gamma},\Omega)$, а в выражении (19) присутствует требование $F^{\gamma}(QM_{\gamma},\Omega) > F^{\beta}(QM_{\gamma},\Omega)$, что дает противоречие в требованиях к функционированию агента и входящих в его состав объектов.

Представляется принципиально важным отметить следующие особенности, которые обозначим как исходные посылки.

P1. Определение состояния объекта из состава агента не зависит от принадлежности аккаунта данного агента Защитнику или Нарушителю.

P2. Определение состояния объекта из состава агента основывается на алгоритмически заданных событиях, которые не могут быть изменены в процессе функционирования агента.

P3. Для Защитника и Нарушителя, представленных в виде аккаунта агента, базовые действия эквивалентны.

P4. Определение базовых действия основывается на тех же алгоритмически заданных событиях объектов.

P5. Отличие между базовыми действиями и определением состояния заключается в способах фильтрации событий объекта.

P6. Защитник не может ограничить действие $lim(SA_{MS^{\gamma}}(D)) \to 0$ и $lim(SA_{MS^{\beta}}(D)) \to 0$ в силу необходимости обеспечения доступности ИР и ИП агента, что означает невозможность исключения деструктивных действий Нарушителя.в отношении агента.

P7. В выражении (16) присутствует требование $F^{\beta}(QM_{\gamma},\Omega) > F^{\gamma}(QM_{\gamma},\Omega)$, а в выражении (19) присутствует требование $F^{\gamma}(QM_{\gamma},\Omega) > F^{\beta}(QM_{\gamma},\Omega)$, что дает противоречие в требованиях к функциониро-

ванию агента и входящих в его состав объектов

Посылки *P1-P7* дают основание выдвинуть следующую гипотезу.

Объекты из состава агента и агент в целом, осуществляющие обработку информации в интересах Пользователя, имманентно не обладают способностью обеспечить конфиденциальность, целостность и доступность информации. В случае получения Нарушителем аккаунта агента, все объекты агента неизбежно становятся инструментом Нарушителя.

В терминах теории категорий можно также выдвинуть «*ко*-»гипотезу.

Защиту информации в информационной системе можно обеспечить только за счет наличия и топографии размещения специализированных агентов, которые на любое внешнее воздействие респондентов, связанное с обработкой информации в интересах Пользователя, обеспечивают состояние отношений «Безразличное», когда агент целенаправленно не участвует в процессах обработки информации респондентами, но при этом обладает способностью влиять на информационные потоки взаимодействия респондентов.

Следует отметить, что современные технологии построения информационных систем, такие как виртуализация, микросервисы и инфраструктура как код, может быть впервые за всю историю развития вычислительной техники, дают возможность реализации таких агентов. Главным качеством таких агентов будет их построение на основе принципа отсутствия физических и логических адресов на всех интерфейсах, кроме управляющего. Такие возможности предоставляют технологии типа «ethernet-bridge», успешным примером практической реализации которых является, например, изделии ССПТ-2 НПО «Фрактел».

Заключение

Результаты исследования и разработок данной статьи дают возможность определять состояние отношений информационных потоков и информационных ресурсов из состава агента с его респондентами на основе матрицы сверток событий, что позволяет:

- Обеспечить линейную зависимость операций проверки вхождения текущего набора событий в эталонный только от размерности текущего набора.
- Обеспечить возможность параллельного и независимого определения состояния отношений для разных объектов.
- Обеспечить предварительное формирование на этапе разработки правил отбора, ортогонализации, формирования эталонных наборов и матриц свертки событий, что позволит значительно ускорить определение состояния отношений в процессе работы агента.

Целесообразно обеспечить формирование правил отбора, ортогонализации, формирования эталонных наборов и матриц свертки событий разработчиками ИП и ИР в рамках выполнения нормативных требований по ИБ (например, в рамках выполнения ГОСТ ИСО/МЭК 15408).

Кроме того, в рамках ортогонализации событий, целесообразно обеспечить выработку экспертным сообществом признаков и параметров ортогонализации и внесение соответствующих изменений в состав и способы регистрации событий информационных ресурсов и информационных потоков агентов.

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. Инфраструктура как код: формируется новая реальность информационной безопасности / А.О. Калашников, К.А. Бугайский // Информация и безопасность. – 2019. – Т. 22, № 4. – С. 495-506.
13. Бугайский, К.А. Расширенная модель открытых систем (Часть 1) / К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда // Информация и безопасность. – 2022. – Т. 25, № 2. – С. 169-178. – DOI 10.36622/VSTU.2022.25.2.001.
14. Калашников А.О. Применение логико-вероятностного метода в информационной безопасности (Часть 1) / Калашников А.О., Бугайский К.А., Бирин Д.С., Дерябин Б.О., Цепенда С.О., Табаков К.В. // Вопросы кибербезопасности. – 2023. – №4(56). – С. 23-32.
15. Калашников А.О. Применение логико-вероятностного метода в информационной безопасности (Часть 2) / Калашников А.О., Бугайский К.А., Аникина Е. И., Перескоков И.С., Петров Ан.О., Петров Ал.О., Храмченкова Е.С., Молотов А.А. // Вопросы кибербезопасности. – 2023. – №5(57). – С. 113–127. DOI:10.21681/2311-3456-2023-6-113-127.
16. Бугайский, К.А. Расширенная модель открытых систем (Часть 2) / К.А. Бугайский, И.С. Перескоков, А.О. Петров, А.О. Петров // Информация и безопасность. – 2022. – Т. 25, № 3. – С. 321-330. – DOI 10.36622/VSTU.2022.25.3.001.
17. Бугайский, К.А. Расширенная модель открытых систем (Часть 3) / К.А. Бугайский, Б.О. Дерябин, К.В. Табаков, Е.С. Храмченкова, С.О. Цепенда // Информация и безопасность. – 2022. – Т. 25, № 4. – С. 501-512.
18. Калашников, А. О. Модель количественного оценивания агента сложной сети в условиях неполной информированности / А. О. Калашников, К. А. Бугайский // Вопросы кибербезопасности. – 2021. – № 6(46). – С. 26–35. – DOI 10.21681/2311-3456-2021-6-26-35.
19. Котенко И. В. Технологии больших данных для корреляции событий безопасности на основе учета типов связей / И. В. Котенко, А. В. Федорченко, И. Б. Саенко, А. Г. Кушнеревич // Вопросы кибербезопасности. – 2017. – № 5(24). – С. 2-16. – DOI 10.21681/2311-3456-2017-5-2-16.
20. Дойникова, Е. В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер / Е. В. Дойникова, И. В. Котенко // Труды СПИИРАН. – 2018. – № 2(57). – С. 211-240.
21. Кулик, Б. А. Логика и математика: просто о сложных методах логического анализа / Б. А. Кулик. – Санкт-Петербург : Издательство «Политехника», 2021. – 141 с. – ISBN 978-5-7325-1166-6. – DOI 10.25960/7325-1166-6.

APPLICATION OF THE LOGICAL-PROBABILISTIC METHOD IN INFORMATION SECURITY (PART 1)

Kalashnikov A.O.[9], Bugajskij K.A.[10], Anikina E.V.[11], Pereskokov I.S.[12], Petrov Andrej O.[13], Petrov Aleksandr O.[14], Khramchenkova E.S.[15], Molotov A.A.[16]

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, category theory, methods for evaluating events under the condition of incomplete information, logical-probabilistic methods 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. It is shown that the state of the agent's relations can be obtained on the basis of appropriate assessments of states at the level of information resources and information flows from the agent. A scheme of features for representing events from the point of view of information security has been developed and a method for uniform representation of events and messages coming from different sources has been proposed. It is proved that the state of the relationship at the level of an information resource or information flow is determined as a result of the correlation of the current and reference sets of events. It is proved that events and their sets can be represented as multi-place relations of features. It is proved that each feature relation for an event can be named by the first element of the feature scheme. A feature convolution matrix has been developed containing only permitted combinations of feature parameters for sets of events describing the state of relations. It is proved that the application of the convolution matrix gives a linear dependence on the dimension of the sets of events. Formal definitions of the basic actions of the Defender and the Violator on the agent are given. The necessity of making changes to the composition and methods of registering information security events of information resources and information flows is substantiated.*

Scientific novelty: *consideration of information security issues using the apparatus of mathematical and logical relations, as well as category theory. Development of an event convolution matrix based on a categorical approach to determine the state of an agent's relationships. Proof of the linear dependence of the comparison operations of the current and reference sets of events when using the event convolution matrix. Development of formal definitions of basic agent operations for the Defender and the Violator. Two hypotheses describing the agent's capabilities in the field of information security are formulated.*

Keywords: *information security model, assessment of complex systems, logical-probabilistic method, category theory, system analysis, multi-agent system.*

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.

9 Andrey O. Kalashnikov, Dr.Sc. (Technology), Principal Researcher at the Laboratory "Complex networks", Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: aokalash@ipu.ru

10 Konstantin A. Bugajskij, Junior Researcher at the Laboratory "Complex networks", Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E mail: kabuga@ipu.ru

11 Eugenia V. Anikina, Research Fellow, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: ajanet@ipu.ru

12 Ilia S. Pereskokov, Junior Researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: pereskokov @phystech.edu

13 Andrei O. Pereskokov, Junior Researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: petrovaojob@gmail.com

14 Aleksandr O. Petrov – Junior Researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: petrovalexandr@ipu.ru

15 Khramchenkova E.S.– Junior Researcher, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E-mail: hramchenkovaes@yandex.ru

16 Aleksandr A. Molotov, software engineer at the Institute of Control Sciences of Russian Academy of Sciences. E mail: alpha.sphere@ya.ru

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.
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. Infrastruktura kak kod: formiruetsya novaya real'nost' informacionnoj bezopasnosti / A.O. Kalashnikov, K.A. Bugajskij // Informaciya i bezopasnost'. – 2019. – T. 22, № 4. – pp. 495-506.
13. Bugajskij, K.A. Rasshirennaya model' otkrytyh sistem (CHast' 1) / K. A. Bugajskij, D. S. Birin, B. O. Deryabin, S. O. Cependa // Informaciya i bezopasnost'. – 2022. – T. 25, № 2. – pp. 169-178. – DOI 10.36622/VSTU.2022.25.2.001.
14. Kalashnikov A.O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 1) / Kalashnikov A.O., Bugaiskii K.A., Birin D.S., Deriabin B.O., Tsependa S.O., Tabakov K.V. // Voprosy kiberbezopasnosti. – 2023. – №4(56) – pp. 23-32.
15. Kalashnikov A.O. Primenenie logiko-veroiatnostnogo metoda v informatsionnoi bezopasnosti (Chast 2) / Kalashnikov A.O., Bugaiskii K.A., Anikina E. I., Pereskokov I.S., Petrov An.O., Petrov Al.O., Khramchenkova E.S., Molotov A.A. // Voprosy kiberbezopasnosti. – 2023. – №5(57). – pp. 113-127. DOI:10.21681/2311-3456-2023-6-113-127.
16. Bugajskij, K.A. Rasshirennaya model' otkrytyh sistem (CHast' 2) / K.A. Bugajskij, I.S. Pereskokov, A.O. Petrov, A.O. Petrov // Informaciya i bezopasnost'. – 2022. – T. 25, № 3. – pp. 321-330. – DOI 10.36622/VSTU.2022.25.3.001.
17. Bugajskij, K.A. Rasshirennaya model' otkrytyh sistem (CHast' 3) / K.A. Bugajskij, B.O. Deryabin, K.V. Tabakov, E.S. Hramchenkova, S.O. Cependa // Informaciya i bezopasnost'. – 2022. – T. 25, № 4. – pp. 501-512.
18. Kalashnikov, A. O. Model kolichestvennogo otsenivaniia agenta slozhnoi seti v usloviiakh nepolnoi informirovannosti / A. O. Kalashnikov, K. A. Bugaiskii // Voprosy kiberbezopasnosti. – 2021. – № 6(46). – pp. 26-35. – DOI 10.21681/2311-3456-2021-6-26-35.
19. Kotenko I. V. Tekhnologii bolshikh dannykh dlia korreliatsii sobytii bezopasnosti na osnove ucheta tipov sviazei / I. V. Kotenko, A. V. Fedorchenko, I. B. Saenko, A. G. Kushnerevich // Voprosy kiberbezopasnosti. – 2017. – № 5(24). – pp. 2-16. – DOI 10.21681/2311-3456-2017-5-2-16.
20. Doinikova, E. V. Sovershenstvovanie grafov atak dlia monitoringa kiberbezopasnosti: operirovanie netochnostiami, obrabotka tsiklov, otobrazhenie intsidentov i avtomaticheskii vybor zashchitnykh mer / E. V. Doinikova, I. V. Kotenko // Trudy SPIIRAN. – 2018. – № 2(57). – pp. 211-240.
21. Kulik, B. A. Logika i matematika: prosto o slozhnykh metodakh logicheskogo analiza / B. A. Kulik. – Sankt-Peterburg: Izdatelstvo «Politekhnika», 2021. – 141 p. – ISBN 978-5-7325-1166-6. – DOI 10.25960/7325-1166-6.

ИССЛЕДОВАНИЕ МЕТОДОВ ФОРМИРОВАНИЯ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ ОТ ВНУТРЕННИХ ИСТОЧНИКОВ ИНФОРМАЦИОННЫХ И КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Мещеряков Р.В.[1], Исхаков С.Ю.[2]

Цель работы: *исследование методов формирования индикаторов компрометации внутри инфраструктуры для применения в системах защиты информационных и киберфизических систем.*

Метод исследования: *системный анализ открытых источников данных об индикаторах компрометации, способах их извлечения и методах применения при организации киберразведки внутри защищаемой инфраструктуры и систематизация знаний.*

Полученный результат: *сформулированы актуальные проблемы извлечения индикаторов компрометации от внутренних источников в информационных и киберфизических системах. Предложено алгоритмическое обеспечение для применения таких индикаторов в процессах киберразведки. Сформулированы базовые сценарии применения индикаторов компрометации от внутренних источников при обработке динамических потоков данных об угрозах в условиях изменяемых векторов атак.*

Установлено, что в отрасли киберразведки на сегодняшний день отсутствует унификация в части формирования индикаторов компрометации на основе данных защищаемых систем и дальнейшего обмена информацией между различными средствами защиты, но при этом имеют место ряд доминирующих форматов обмена подобными данными. В ходе исследования рассмотрены и структурированы задачи поиска и извлечения данных из внутренних источников для обогащения систем киберразведки и выявления целенаправленных методов атак на основе применения собственных наборов индикаторов компрометации и предложены методы их решения.

Научная новизна: *систематизированы методы формирования индикаторов компрометации внутри защищаемой инфраструктуры. Разработано алгоритмическое обеспечение применения индикаторов от внутренних источников и предложены базовые сценарии обработки таких данных для защиты киберфизических систем в условиях изменяемых векторов атак.*

Ключевые слова: *индикатор компрометации, киберразведка, контекст, киберфизическая система, система управления событиями безопасности, обогащение, ранжирование.*

DOI:10.21681/2311-3456-2023-6-35-49

Введение

Действительность сегодняшнего дня обуславливает постоянное изменение ландшафта киберугроз, поэтому в современном мире большинство компаний активно применяют системы обнаружения и предотвращения вторжений для защиты своей инфраструктуры. Системы подобного класса позволяют обнаруживать и сигнализировать о подозрительных действиях на периметре сети или на одном из внутренних хостов, однако зачастую обнаружение происходит лишь постфактум, когда уже зафиксированы последствия действий злоумышленников. Кроме того, во многих случаях атака может быть не зафиксирована, поскольку в системах защиты отсутствуют необходимые правила детектирования,

1 Мещеряков Роман Валерьевич, доктор технических наук, профессор, главный научный сотрудник ИПУ РАН, Москва, Россия. E-mail: mrv@ieee.org, ORCID: 0000-0002-1129-8434.

2 Исхаков Сергей Юнусович, кандидат технических наук, начальник отдела анализа и реагирования на компьютерные инциденты ПАО «Промсвязьбанк», Москва, Россия. E-mail: sergey@iskhakov.ru, ORCID: 0000-0003-3346-9262.

учитывающие актуальные изменения в ландшафте киберугроз.

Поэтому решение задачи обнаружения и предотвращения атак на современные информационные и киберфизические системы требует наличия механизмов, позволяющих выявлять ранее неизвестные методы и тактики действий злоумышленников. Применение классических средств защиты, например, средств антивирусной защиты или систем обнаружения вторжений на основе сигнатур, в данном случае весьма ограничено, поскольку подобные технологии не позволяют выявлять атаки с применением легитимного программного обеспечения и определять последовательность действий, способные привести к инцидентам. Кроме того, в современных системах число классических средств защиты информации (СЗИ) зачастую так велико, что генерируемые ими уведомления о возможных инцидентах требуют тщательного профилирования.

Для выявления передовых техник взлома на ранних стадиях атаки сегодня активно применяются механизмы кибербразведки (threat intelligence, TI) [1], включающие в себя сбор и анализ информации о злоумышленниках в части изучения техник, тактик и процедур, используемых при атаках. Одним из основных методов кибербразведки является использование индикаторов компрометации (indicator of compromise, IoC) [1,2] для обогащения СЗИ в информационных и киберфизических системах. IoC представляют собой технические данные, которые можно использовать для идентификации действий злоумышленников, отделяя их при этом от действий легитимных пользователей системы и штатных процессов ее функционирования. Индикаторы компрометации – один из результатов процесса кибербразведки по сбору информации об угрозах. Они могут применяться на операционном и тактическом уровнях кибербразведки [3] для выявления вредоносных объектов или действий и атрибуции их с известными угрозами. Проактивный подход позволяет обеспечить постоянное обновление знаний о киберугрозах и предотвращать атаки, сценарии которых еще не выявляются имеющимися СЗИ.

Поскольку эффективное применение индикаторов компрометации позволяет влиять на скорость реагирования на угрозы, то обсуждению данной проблемы и выдвижению различных подходов и методов посвящено множество исследований отечественных и зарубежных авторов, а также материалов профильных конференций. Активное обсуждение методов кибербразведки мировым научным сообществом отражает актуальность развития данной отрасли научного знания и формированию научно-методологической базы. Однако, результаты исследований, рассмотренные далее, свидетельствуют о том, что в отрасли кибербразведки отсутствуют комплексные решения по формированию индикаторов компрометации на основе данных, генерируемых внутри защищаемых инфраструктур. Большинство научных работ, а также коммерческих продуктов, ориентировано на работу с внешними источниками данных. С одной стороны, внутри инфраструктуры промышленных систем имеется множество источников данных, на основе которых можно организовать процесс формирования индикаторов компрометации. С другой стороны, на практике внутренняя кибербразведка сопряжена со значительными трудозатратами при низкой вероятности быстрого получения результатов. Помимо персонала, сопровождающего средства защиты и системы, необходимо нанимать в штат специалистов для анализа и практического применения подобной информации. К выстраиванию кибербразведки внутри инфраструктуры и работе с внутренними источниками приступают, когда основные процессы информационной безопасности уже находятся на высоком уровне зрелости.

В случае, если команда специалистов уже сформирована, то в инфраструктурах, где процессы уже ИБ выстроены, реальных инцидентов обычно немного, и они однотипны. Таким образом, в настоящее время в научной литературе практически не представлено методическое обеспечение по выстраиванию процессов кибербразведки внутри защищаемых инфраструктур. Настоящая статья посвящена исследованию проблем развития внутренней кибербразведки и вопросам формирования индикаторов компрометации на основе данных от внутренних источников.

1. Современные направления и методы кибербразведки

Интенсивное изменение ландшафта угроз и развитие инструментов автоматизации управления информационными и киберфизическими системами влечет за собой необходимость совершенствования методов кибербразведки. Современный подход к threat intelligence включает в себя выявление, анализ и описание индикаторов компрометации. Выполнение всех указанных действий позволяет получить действительно качественные данные кибербразведки, которые могут быть применены для реальной защиты объекта.

Индикаторы компрометации – это технические данные, применяемые СЗИ для обнаружения вре-

доносных объектов или процессов. Ключевым свойством индикатора являются определенные технические артефакты. При этом индикаторы, в описании которых имеется контекст, представляют наибольшую ценность. Контекст –дополнительное описание угрозы, с которой связан индикатор, позволяющее оценить возможность применения IoC в конкретном случае на защищаемом объекте. Наиболее простой способ описания контекста – текстовое поле, в котором в свободной форме представлена информация, имеющая отношение к индикатору. Например, время первого обнаружения, атрибуция к группировкам злоумышленников и др. В случае использования для описания контекста единого поля его обработка будет осложнена, поскольку для автоматизированного парсинга в таком случае необходимы четкие правила формирования текста. Иначе определить возможность применения и ценность отдельного индикатора для конкретной инфраструктуры можно будет только вручную. В [4] представлена классификация источников данных для индикаторов компрометации: внутренние источники, внешние модерируемые источники и внешние открытые источники.

Работы [5, 6] посвящены обзору рынка технологий передачи индикаторов и управления ими. При этом в [5] основной фокус нацелен на изучение влияния отношений между поставщиками данных кибрерразведки на механизмы обмена IoC, в то время как исследование [6] посвящено анализу непосредственно TI-платформ и протоколов обмена информацией об киберугрозах. Указанные работы свидетельствуют, что в отрасли threat intelligence до сих пор нет единых стандартов для представления и обмена индикаторами компрометации. При этом отмечается, что стандарты STIX и OpenIOC являются доминирующими на современном рынке кибербразведки.

В [7] рассмотрены инструменты для автоматизации извлечения индикаторов компрометации из публикаций в средствах массовой информации и различных отчетов, содержащих неструктурированные данные. Также представлен метод для сравнения таких инструментов. Однако, предлагаемые авторами механизмы ориентированы на внешние источники индикаторов и не могут быть применимы к источникам внутренним.

В [8] рассматривается фреймворк, позволяющий обрабатывать внешние источники кибербразведки, представленные в виде структурированных данных. Характерным отличием решения является возможность автоматизировать классификацию индикатора в соответствии с методологией матрицы Mitre ATT&CK [9]. Подобные механизмы в теории могут быть применимы и к индикаторам от внутренних источников, но только после того, как эти индикаторы уже извлечены и приведены к одному из форматов обмена данными кибербразведки [10].

В [11] затронута тема интеграции средств защиты при отражении DDoS-атак с помощью систем управления событиями безопасности (security information event management, SIEM). Предложенные авторами варианты парсинга событий СЗИ являются позволяют автоматизировать передачу между средствами защиты признаков, на основе которых необходимо корректировать набор контрмер, применяемых к атакующим. И хотя в данном исследовании не затронуты напрямую вопросы кибербразведки, такой подход может быть применен для извлечения индикаторов компрометации из внутренних источников.

Работа [12] посвящена классификации типов разведданных с точки зрения технических аспектов. Рассмотрены вопросы обмена IoC и определены факторы, при наличии которых производитель исследователь, получивший IoC, может отказаться от тиражирования и распространения конкретных индикаторов. Особое внимание уделено соотношению объема распространяемых фидов и качества содержащихся в них индикаторов компрометации. Указанная статья дополняет упомянутые выше публикации в вопросах проблем качества данных TI оценки возможности их применения для защиты конкретных информационных и киберфизических систем. Сформулированы возможные ограничения при обмене IoC между различными платформами, включая различия форматов данных и сложности их преобразования. Исследование

В [13] представлены результаты исследования способов публикации и обнародования данных threat intelligence, по результатам которого предложена классификация факторов, препятствующего подобным процессам. Помимо операционных, организационных, экономических и политических также рассмотрены факторы, влияющие на релевантность IoC, риск нарушения конфиденциальности при их публикации и затраты на создание инфраструктуры для формирования собственных фидов.

Исследование [14] посвящено проблемам эффективности используемых источников данных для кибербразведки, в том числе метрик индикаторов компрометации. Авторы формулируют проблемы разметки индикаторов и отсутствие объективных моделей ранжирования, кроме того, в статье наглядно представлена проблема длительного распространения

индикаторов компрометации в подготовленном структурированном формате, что нередко приводит к большому числу успешных «лавинообразных» атак, хотя при этом в неструктурированном виде индикаторы распространяются по Интернет достаточно быстро. Это несоответствие вполне объяснимо тем, что количество компаний, которые генерируют собственные индикаторы все еще невелико, число производителей коммерческих фидов весьма ограничено, а цены на их услуги высоки.

Таким образом, проведенный обзор научных исследований в области киберразведки свидетельствует, что большинство изысканий затрагивает автоматизацию обнаружения IoC из внешних источников, ранжирования полученных индикаторов и контроля их жизненного цикла применительно к задачам обогащения средств защиты. При этом вопросы развития киберразведки внутри защищаемых систем и формирования собственных индикаторов компрометации остаются нерассмотренными. В то же время рынок коммерческих индикаторов компрометации невозможен без решения задач по их формированию на основе данных защищаемых объектов. Вышеуказанные исследования, в своей совокупности отражают факт, что при обнаружении в работе защищаемого объекта даже небольшого числа IoC, атрибуты которых хотя бы частично совпадают с индикаторами с высоким рейтингом, может потенциально свидетельствовать о присутствии следов сложной целенаправленной атаки и требовать немедленных мер по реагированию.

Именно это и обуславливает затрагиваемую в данной статье проблему отсутствия методического обеспечения в части механизмов формирования индикаторов компрометации на основе данных внутренних источников киберразведки.

Таблица 1

Виды внутренних источников получения индикаторов компрометации

Источник киберразведки	Системы	Описание
Журналы регистрации событий	Все системы	Активность пользователей и служб, ошибки в работе программного обеспечения и события аудита безопасности
Сетевые события	Межсетевые экраны, маршрутизаторы, коммутаторы	Регистрация сетевых соединений, уведомления о срабатывании правил ограничения доступа, успешные и неуспешные попытки аутентификации
Профили сетевого трафика	Коммутаторы, маршрутизаторы, активное сетевое оборудование	Уведомления о превышении показателей по нагрузке, SNMP-трапы, метаданные траффика
Уведомления от периметральных средств защиты	Системы обнаружения и предотвращения вторжений, межсетевые экраны различного уровня	Уведомления и события обнаружения аномалий
Уведомления средств антивирусной защиты и системы обнаружения вторжений уровня хоста	Средства управления антивирусной защитой и системы защиты конечных точек	Уведомления об обнаружении вредоносного ПО и аномального использования системных утилит
Сотрудники	Все системы	Сообщения от пользователей и администраторов об аномальной работе систем
Внутренние расследования	Все системы	Индикаторы и артефакты, собранные в результате внутренних расследований инцидентов

2. Формирование индикаторов компрометации внутри защищаемой инфраструктуры

Данные киберразведки могут быть получены в результате мониторинга журналов событий СЗИ, а также самих защищаемых систем. При использовании внутренних источников речь в основном идет об IoC, поскольку формирование техник и тактик злоумышленников в этом случае возможно лишь в результате расследования инцидентов, которые не были предотвращены имеющимися средствами.

2.1 Источники индикаторов компрометации

В [4] представлена классификация индикаторов по источникам их получения, в которой выделяются хостовые, сетевые и поведенческие индикаторы. Согласно ей, к поведенческим индикаторам относятся данные из систем контроля и управления доступом и видеонаблюдения, поэтому их формирование требует привлечения человеческих ресурсов и ручного анализа. Данный тип источников не рассматривается в рамках текущей статьи. Таким образом, в случае КФС рассмотрению подлежат две группы – хостовые и сетевые индикаторы компрометации. Детектирование сетевых IoC в большинстве случае не является однозначным свидетельством компрометации системы и требует дополнительных процедуры проверки, тогда как хостовые индикаторы намного чаще сигнализируют об успешности атаки [15].

Ключевыми источниками данных внутри инфраструктуры являются СЗИ, защищающие периметр сети, средства контроля доступа между внутренними сегментами и хостовые средства защиты. Другие типы средств защиты тоже могут быть источниками данных киберразведки, но скорее для процессов обогащения обнаруженных индикаторов контекстом. При этом наблюдение таких событий во времени позволяет накапливать статистику и определять шаблоны штатной работы системы, чтобы в последствии выявлять инциденты на основе обнаруженных отклонений в поведении объектов. В таблице 1 представлены виды внутренних источников индикаторов компрометации.

Полученные в рамках одного оповещения об угрозе индикаторы целесообразно объединить в одну группу. Это позволит облегчить определение тип атаки, а также проверить потенциально скомпрометированную систему на предмет наличия других IoC.

При автоматизированном извлечении часто встречаются индикаторы, которые не позволяют однозначно говорить о компрометации системы. Например, IP адреса крупных хостинговых сервисов, хэш-суммы легитимных файлов и т.д. Для снижения количества ошибок первого рода необходимо предусмотреть механизм управления исключениями. Кроме того, при формировании собственного набора индикаторов на основе внутренних источников целесообразно устанавливать время жизни индикатора (time to live, TTL) [5, 16] больше, чем для IoC от внешних источников. В первую очередь, это актуально для хэш-сумм файлов. Эксплуатация систем часто подразумевает присоединение сегментов из смежных инфраструктур, и если в подключенном сегменте уже имелись следы присутствия злоумышленников, то увеличенное TTL позволит их обнаружить.

2.2 Методы извлечения индикаторов компрометации

Основными методами извлечения индикаторов компрометации из внутренних источников являются ручной анализ событий, трафика или его метаданных, а также автоматизированное извлечение из инцидентов. При этом автоматизированное извлечение возможно, как на стороне СЗИ, так и в системах, агрегирующих журналы событий, например, SIEM-системы. Также возможен подход, когда средства защиты генерируют индикаторы и направляют их в TI-платформу либо распространяют на другие СЗИ.

Ручной анализ. В первую очередь этот подход подразумевает работу аналитиков в консолях различных СЗИ. Суть подхода заключается в ручном выявлении аномалий, формировании и проверке гипотез и в случае их подтверждения формирования индикаторов в ходе реагирования на инцидент, а также формирование IoC, полученных в ходе расследования инцидентов.

Применение метода зачастую нецелесообразно выделять в отдельный процесс из-за высокого уровня трудозатрат. На практике такой подход активно используется в виде дополнительного этапа постинцидент анализа: IoC формируются после детального разбора инцидента и направляются в СЗИ для недопущения таких инцидентов. С одной стороны, индикаторы, полученные таким методом, имеют более высокий уровень достоверности, поскольку уже проведен тщательный анализ и криминалистические исследования. С другой стороны, указанные выше процессы занимают длительное время, IoC будут сформированы недостаточно оперативно, что может негативно сказаться на вероятности повторения подобных инцидентов. Также характерно использование широкого набора утилит и инструментов, перечень которых зависит от экспертов, проводящих исследование. Это

Таблица 2

Источники артефактов и инструменты извлечения хостовых IoC

Тип	Источник артефактов	Инструмент
Журналы удаленных подключений	C:\Windows\System32\winevt\Logs\Security.evtx	Windows Event Viewer Event Log Explorer
	C:\Windows\System32\winevt\Logs\Microsoft-Windows RemoteDesktopServicesRdpCoreTS%4Operational.evtx	
Аудит доступа к файлам	NTUSER.DAT|Software\Microsoft\Windows\ CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU	Registry Exlporer RegRipper
	C:\Users\%USERPROFILE%\AppData\Roaming\ Microsoft\ Windows\Recent\AutomaticDestinations	JLECMD.exe
Журналы браузеров	C:\Users\%USERNAME%\AppData\Local\ Microsoft\Edge\ User Data\Default\History	BrowsingHistoryView DB Browser for SQLite
	C:\Users\%USERPROFILE%\AppData\Roaming\ Mozilla\Firefo x\Profiles*.default*\places.sqlite	
Журналы запуска ПО	C:\Windows\Prefetch	PECMD.exe
Журналы доступа к USB	C:\Windows\appcompat\Programs\Amcache.hve	USB Detective
	C:\%USERPROFILE%\NTUSER.DAT	

может быть ПО для анализа реестра операционных систем, дампов трафика и оперативной памяти, а также извлечения данных журналов файловой системы, журналов интернет-браузеров и т.д. В таблице 2 представлены примеры источников артефактов и инструментов для извлечения из них хостовых индикаторов компрометации.

Автоматизированное извлечение. Поскольку объемы данных, генерируемых средствами защиты современных систем значительны, то извлечение индикаторов компрометации из них целесообразно автоматизировать. Кроме того, при наличии TI-платформы [6, 17] возможна реализация различных алгоритмов обработки таких IoC и использование их для автоматизированного обогащения средств защиты.

1. Извлечение индикаторов напрямую из СЗИ.

Современные СЗИ при срабатывании защитных механизмов делают записи в журналах событий, которые могут храниться, как на защищаемых объектах, так и в централизованном хранилище. При этом в большинстве СЗИ присутствует возможность удаленных запросов через API [18], которые позволяют получать в ответ искомые индикаторы. Например, данные о вредоносном объекте, полученные в результате эмуляции его работы в системе поведенческого анализа:

«file_info»: {
«file_uri»: «sha256:215a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f»,
«md5»: «44d88612fea8a7f36de82e1278abb02f»,
«mime_type»: «text/plain; charset=us-ascii»,
«sha1»: «3395856ce81f1b7382dee72602f798b642f14140»,
«sha256»: «275a021bbfb5489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f»,
«size»: 69
},

Стоит отметить, что распространенным является подход, при котором сбор IoC осуществляется с нескольких СЗИ в единое хранилище (например, TI-платформу) для последующей обработки.

2. Извлечение индикаторов компрометации из SIEM

При наличии в инфраструктуре SIEM-системы ее возможности часто используются для формирования собственных индикаторов компрометации. В SIEM агрегируются события со всей инфраструктуры, включая журналы аудита защищаемых объектов и СЗИ. При срабатывании правил корреляции часть данных из нормализованных событий записывается в отдель-

ные структуры (например, табличные списки), а потом доступна к извлечению посредством API-запросов или выгрузки в другие системы.

Если ведение подобных списков оказывается ресурозатратным (например, поток событий слишком большой, а извлекающие их правила корреляции используются не для реагирования, а только для получения набора IoC), применяется метод, когда к SIEM периодически выполняется внешний запрос на поиск событий за определенный период времени, в условиях которого задан возврат наиболее часто встречающихся индикаторов (например, 20 самых часто блокируемых URL за последние 24 часа). Формирование и отправка индикаторов компрометации непосредственно СЗИ и их распространение.

Некоторые СЗИ способны самостоятельно направлять данные в другие средства защиты или публиковать их на общих ресурсах для последующего использования другими СЗИ. Например, во многих межсетевых экранах для веб-приложений (Web Application Firewall, WAF) [19] есть функционал выгрузки списка наиболее часто атакующих IP-адресов. Например, Positive Technologies Application Firewall при API-запросе вида

GET https://waf.local/api/ptaf/v4/config/global_lists/045af7b7 -bc30-4a50-97ae-ea914eb06039/file

возвращает файл подобного содержания:

HTTP/1.1 200 OK

Content-Type: text/plain

Content-Disposition: attachment; filename=»DDoS list.txt»

Content-Encoding: gzip

198.51.100.1

198.51.100.5

198.51.100.238

Такой список может быть размещен на сетевом ресурсе для последующего импорта в средства защиты от DDoS-атак [20] на уровне L3-L4 модели OSI [15, 21] или передаваться на оборудование провайдеров для полной блокировки любого трафика с таких источников.

3. Алгоритмы применения индикаторов от внутренних источников

В зависимости от выбранного метода формирования собственного фида на основе индикаторов компрометации от внутренних источников возможно построение различных алгоритмов их применения. Предположим, что в составе средств защиты имеется система, обеспечивающая возможность агрегации и ранжирования индикаторов компрометации на основе некоторых правил и методов threat intelligence [5, 22].

3.1 Использование индикаторов непосредственно от источников

В случае извлечения IoC напрямую от средств защиты, каждое СЗИ выступает отдельным источником и к поступившим от него данным применяются вышеуказанные правила и методы. Если TI-платформа допускает применение различных правил агрегации и ранжирования для нескольких групп источников, то в случае наличия внешних потоков данных об угрозах и внутренних индикаторов их целесообразно разделить. Таким образом, собирая данные с нескольких СЗИ внутри защищаемого объекта можно сформировать

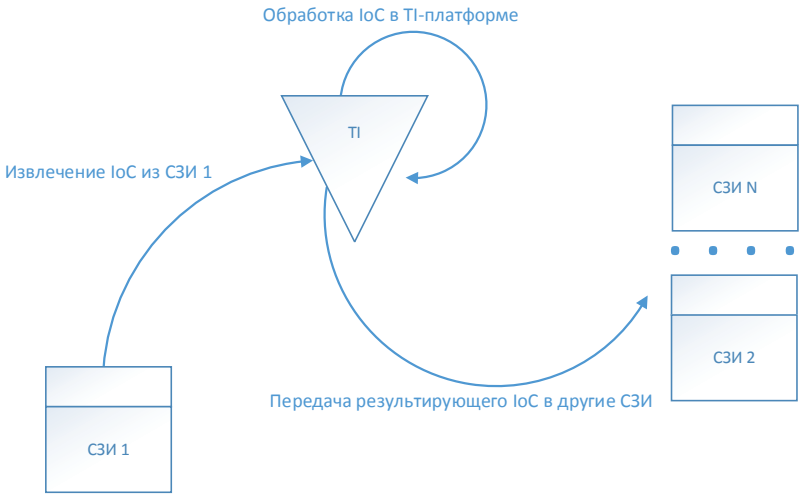

Рис. 1. Схема потоков данных при использовании IoC непосредственно от источников

собственный набор индикаторов для дальнейшего применения (кастомный фид).

Полученный фид может быть направлен в конкретные СЗИ для принятия превентивных мер, автоматизированного реагирования и предотвращения возможных инцидентов. Например, предположим, что в системе используется несколько антивирусных решений – в зависимости от защищаемых контуров. С одного из них получены данные о множественных попытках подключения к вредоносному сайту. Полученные данные направлены и обработаны в TI-платформе. Сформированный на их основе фид направлен в корпоративный прокси-сервер для блокировки обнаруженного URL. Это позволит обеспечить превентивную меру реагирования и исключит возможность подключения к данному ресурсу с хостов, где по какой-то причине еще не обновились базы антивирусов. Схема потоков данных для данного примера представлена на рис. 1, а блок-схема алгоритма применения метода представлена на рис. 4а.

3.2 Извлечение индикаторов через нормализацию событий

Если TI платформа поддерживает возможность приема событий из SIEM, то на основе фильтров часть данных дублируется и отправляется для анализа в TI. В этом случае извлечение индикаторов полностью производится на стороне системы, агрегирующей IoC. Это позволяет снизить нагрузку на SIEM и тратить ресурсы коррелятора на непрофильную задачу, особенно если события, из которых извлекаются данные, не участвуют в правилах детектирования угроз. В то же время возникает необходимость дублировать данные между двумя системами и при больших потоках данных существенно нагружать сетевое оборудование. Дублирование может быть частично исключено, если на стороне SIEM существует возможность управлять очередями событий и реализовать отправку в TI их усеченной копии, в которой точно будут содержаться IoC. После обработки полученных из SIEM событий TI извлекает IoC и также обеспечивает формирование собственного фида. Этот фид может быть направлен напрямую в СЗИ, как в случае с получением IoC от СЗИ. Также фид может быть использован вместе со внешними потоками данных и включен в механизм ранжирования. При этом целесообразно повысить значение параметра, отвечающего за уровень опасности индикатора, поскольку он уже получен от внутренних источников и на защищаемом объекте имеются следы взаимодействия с ним.

Затем набор таких индикаторов может быть направлен в СЗИ для принятия мер по блокировке и при этом обратно в SIEM для обновления табличных списков и использования в правилах корреляции. Такой подход позволяет оставить за SIEM-системой механизм выявления инцидентов на основе IoC, но при этом снизить нагрузку на подсистему корреляции за счет проверки и ранжирования индикаторов в другой системе. Схема потоков данных для данного варианта представлена на рис. 2, а блок-схема алгоритма применения метода представлен на рис. 4б.

Рис. 2. Схема потоков данных при извлечении IoC через нормализацию событий в SIEM

3.3 Применение корреляции для обработки индикаторов

Если же в TI платформе нет механизма получения событий из SIEM, используется подход, основанный на извлечении индикаторов с помощью коррелятора. В случае срабатывания правил корреляции реализуется обновление динамических или табличных списков, куда помещаются уже извлеченные IoC. Эти списки передаются в TI платформу, где происходит их агрегация и ранжирование. При таком подходе основным инструментом извлечения IoC остается SIEM, но при этом работа в части агрегации, ранжирования и отправки индикаторов в СЗИ происходит на стороне TI. Схема потоков данных такого решения представлена на рис.3, а блок-схема алгоритма применения метода на рис. 4в.

3.4 Интеграция средств защиты через собственные наборы индикаторов

Поскольку многие средства защиты имеют собственные механизмы формирования индикаторов и могут быть интегрированы с другими СЗИ, то нередко формирование собственного фида осуществляется этими средствами. Например, системы поведенческого анализа («песочницы») зачастую обеспечивают возможность повторных проверок – при обновлении базы знаний в выборочном порядке производится анализ объектов, проверенных ранее. В случае выявления фактов, что вредоносный объект был пропущен, «песочница» формирует набор IoC, например, хеш-суммы файлов. Этот набор может быть передан через API в систему защиты конечных точек (Endpoint Detection and Response, EDR) [15] для автоматического поиска и блокировки таких файлов на всех хостах в сети. Поскольку данный метод предполагает точечные интеграции между средствами защиты, которые могут быть выполнены с использованием различных механизмов, то типового алгоритма в этом случае не существует. Наборы интеграций и механизмы реализации уникальны для каждого объекта.

В то же время для случаев, перечисленных в пунктах 3.1 – 3.3, в результате исследований авторами были выделены основные этапы и разработаны алгоритмы применения индикаторов компрометации для обогащения СЗИ (рисунок 4).

4. Сценарии применения индикаторов компрометации для защиты киберфизических систем

Сценарий 1. В одном из сетевых СЗИ, например, системе класса IDS [23] или NTA [23], обнаружена подозрительная сетевая активность. В качестве IoC в большинстве подобных случаев будут выступать IP-адреса источника или назначения. Эти индикаторы необходимо передать в TI платформу для обработки и дальнейшего принятия решения. Если передача IoC происходит через SIEM, то они могут быть обогащены контекстом (поиск хоста, с которого идет вредоносный трафик, затем идентификация процесса, связанного с этим сетевым соединением). На стороне TI происходит обработка индикаторов – ранжирование с другими потоками данных об угрозах, определение критичности и времени жизни.

Сценарий 2. В одном из средств защиты на хосте (антивирусное ПО или EDR агент [4, 22]) быстрее обновились базы и была зафиксирована потенциальная

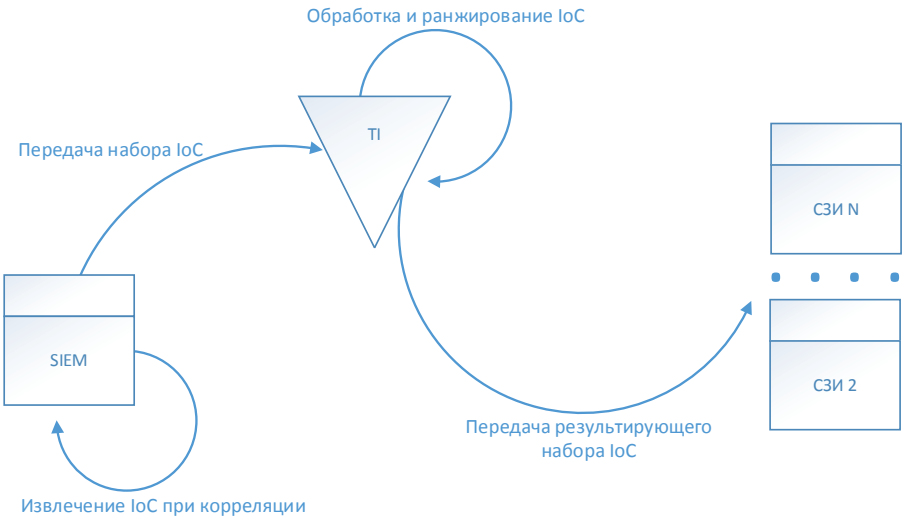

Рис. 3. Схема потоков данных при извлечении IoC через корреляцию в SIEM

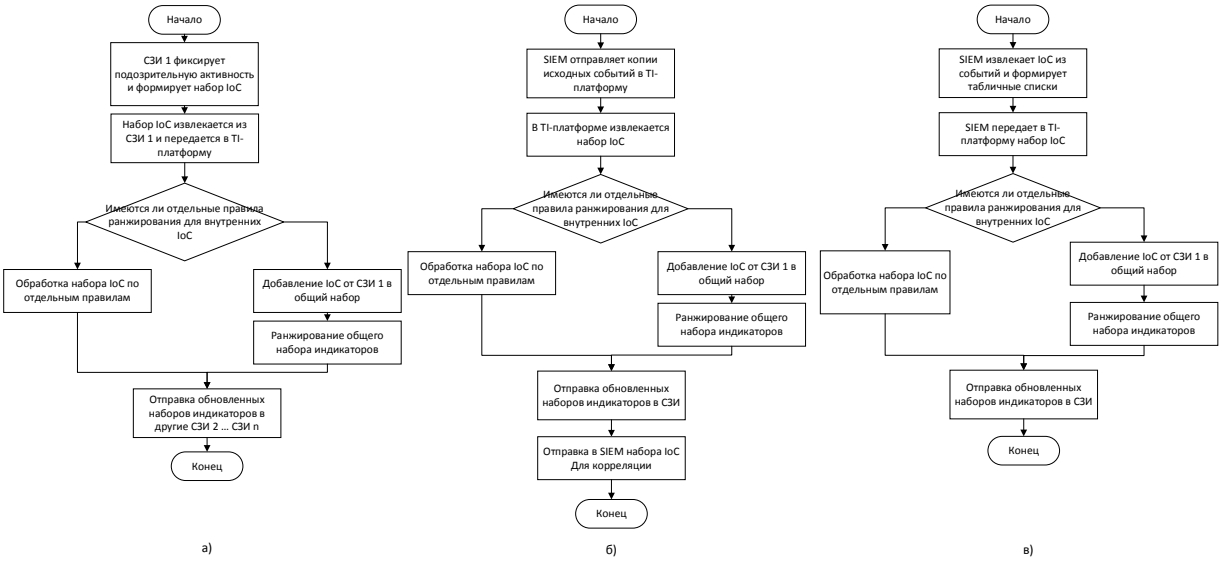

Рис. 4. Алгоритмы применения индикаторов от внутренних источников

вредоносная активность, события об этом направлены в SIEM. Далее в зависимости от алгоритма и механизма интеграции в TI платформу направляются данные события или извлеченные из них индикаторы. В зависимости от реализации данного алгоритма дублирование может быть исключено частично, если на стороне SIEM существует возможность управлять очередями событий и реализовать отправку в TI их усеченной копии, в которой будут содержаться IoC. В этой платформе они проходят обработку в рамках обновленного собственного фида распространяются на все другие хосты. Кроме того, полученные и обогащенные индикаторы направляются обратно в SIEM для использования в правилах корреляции. Подобный сценарий позволяет реализовать прообраз самообучения системы защиты – СЗИ выявляют угрозы на конечных хостах, эти данные обогащаются через TI и автоматически добавляются в условия правил корреляции в случае высокого скоринга по результатам ранжирования с другими потоками данных.

Сценарий 3. Рассмотрим случаи применения индикаторов от внутренних источников без применения TI платформ. Например, часть сервисов КФС доступна через веб-интерфейс и защищена WAF. Помимо этого, на периметре сети расположен межсетевой экран класса NGFW [20] с функциями IDS и IPS. Предположим, что WAF обнаруживает признаки DDoS-атаки на уровне L7 и начинает блокировать запросы с наиболее активных адресов атакующих. В случае наличия у злоумышленников значительных мощностей для проведения атаки нагрузка как WAF, так и защищаемое приложение может стремительно возрасти до критического уровня. Здесь целесообразным является подключение механизма IPS и сброс пакетов от наиболее активных атакующих. WAF формирует списки IP-адресов атакующих, которые перенаправляются в периметровый NGFW, например через запросы к API или выгрузку на общий ресурс текстового файла. При этом возможно создание нескольких типов списков с различным временем жизни индикатора (TTL). Это необходимо, чтобы обеспечить возможность снижения количества ошибок первого рода и блокировки легитимных пользователей.

Сценарий 4. Данный сценарий относится не столько к извлечению IoC из внутренних источников, сколько к дополнительной обработке данных, поступающих с них, с целью проверки взаимосвязей с индикаторами из внешних источников. Большинство целенаправленных атак осуществляются без использования вредоносного ПО и активных действий по сканированию сети или передачи большого объема данных. Поэтому зачастую СЗИ не позволяют определить является ли запуск задачи или создание сервиса легитимным.

Для решения этой задачи часто используют SIEM, создавая правила корреляции на определенные последовательности событий или значения конкретных параметров. Такие «пакеты правил» сложно поддаются оперативной корректировки, особенно в части детектирования новых техник и тактик злоумышленников. При наличии внешних источников IoC актуальным является следующий сценарий. С помощью SIEM агрегируются события с внутренних источников, из них извлекаются данные о параметрах запуска процессов, создания сервисов и других легитимных дей-

Таблица 3

Примеры собираемых данных от внутренних источников

Тип индикатора	Наблюдаемое значение из событий	Индекс источника
windows_path	.\powershell	32
url	http://c2cdomain/malicious-picrure-1.jpg’	39
windows_path	.\pOWErS^H^EIL^.eX^e^	41
md5_hash	81ed03caf6901e444c72ac67d192fb9c	54
url	http://evilserver/pwnme»	46
windows_path	.\reg query add mscfile\\\\open	59
windows_path	\system\CurrentControlSet\Control\Terminal	63
ipv4	1.2.3.4	79
ipv4	127.0.0.1	114

ствиях. Это данные передаются в TI платформу, где сверяются с регулярно обновляемыми внешними потоками данных об угрозах. При этом сравнение происходит на основе полей, относящихся к контекстной составляющей индикаторов. В случае обнаружения совпадений данные о хостах, где зафиксирована такая активность, возвращаются в SIEM в виде обновляемых табличных списков. Эти списки используются для правил корреляции и накопления статистики, глубину которой можно регулировать временем жизни таких списков.

Таким образом, на защищаемых хостах фиксируется определенный набор легитимных действий (пример событий с извлеченными данными представлен в таблице 3). Эти события проверяются на основе внешних IoC и в случаях совпадения объекты, где зафиксирована активность, ставятся на усиленный контроль. При срабатывании других правил корреляции с такими хостами повышается приоритет инцидентов, кроме того обеспечивается возможность построения длительных цепочек событий и обнаружения целенаправленных атак.

5. Анализ источников данных киберразведки

Получение индикаторов компрометации из внутренних источников в большинстве случаев относится к проприеритарным технологиями, что обуславливает характерную особенность такого вида источников – отсутствие какой-либо типизации при определении контекста. В одних случаях дополнительную информацию можно извлечь из специальных полей события, в других требуется дополнительно обогащать данные из справочников или анализировать запросы внутри сессий, а в некоторых случаях контекст отсутствует. Кроме того, во многих источниках имеются схожие базы знаний и извлеченные индикаторы многократно дублируются. Особенно это характерно для IP-адресов, dns-записей и URL. Например, попытки подключения к вредоносному веб-ресурсу могут зафиксироваться в событиях прокси-сервера, антивируса, периметрального NGFW и т.д. При этом часть извлеченных IoC будет дублирована и подлежит обработке и ранжированию.

В части определения контекста наиболее часто наблюдались проблемы при извлечении URL. В большинстве внутренних источников отсутствует какая-либо подробная информация и детальное описание. Изредка в событиях блокировки доступа к таким ресурсам отмечается принадлежность к некоторой категории согласно классификации вендора данного СЗИ. На практике это является одним из ограничивающих факторов применения таких данных для киберразведки. В то же время некоторые поставщики IoC предоставляют достаточно полное описание контекста подобным индикаторам. Поэтому в большинстве случаев обработка контекста индикаторов компрометации внутренних источников требует ручного процесса для преобразования данных в машиночитаемый формат или автоматизации ранжирования и обогащения с потоками данных от внешних источников. Тем не менее эти данные не могут быть полностью игнорированы как источник информации о киберразведке, поскольку именно в них может содержаться ценная информация для выявления и реагирования на инцидент.

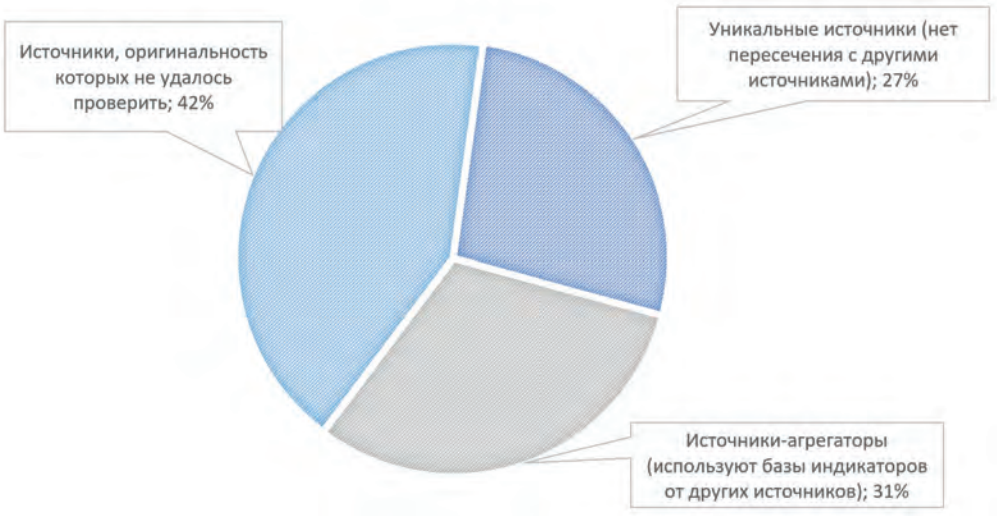

Рис. 5. Анализ оригинальности индикаторов в внутренних источниках TI

Анализ исследуемых внутренних TI-источников выявил, что многие из них являются ретрансляторами данных, получаемых из внешних потоков данных об угрозах. Это обусловлено тем, что многие производители СЗИ используют внешние обновляемые базы знаний, что часто приводит к дублированию информации. В большей степени это относится к источникам, поставляющим IoC в более сложных форматах. На рис. 5 представлены результаты анализа исследуемых источников на предмет оригинальности. Следует отметить, что в некоторых случаях реализовать достоверную проверку на предмет оригинальности было невозможно из-за преобразования информации при ее ретрансляции.

Было обнаружено, что при агрегации и ретрансляции индикаторов некоторые данные могут быть потеряны или изменены. В основном, это связано с ошибками форматирования данных, искажением дат обнаружения, дублированием или агрегацией нескольких индикаторов. Подобные трансформации существенно снижают качество данных кибербразведки и повышают вероятность ошибок первого рода при работе с ними.

Заключение

Обеспечение надлежащего уровня защищенности является одной из ключевых задач при эксплуатации информационных и киберфизических систем, в том числе относящихся к категории критической инфраструктуры. При этом одним из трендов в решении этой задачи является развитие методов кибербразведки и оркестрации работы множества средств защиты. Стремительно развиваются направления проактивного поиска угроз и опережения действий злоумышленников с использованием методов кибербразведки, среди которых наиболее распространено применение индикаторов компрометации для обогащения средств защиты киберфизических систем. Их использование позволяет проводить действия, направленные на выявление новых, ранее неизвестных угроз и обеспечивать защиту подобных объектов на качественно новом уровне, оперируя тактиками и процедурами и предугадывая действия злоумышленников.

В настоящей статье рассмотрены и структурированы задачи поиска и извлечения данных из внутренних источников для обогащения систем кибербразведки и выявления целенаправленных методов атак на основе применения собственных наборов индикаторов компрометации и предложены методы их решения. Установлено, что в отрасли кибербразведки отсутствует унификация в части формирования индикаторов компрометации на основе данных защищаемых систем и дальнейшего обмена информацией между различными средствами защиты, но при этом имеют место ряд доминирующих форматов обмена подобными данными. Разработано алгоритмическое обеспечение применения индикаторов от внутренних источников и предложены базовые сценарии обработки таких данных для защиты киберфизических систем в условиях изменяемых векторов атак. Кроме того, при работе с внутренними источниками кибербразведки в рамках данного исследования был выявлен ряд проблем эффективной обработки таких данных, поскольку решение каждой из них обуславливает несколько отдельных задач, их рассмотрение будет проведено и представлено на дальнейших этапах исследования.

Работа выполнена при финансовой поддержке гранта РНФ № 22-21-00846.

Литература

1. Abu M.S.; Selamat S.R., Ariffin A., Yusof R. Cyber Threat Intelligence – Issue and Challenges. Indones // Indonesian Journal of Electrical Engineering and Computer Science. – 2018. Vol. 10, no. 1. – P. 371–379.
2. Sauerwein C., Pekaric I., Felderer M., Breu R. An analysis and classification of public information security data sources used in research and practice // Computers & Security. – 2019. – Vol. 82. – P. 140-155.
3. Pala A., Zhuang J. Information sharing in cybersecurity: A review // Decision Analysis. – 2019. – Vol. 16, no. 3. – P. 172-196.
4. 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: 10.21681/2311-3456-2022-5-82-89
5. Sauerwein C., Sillaber C., Mussmann A., Breu R. Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives // Wirtschaftsinformatik und Angewandte Informatik. – 2017. – P. 837-851.
6. Zrahia A. Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views // Journal of Cybersecurity. – 2018. – Vol. 4, issue 1. – P. 1–16.
7. Caballero J., Gomez G., Matic S., Sanchez G., Sebastian S., Villacanas A. The Rise of GoodFATR: A Novel Accuracy Comparison Methodology for Indicator Extraction Tools // Future Generation Computer Systems. – 2023. – Vol. 144. – P. 74-89.
8. Alam M., Bhusal D., Park Y., Rastogi N. Looking Beyond IoCs: Automatically Extracting Attack Patterns from External [Электронный ресурс]. – 2022. –URL: https://arxiv.org/abs/2211.01753 (дата обращения 19.09.2023).
9. Allegretta M., Siracusano G., Gonzalez R., Gramaglia M. Are crowd-sourced CTI datasets ready for supporting anti-cybercrime intelligence? // Computer Networks. – 2023. – Vol. 234. – P. 109920.
10. Liu R., Zhao Z., Sun C., Yang X., Gong X., Zhang J. A Research and Analysis Method of Open Source Threat Intelligence Data // Communications in Computer and Information Science (CCIS). – 2017. – Vol. 727. – P. 352–363.
11. Тергеуов О.С., Маликова Ф.У. Обнаружение и устранение DDoS-атаки IoT-ботнетов на основе SIEM // Universum: технические науки. – 2022. – №4-1 (97). – С. 54-63.
12. Tounsi W., Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks // Computer Security. – 2018. – Vol. 72. – P. 212–233.
13. Zibak A., Simpson A. Cyber threat information sharing: Perceived benefits and barriers // Proceedings of the 14th International Conference on Availability, Reliability and Security. – Canterbury, UK, 26–29 August 2019. – P. 1–9.
14. Guo Li V., Dunn M., Pearce P., McCoy D., Voelker G., Savage S, Levchenko K. Reading the tea leaves: a comparative analysis of threat intelligence // Proceedings of the 28th USENIX Conference on Security Symposium (SEC'19). – Santa Clara, USA, 14-16 August 2019. – P. 851-867.
15. Schaberreiter T., Kupfersberger V., Rantos K., Spyros A., Papanikolaou A., Ilioudis C., Quirchmayr G. A quantitative evaluation of trust in the quality of cyber threat intelligence sources // Proceedings of the 14th International Conference on Availability, Reliability and Security. – 2019. – P. 1-10.
16. Brown S., Gommers J., Serrano O. From Cyber Security Information Sharing to Threat Management // Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. – Denver, CO, USA, 12–16 October 2015. – P. 43–49.
17. Wagner C., Dulaunoy A., Wagener G., Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform // Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. – Vienna, Austria, 24 October 2016. – P. 49-56.
18. Wei Y., Bo L., Sun X., Li B., Zhang T., Tao C. Automated event extraction of CVE descriptions // Information and Software Technology. – 2023. – Vol. 158. – P. 107178.
19. Calva M., Beltran M. A Model for risk-Based adaptive security controls // Computers & Security. – 2022. – Vol. 115. – P. 102612.
20. Skopik F. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at National Level. – CRC Press: Boca Raton, FL, USA, 2018. – 446 p.
21. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. – 2016. – Vol. 50. – P. 673-681.
22. Bryant B., Saiedian H. Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model // Computers & Security. – 2020. – Vol. 94. – P. 101817.
23. Mavroeidis V., Bromander S. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence // Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC). – Athens, Greece: IEEE, 2017. – P. 91–98.

RESEARCH OF METHODS FOR FORMING INDICATORS OF COMPROMETATION FROM INTERNAL SOURCES OF INFORMATION AND CYBERPHYSICAL SYSTEMS

Meshcheryakov R.V.[3], Iskhakov S.Yu.[4]

Purpose of work: *research of methods for generating indicators of compromise within the infrastructure for use in systems for protecting information and cyber-physical systems.*

Research method: *system analysis of open sources of data on indicators of compromise, methods of extracting them and methods of application when organizing cyber reconnaissance within the protected infrastructure.*

The result obtained: current problems of extracting indicators of compromise from internal sources in information and cyber-physical systems are formulated. Algorithmic support for the use of such indicators in cyber intelligence processes is proposed. Basic scenarios for using indicators of compromise from internal sources when processing dynamic streams of threat data in the context of changing attack vectors are formulated.

It was found that the cyberintelligence industry currently lacks unification in terms of forming compromise indicators based on data from protected systems and further exchange of information between different defenses, but there are a number of dominant formats for the exchange of such data. In the course of the research, the tasks of searching and extracting data from internal sources to enrich cyberintelligence systems and identify targeted attack methods based on the use of proprietary sets of compromise indicators are considered and structured, and methods for their solution are proposed.

Scientific novelty: *methods for generating indicators of compromise within the protected infrastructure have been reviewed and systematized. Algorithmic support for the use of indicators from internal sources has been developed and basic scenarios for processing such data have been proposed to protect cyber-physical systems in the face of variable attack vectors.*

Keywords: *indicator of compromise, cyber-intelligence, context, cyber-physical system, security information event management, enrichment, ranking.*

References

1. Abu M.S.; Selamat S.R., Ariffin A., Yusof R. Cyber Threat Intelligence – Issue and Challenges. Indones // Indonesian Journal of Electrical Engineering and Computer Science. – 2018. Vol. 10, no. 1. – P. 371–379.
2. Sauerwein C., Pekaric I., Felderer M., Breu R. An analysis and classification of public information security data sources used in research and practice // Computers & Security. – 2019. – Vol. 82. – P. 140-155.
3. Pala A., Zhuang J. Information sharing in cybersecurity: A review // Decision Analysis. – 2019. – Vol. 16, no. 3. – P. 172-196.
4. Meshherjakov R.V., Ishakov S.Ju. Issledovanie indikatorov kompрometacii dlja sredstv zashhity informacionnyh i kiberfizicheskih sistem // Voprosy kiberbezopasnosti. – 2022. – № 5 (51). – S. 82-99. DOI: 10.21681/2311-3456-2022-5-82-89
5. Sauerwein C., Sillaber C., Mussmann A., Breu R. Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives // Wirtschaftsinformatik und Angewandte Informatik. – 2017. – P. 837-851.
6. Zrahia A. Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views // Journal of Cybersecurity. – 2018. – Vol. 4, issue 1. – P. 1–16.
7. Caballero J., Gomez G., Matic S., Sanchez G., Sebastian S., Villacanas A. The Rise of GoodFATR: A Novel Accuracy Comparison Methodology for Indicator Extraction Tools // Future Generation Computer Systems. – 2023. – Vol. 144. – P. 74-89.
8. Alam M., Bhusal D., Park Y., Rastogi N. Looking Beyond IoCs: Automatically Extracting Attack Patterns from External [Jelektronnyj resurs]. – 2022. –URL: https://arxiv.org/abs/2211.01753 (data obrashhenija 19.09.2023).
9. Allegretta M., Siracusano G., Gonzalez R., Gramaglia M. Are crowd-sourced CTI datasets ready for supporting anti-cybercrime intelligence? // Computer Networks. – 2023. – Vol. 234. – P. 109920.
10. Liu R., Zhao Z., Sun C., Yang X., Gong X., Zhang J. A Research and Analysis Method of Open Source Threat Intelligence Data // Communications in Computer and Information Science (CCIS). – 2017. – Vol. 727. – P. 352–363.

3 Roman V. Meshcheryakov, Dr. Sc. (Technology), Professor, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: mrv@ieee.org, ORCID: ORCID: 0000-0002-1129-8434.

4 Sergey Yu. Iskhakov, Ph.D. (Technology), Promsvyazbank, Moscow, Russia. E-mail: sergey@iskhakov.ru, ORCID: 0000-0003-3346-9262.

11. Tergeuov O.S., Malikova F.U. Obnaruzhenie i ustranenie DDoS-ataki IoT-botnetov na osnove SIEM // Universum: tehnicheskie nauki. – 2022. – №4-1 (97). – S. 54-63.
12. Tounsi W., Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks // Computer Security. – 2018. – Vol. 72. – P. 212–233.
13. Zibak A., Simpson A. Cyber threat information sharing: Perceived benefits and barriers // Proceedings of the 14th International Conference on Availability, Reliability and Security. – Canterbury, UK, 26–29 August 2019. – P. 1–9.
14. Guo Li V., Dunn M., Pearce P., McCoy D., Voelker G., Savage S, Levchenko K. Reading the tea leaves: a comparative analysis of threat intelligence // Proceedings of the 28th USENIX Conference on Security Symposium (SEC'19). – Santa Clara, USA, 14-16 August 2019. – P. 851-867.
15. Schaberreiter T., Kupfersberger V., Rantos K., Spyros A., Papanikolaou A., Ilioudis C., Quirchmayr G. A quantitative evaluation of trust in the quality of cyber threat intelligence sources // Proceedings of the 14th International Conference on Availability, Reliability and Security. – 2019. – P. 1-10.
16. Brown S., Gommers J., Serrano O. From Cyber Security Information Sharing to Threat Management // Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. – Denver, CO, USA, 12–16 October 2015. – P. 43–49.
17. Wagner C., Dulaunoy A., Wagener G., Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform // Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. – Vienna, Austria, 24 October 2016. – P. 49-56.
18. Wei Y., Bo L., Sun X., Li B., Zhang T., Tao C. Automated event extraction of CVE descriptions // Information and Software Technology. – 2023. – Vol. 158. – P. 107178.
19. Calva M., Beltran M. A Model for risk-Based adaptive security controls // Computers & Security. – 2022. – Vol. 115. – P. 102612.
20. Skopik F. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at National Level. – CRC Press: Boca Raton, FL, USA, 2018. – 446 p.
21. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. – 2016. – Vol. 50. – P. 673-681.
22. Bryant B., Saiedian H. Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model // Computers & Security. – 2020. – Vol. 94. – P. 101817.
23. Mavroeidis V., Bromander S. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence // Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC). – Athens, Greece: IEEE, 2017. – P. 91–98.

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ НА ОСНОВЕ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ: АРХИТЕКТУРА СИСТЕМЫ И ЭКСПЕРИМЕНТЫ

Новикова Е.С.[1], Котенко И.В.[2], Мелешко А.В.[3], Израилов К.Е.[4]

Цель исследования: *разработка подхода к построению системы обнаружения вторжений на основе федеративного машинного обучения.*

Полученный результат: *разработана концепция и архитектура системы обнаружения вторжений на основе федеративного машинного обучения. Предложенная архитектура включает новые компоненты, отвечающие за организацию федеративного обучения, такие как компоненты выбора данных, обучения локальной модели, оценки рисков конфиденциальной информации, выявления атак на федеративное обучение, а также определяет их связи с другими функциональным элементами системы. Для выполнения экспериментальной оценки компонентов системы обнаружения вторжений на основе федеративного обучения сформулированы метрики оценки их эффективности, которые позволяют оценить в том числе требования к вычислительным ресурсам системы. Предложен подход к моделированию распределения данных между взаимодействующими компонентами, и получены экспериментальные оценки эффективности обнаружения вторжений с помощью моделей машинного обучения, обученных в федеративном режиме.*

Научная новизна: *анализ литературы показал, что применение федеративного обучения для построения систем обнаружения вторжений связано с рядом открытых практических задач; в частности, отсутствует общая методология построения и оценки эффективности таких систем. В настоящей работе предлагается архитектура системы обнаружения вторжений, которая учитывает практические особенности использования федеративного обучения, а также представляются результаты экспериментальной оценки эффективности применения моделей обнаружения вторжений, обученных в федеративном режиме.*

Вклад: *Новикова Е. С. и Котенко И. В. — общая концепция построения и архитектура системы обнаружения вторжения с использованием федеративного машинного обучения, методология сбора данных для исследования безопасности киберфизических систем; Новикова Е. С. и Израилов К. Е. — проработка функциональности отдельных компоненты системы обнаружения вторжения, Мелешко А. В. — проведение экспериментов.*

Ключевые слова: *кибербезопасность, киберфизические системы, выявление аномалий и кибератак, распределенное машинное обучение, сверточная нейронная сеть, оценка эффективности.*

DOI: 10.21681/2311-3456-2023-6-50-66

Введение

В настоящее время предложены разнообразные подходы к обнаружению вторжений и аномалий в компьютерных сетях [1-3]. В их основе лежат методы на основе сигнатурного анализа, статистического анализа временных рядов [4], а также алгоритмы на основе методов классического машинного обучения (МО) [5] и глубокого обучения [6-7]. На практике наибольшее распространение получили методы на осно-

1 Новикова Евгения Сергеевна, кандидат технических наук, доцент, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. ORCID: 0000-0003-2923-4954. Scopus Author ID: 55415626100. E-mail: novikova@comsec.spb.ru

2 Котенко Игорь Витальевич, заслуженный деятель науки РФ, доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург. ORCID: 0000-0001-6859-7120. Scopus Author ID: 15925268000. E-mail: ivkote@comsec.spb.ru.

3 Мелешко Алексей Викторович, младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург. ORCID: 0000-0002-1209-4230. Scopus Author ID: 57214672771. E-mail: meleshko.a@iias.spb.su.

4 Израилов Константин Евгеньевич, кандидат технических наук, доцент, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург. ORCID: 0000-0002-9412-5693. Scopus Author ID: 56123238800. E-mail: konstantin.izrailov@mail.ru.

ве правил и сигнатур в силу их простоты внедрения и прозрачности получаемых результатов. Ключевой преградой к широкому практическому применению подходов на основе МО является необходимость их адаптации (переобучения) к защищаемой системе, что является ресурсоемким и трудоемким процессом, который требует наличия хорошо структурированных размеченных наборов данных. Доступ к таким данным часто ограничен, что также значительно затрудняет процесс тестирования и внедрения компонент обнаружения вторжения на основе МО, несмотря на их способность обнаруживать сложные, многошаговые и растянутые во времени атаки.

Одним из заметных достижений в области МО в последнее время стало определение концепции федеративного обучения (ФО) как способа организации распределенного МО, при котором владельцы данных не обязаны делиться ими для построения модели МО [8]. Формирование глобальной модели осуществляется итеративно на основе обновлений, полученных от узлов — владельцев данных. Такая распределенная схема позволяет строить аналитические системы [9], в основе которых лежит МО, при этом сохраняя конфиденциальность данных конечных пользователей. Кроме того, она дает возможность естественным образом расширить обучающую выборку.

В кибербезопасности ФО может быть рассмотрено как механизм обмена данными об угрозах и атаках на защищаемые системы без необходимости распространения реальных данных, способствуя тем самым развитию совместных подходов к реализации и построению эффективных систем обнаружения и противодействия кибератакам. Несмотря на то, что в последнее время предложено большое число подходов к обнаружению вторжений на основе ФО, многие практические вопросы по его использованию остаются открытыми [10-13]: например, построение системы обнаружения вторжений (СОВ) на основе ФО, оценивание эффективности обнаружения вторжений, определение требований к вычислительным ресурсам и пропускной способности канала связи компонентов (что особенно важно для систем на базе технологии Интернета Вещей).

В настоящей работе представлена архитектура СОВ на основе ФО и даны описания основных ее компонентов. Для оценки эффективности применения ФО в СОВ и определения вычислительных требований к компоненту СОВ на его основе предложен сценарий эксперимента, который определяет схему распределения данных между клиентами и метрики оценки эффективности моделей МО, обученных в федеративном режиме.

Статья структурирована следующим образом. В разделе 1 кратко представлена концепция ФО, а в разделе 2 дается анализ релевантных работ. В разделе 3 обсуждается архитектура СОВ и приводится описание ее компонентов, выполняющих ФО, в разделе 4 представлены описание экспериментов и полученные результаты. В разделе 5 делаются выводы и формулируются направления дальнейших работ.

1. Федеративное обучение

ФО является способом организации распределенного МО, при котором данные не собираются в единое централизованное хранилище, а используются для выполнения локального обучения на узлах их генерации; для формирования общей или глобальной аналитической модели результаты локального обучения объединяются (агрегируются) специальным образом, который зависит от модели. Таким образом, составными элементами ФО являются следующие компоненты:

1) клиенты — узлы, которые генерируют и накапливают данные, а также выполняют обучение локальных моделей;

2) агрегирующий сервер — узел, который управляет процессом обучения в федеративном режиме и вычисляет глобальную модель;

3) коммуникационно-вычислительная среда — сетевое пространство, обеспечивающее передачу информации между клиентами и сервером.

Формально, ФО определяется следующем образом. Пусть $C = \{c_i\}_{i=0}^{n}$ –множество из n клиентов, каждый из которых владеет некоторым набором данных d_i; при этом, клиенты желают совместно обучить некоторую аналитическую модель на всем множестве наборов данных. В случае традиционного МО все наборы данных d_i объединяются в единый набор $D = \{d_0 \cup d_1 \cup \ldots \cup d_n\}$, на котором обучается модель M_D с некоторой точностью $A(M_D)$. В случае ФО множество наборов данных не объединяется, а глобальная модель M_{FL} вычисляется на основе локально обученных моделей M_{di}, причем ее точность $A(M_{FL})$ должна удовлетворять следующему требованию:

$$|A(M_D) - A(M_{FL})| \leq \delta,$$

где δ — неотрицательное вещественное число, т.е. разница в точности этих моделей не должна превышать некоторый заданный порог δ.

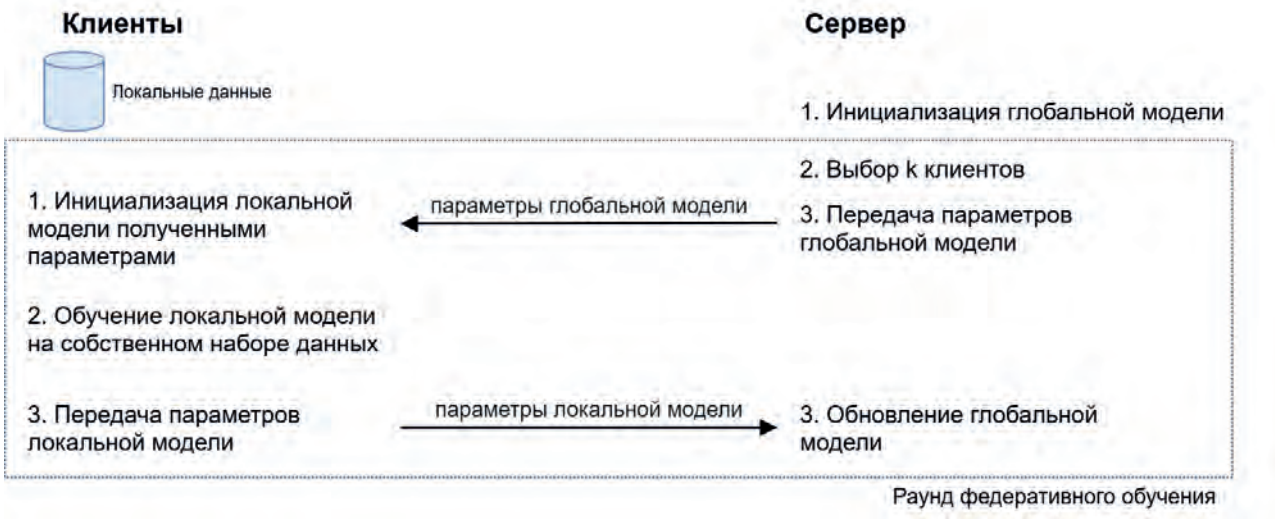

Рис. 1. Упрощенная схема раунда федеративного обучения

Процесс ФО состоит из нескольких шагов, которые выполняются итеративно. В начале каждого раунда (т. е. итерации) из *n* клиентов случайным образом выбирается *k* клиентов, которым агрегирующий сервер пересылает текущие параметры глобальной модели. Затем каждый отобранный клиент выполняет обучение локальной модели на собственном наборе данных, а полученные результаты отправляет агрегирующему серверу. Последний, получив новые данные от клиентов, обновляет глобальную модель, и процесс обучения повторяется. Упрощенная схема раунда ФО представлена на рис. 1.

В настоящее время предложены варианты протоколов ФО, которые обеспечивают аутентификацию клиентов и агрегирующего сервера, а также подтверждение подлинности источника передаваемых параметров модели [14, 15].

Наиболее часто используемым алгоритмом агрегирования для формирования глобальной модели является *федеративное усреднение* (*FederatedAveraging*) [8], который основан на определении весовой суммы параметров локальных моделей, чьи веса пропорциональны размеру соответствующей обучающей выборки клиента.

Системы ФО обычно характеризуются тремя следующими свойствами: схемой взаимодействия между клиентами, схемой разделения данных, а также вычислительными и сетевыми ресурсами, доступными взаимодействующим клиентам.

Схема взаимодействия между клиентами определяет то, каким образом осуществляется координация процесса ФО в целом, и какой участник отвечает за формирование глобальной модели — т.е. кто выполняет функции агрегирующего сервера. В централизованной схеме ФО выделяется отдельный узел, выполняющий роль сервера-агрегатора. Другие участники ФО передают параметры локальных моделей данному узлу и, соответственно, получают от него обновления глобальной модели. В случае децентрализованной схемы ФО (также известной как роевое обучение), функции агрегирующего сервера распределены между всеми участниками процесса, а для формирования глобальной модели результаты локального обучения рассылаются всем участникам.

Схема разделения данных определяет распределение атрибутов и объектов в наборах данных, принадлежащих разным клиентам. Пусть набор данных *DS* задается парой множеств $DS = \langle E, A \rangle$, где E — это множество объектов (например, сетевых потоков), а A — множество атрибутов, характеризующих эти объекты (например, длительность потока, число переданных байт или пакетов, количество соединений и т. п.). Выделяют два основных способа разделения данных между k клиентами — горизонтальный и вертикальный.

В первом случае каждый *i*-й клиент владеет собственным набором данных DS_i, полученных путем выделения подмножества объектов:

$$\begin{cases} \forall 1 \geq i \geq k : DS_i = \langle E_i, A \rangle \\ E = \{E_1 \cup E_2 \cup \ldots \cup E_k\} \\ \forall 1 \geq j \geq k, j \neq i : E_j \cap E_i = \emptyset \end{cases}.$$

Во втором случае каждый j-й клиент владеет собственным набором данных DS_j, полученных путем выделения подмножества атрибутов:

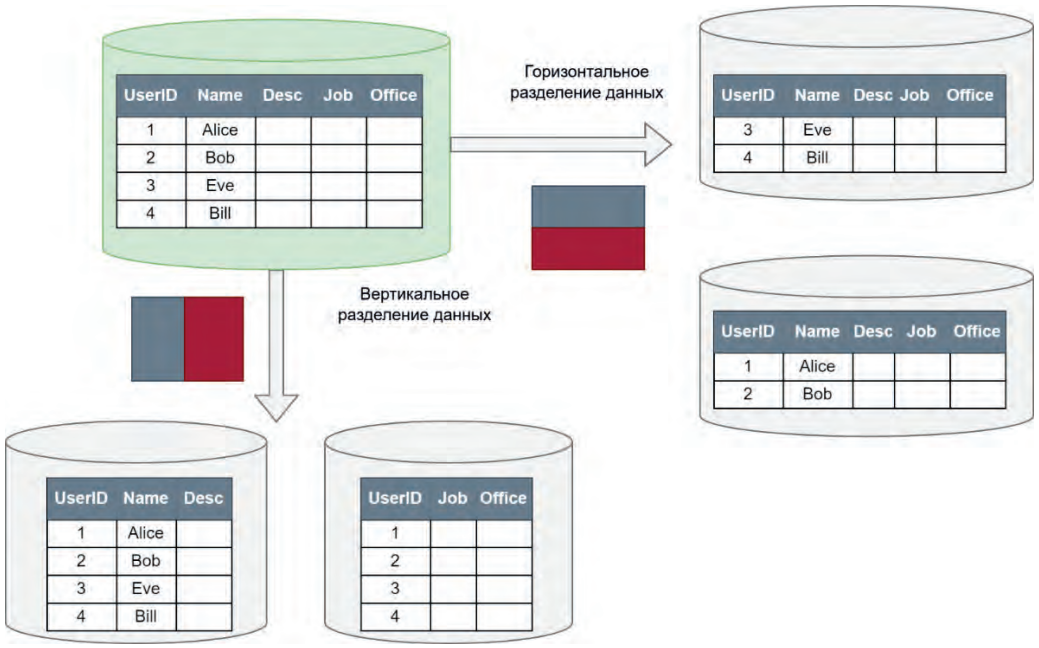

Рис. 2. Схема разделения данных

$$\begin{cases} \forall 1 \geq j \geq k: DS_j = \langle E, A_j \rangle \\ A = \{A_1 \cup A_2 \cup \ldots \cup A_k\} \\ \forall 1 \geq i \geq k, i \neq j: A_i \cap A_j = \emptyset \end{cases}.$$

На рис. 2 показаны примеры для указанных схем разделения данных между двумя клиентами.

Исходя из характеристик вычислительных и сетевых ресурсов, которые доступны взаимодействующим клиентам, обычно выделяют федерацию устройств и федерацию организаций. Для федерации устройств характерны (1) большое число возможных участников ФО с достаточно ограниченными вычислительными ресурсами и (2) нестабильное подключение устройств во время обучения; например, объединение мобильных устройств связи. Для федерации организации напротив характерно небольшое число участников с достаточно мощными вычислительными ресурсами, большим каналом связи и стабильным подключением во время обучения; например, крупные компании и организации.

2. Анализ релевантных работ

Исследование работ, посвященных построению систем обнаружения вторжений на основе ФО, показал, что чаще всего для построения СОВ используется централизованная топология ФО с горизонтальным разделением атрибутов [16-18]. Например, в [19] предложен подход к обнаружению вторжений для систем, построенных на основе технологии Интернета вещей. Авторы используют рекуррентную нейронную сеть, обученную в федеративном режиме для выявления аномалий в поведении устройств заданного типа. Построение аналитических моделей для каждого типа устройств позволяет задать горизонтальную схему разделения данных. В качестве тестового набора данных был использован набор данных, собранный с помощью тестового стенда, разработанного авторами [19] и состоящего из 14 устройств «умного» дома.

Похожая задача решается в [20], однако в этой работе в качестве тестового набора данных был использован набор N-BaIoT [21], который моделирует сетевой трафик от 9 реальных устройств Интернета вещей разного типа. Исходный набор данных был разделен между тремя клиентами по 100 000 записей на каждом, а соотношение нормальных и аномальных записей в каждом локальном наборе в проводимых экспериментах варьировалось. Основной акцент в работе был сделан на оценку влияния архитектуры нейронной сети на эффективность выявления аномалий и вторжений в различных сценариях распределения данных.

Система обнаружения FELIDS представлена в [13]. Для моделирования взаимодействия различных агентов авторы использовали несколько наборов данных: CSE-CIC-IDS2018 [22], MQTTset [23], и InSDN [24], а для организации ФО была использована специализированная программная библиотека Sherpa.ai [25]. Авторы тестировали эффективность нейронных сетей с различной архитектурой, обученных в федеративном режиме, и показали, что наиболее эффективной является полносвязная сеть, точность обнаружения атак которой достигла 98.54%.

В [26] предложена двухуровневая иерархическая распределенная СОВ на основе ФО. Причиной такого решения является высокий уровень неоднородности информационных технологий и подходов, используемых для построения информационных систем различных организаций. Авторы предложили разделить подсети отдельных организации на сегменты, и соответственно, процесс ФО выполнялся сначала на уровне сегмента — локальный или промежуточный уровень, а на глобальном уровне модели промежуточного уровня были объединены в единую глобальную модель. Для выполнения экспериментов был использован набор BoT-IoT [27]. Особенностью данной работы является использование технологии блокчейна для обеспечения неизменности результатов промежуточного и глобального обучения.

Децентрализованная схема ФО предложена для построения СОВ, разрабатываемых для интеллектуальных транспортных систем [28-30]. Данное решение обусловлено, в первую очередь, географической распределенностью таких систем и разнообразием транспортных маршрутов. В этом случае также используется иерархическая двухуровневая модель ФО — на нижнем уровне транспортные средства собирают данные вокруг себя и обновляют модели, полученные от базовых станций. Последние, с помощью технологии блокчейн фиксируют и валидируют все обновления, и после опубликования локальных моделей они уже выполняют формирование общей глобальной модели. Следует отметить, что эксперименты в [28] проводились при помощи двух открытых наборов данных — Car-Hacking, TON_IoT, близких к исследуемой предметной области. В [30] эксперименты были выполнены на таких наборах данных, как MNIST и CIFAR, которые представляют собой коллекцию изображений, что не позволяет судить о применимости результатов к задаче обнаружения вторжений.

Случай вертикально разделенных данных гораздо сложнее и практически не исследован в задачах обнаружения вторжений [31].

Таким образом, можно заключить, что на текущий момент все опубликованные подходы в предметной области представляют собой простой анализ применимости ФО к обнаружению аномалий и вторжений, который заключается в использовании современного и актуального набора данных, моделировании его распределения по множеству взаимодействующих клиентов и оценке точности обнаружения. Вопросы, связанные с оценкой требуемых вычислительных ресурсов для СОВ на основе ФО, практически не решаются.

3. Архитектура СОВ на базе федеративного обучения

В работе предлагается следующая архитектура СОВ, построенная с применением ФО. Основными элементами СОВ являются: компоненты сбора данных или сенсоры безопасности; компоненты анализа данных, которые реализуют различные стратегии обнаружения атак и аномалий; хранилища данных, в которых содержатся как исходные «сырые» события безопасности, так и результаты анализа; база знаний для механизмов обнаружения вторжений и аномалий. В состав СОВ также часто включают компонент оценки рисков и принятия контрмер, на вход которого подается информация о конфигурации защищаемой системы. База знаний СОВ должна постоянно обновляться для актуализации перечня детектируемых информационных угроз. В случае «облачных» СОВ потоки данных от сенсоров безопасности также направляются в облачный центр безопасности, что позволяет проводить глобальную аналитику безопасности, а также разрабатывать новые методы обнаружения вторжений на их основе [32].

Применение ФО для построения СОВ позволяет локально настраивать механизмы обнаружения на основе МО с учетом данных, собираемых локально, и регулярно их обновлять без передачи данных на облачный сервер безопасности. Таким образом, использование ФО изменяет существующие потоки данных в среде СОВ. Структура облачного сервера СОВ расширяется за счет компонентов, отвечающих за организацию и координацию ФО, а структура агента СОВ дополняется компонентами, отвечающими за работу с локальной моделью.

На рис. 3 представлена структурная схема интеллектуальной СОВ (в виде внешних и внутренних информационных объектов, выделенных подсистем и решаемых ими задач), которая использует ФО для настройки и обновления компонентов анализа данных (использованы следующие обозначения: синие прямоугольники — подсистемы СОВ, зеленые прямоугольники — решаемые задачи; желтые объекты — внутренние информационные объекты: шестиугольник — аналитическая модель, цилиндр — репозиторий данных; пунктирные фигуры — дублируемые элементы; облако — информационные объекты или сети).

Схема отражает следующие элементы и логические связи между ними:

1) сеть — внешняя система устройств с каналами передачи данных, подверженная атакам и защищаемая СОВ; сети принадлежат разным организациям;

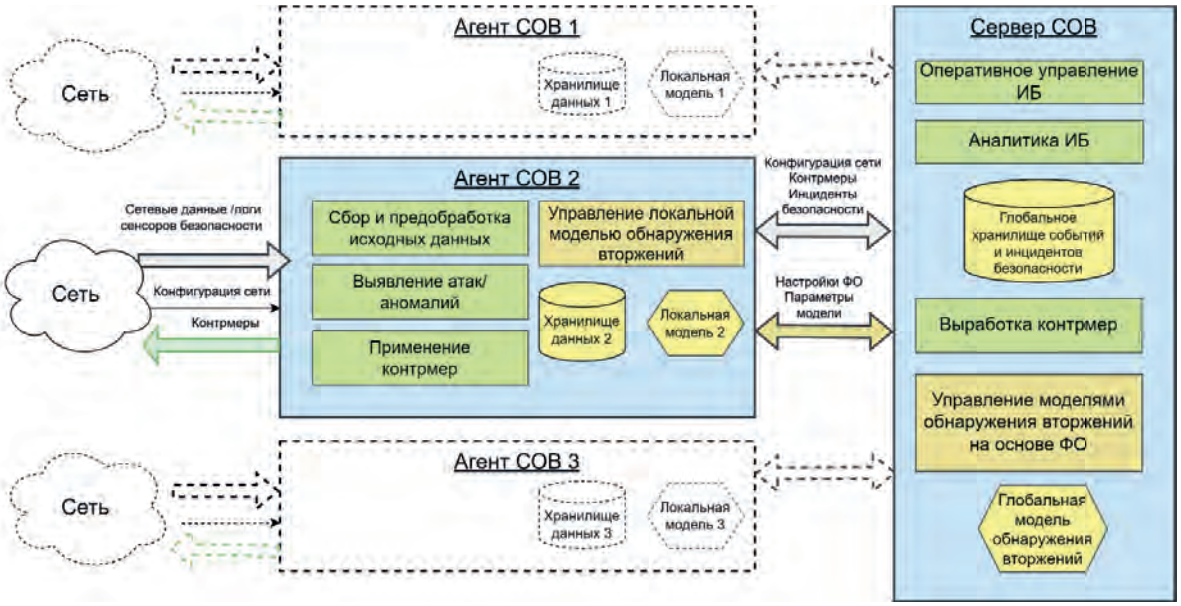

Рис. 3. Структурная схема СОВ, использующая ФО

2) агент СОВ — интеллектуальный агент распределенной СОВ, который обеспечивает анализ состояния и процессов контролируемой сети, выполняет выявление атак и противодействие им;

3) сбор и предобработка исходных данных — задача сбора событий безопасности от различных устройств и приложений, установленных в сети, а также приведения их к виду, подходящему для дальнейшего анализа (включая нормализацию событий, их агрегирование и фильтрацию);

4) выявление атак/аномалий — задача выявления атак и/или аномалий различными методами, реализованными в СОВ; в данной работе рассматриваются методы на базе МО;

5) применение контрмер — задача применения мер противодействия выявленным атакам с учетом текущей конфигурации контролируемой сети; в настоящей работе считается, что выработка контрмер осуществляется сервером СОВ;

6) обучение локальной модели обнаружения вторжений — задача обучения и обновления модели обнаружения вторжений в режиме ФО;

7) локальная модель — аналитическая модель, построенная на основе локальных данных, но с учетом параметров глобальной модели, и выполняющая задачу обнаружения вторжений;

8) хранилище данных — хранилище локальных данных от сенсоров безопасности, которые используются для обучения и обновления модели обнаружения вторжений;

9) сервер СОВ — центральная функциональная подсистема, обеспечивающая координирование всех агентов СОВ, собирающая информацию от них об инцидентах безопасности для формирования глобальной аналитики, настраивающая аналитические модели обнаружения вторжений и вырабатывающая контрмеры на основе полученной информации о конфигурации защищаемой сети и выявленных инцидентах безопасности;

10) оперативное управление информационной безопасностью (ИБ) — задача формирования ситуационной осведомленности о выявленных инцидентах для реагирования на них;

11) аналитика ИБ — задача формирования аналитических отчетов об инцидентах безопасности, выявления основных трендов при нарушении безопасности и т. д.;

12) глобальное хранилище событий и инцидентов безопасности — единая база для всех выявленных инцидентов, служащая для формирования различных механизмов обнаружения вторжений, а также для оценки эффективности глобальной(-ых) модели (моделей) обнаружения вторжений, обучаемых в федеративном режиме.

13) выработка контрмер — задача создания и передачи контрмер конкретным агентам на основании обнаруженных атак, текущей конфигурации сети и процедур противодействия;

14) управление моделями обнаружения вторжений на основе ФО — задача координации процесса об-

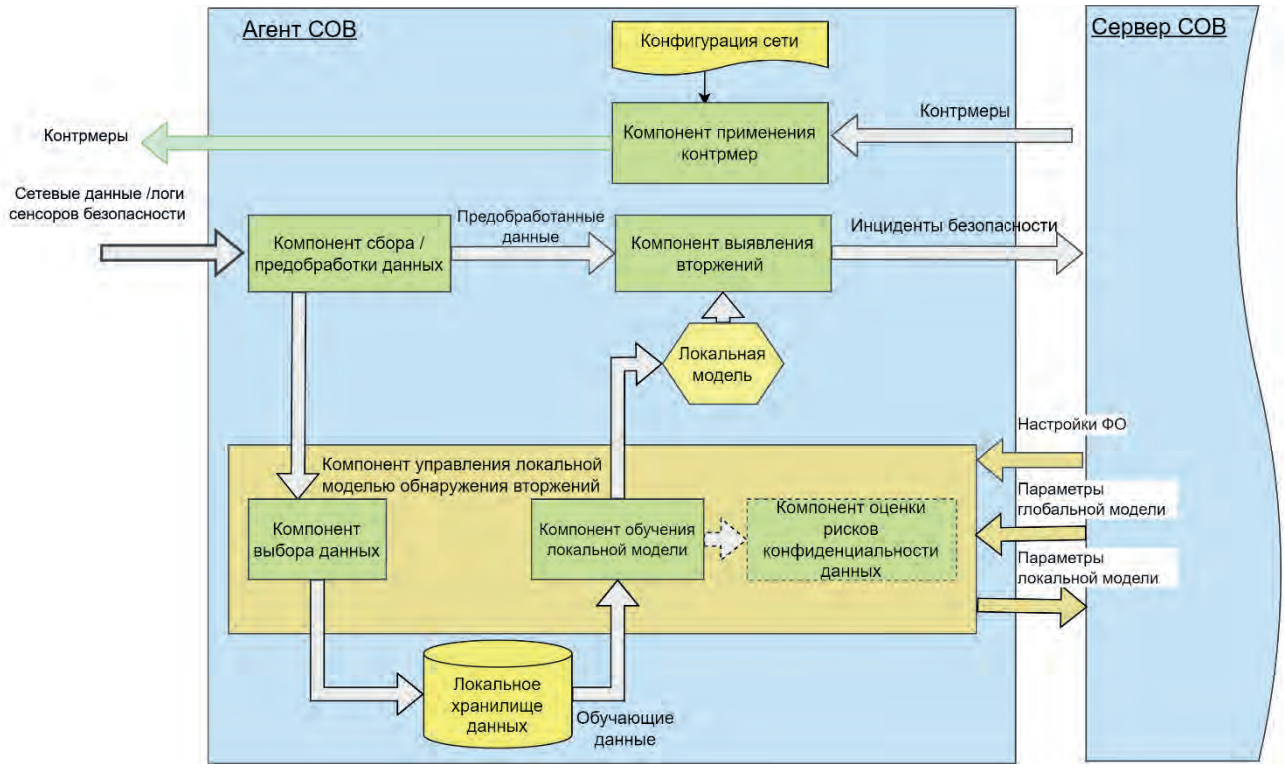

Рис. 4. Структурная схема агента СОВ

учения модели в федеративном режиме, включая выбор агентов СОВ, участвующих в обучении, настройку их конфигурации, обмен параметрами моделей и т. д.;

15) глобальная модель обнаружения вторжений — аналитическая модель, полученная путем синхронизации всех локальных моделей агентов; для простоты будем считать, что такая модель одна, хотя очевидно, что их может быть множество для разных задач и источников данных.

Согласно схеме (см. рис. 3), сервер СОВ выполняет роль агрегирующего сервера ФО, управляя и координируя действия множества обособленных агентов СОВ, отвечающих за безопасность некоторой компьютерной сети(ей). Каждый агент СОВ настраивает и до-обучает глобальную модель на собственном наборе данных, а также выполняет обнаружение атак с ее помощью. При этом, полученные локальные аналитические модели агентов объединяются в общую глобальную модель на сервере, расширяя тем самым диапазон детектируемых ею атак. Следует отметить, что при этом сервер СОВ, как и раньше выполняет роль центра мониторинга ИБ, собирая и агрегируя информацию о выявленных инцидентах безопасности. Полученная таким образом информация может быть использована, в том числе, для валидации и оценки эффективности глобальной модели. Как и в классических решениях по предупреждению вторжений, задача выбора контрмер решается сервером СОВ.

Рассмотрим далее более детально функциональность каждого компонента СОВ — сервера и интеллектуального агента. На рис. 4 представлена функциональная схема агента СОВ (в виде ее функциональных компонентов и обрабатываемых информационных объектов).

Агент СОВ включает следующие элементы:

1) компонент сбора и предобработки данных — осуществляет сбор сетевых данных и логов сенсоров безопасности, а также их обработку для дальнейшего использования;

2) компонент управления локальной модели обнаружения вторжений — выполняет основные функции по формированию обучающей выборки и обучению модели анализа в федеративном режиме в соответствии с полученными настройками ФО;

3) локальное хранилище данных — используется для хранения предобработанных данных, необходимых для обучения локальной модели;

4) компонент выявления вторжений — обнаруживает инциденты безопасности (используя для этого обученную локальную модель обнаружения вторжений) и передает их серверу СОВ;

5) компонент применения контрмер — получает от сервера СОВ контрмеры для противодействия атакам и выполняет их;

6) локальная модель — аналитическая модель анализа, используемая агентом для выявления вторжений.

Компонент управления локальной моделью обнаружения вторжений состоит из трех следующих компонентов: (1) выбора данных, (2) обучения локальной модели и (3) оценки рисков конфиденциальности данных. Компонент выбора данных отвечает за отбор и разметку новых данных, необходимых для настройки локальной модели. Наличие данного модуля связано, в первую очередь, с ограниченными возможностями интеллектуального агента СОВ по хранению данных; например, некоторые сетевые роутеры, которые используются для развертывания системы «умного» дома, имеют только 32Mb памяти для хранения данных. Другой причиной ввода данного компонента в систему является непрерывность генерации данных, в результате чего необходимо в режиме реального времени принимать решение о том, сохранять их или нет. Для реализации компонента может быть использован подход, предложенный в [33], который заключается в оценке поступающих данных в контексте параметров локальной модели и отборе тех образцов, которые соответствуют распределению локальных и глобальных данных, что в конечном итоге уменьшает уровень их разнородности между клиентами и позволяет повысить эффективность ФО. Компонент обучения локальной модели отвечает непосредственно за выполнение ФО, настройки для его выполнения передаются сервером СОВ. Компонент получает параметры глобальной модели, инициализирует с их помощью локальную модель и обновляет ее с учетом данных, накапливаемых локально. Компонент оценки рисков конфиденциальности данных, используемых для выполнения, является необязательным, поскольку его задачей является отслеживание и расчет рисков утечек конфиденциальной информации непосредственно во время обучения. Для реализации компонента может быть использован подход, предложенный в [34], согласно которому оценка рисков учитывает как уровень критичности различных атрибутов, используемых при обучении модели, так и взаимную информационную связь между ними и параметрами модели, передаваемыми серверу СОВ.

На рис. 5 представлена функциональная схема сервера СОВ (в виде ее функциональных компонентов и обрабатываемых информационных объектов). Сервер СОВ включает следующие элементы:

1) компонент выработки контрмер — формирует контрмеры на основе текущей конфигурации защищаемой сети и наблюдаемых инцидентов безопасности;

2) компонент аналитики ИБ — выполняет функцию формирования различных отчетов на основе инцидентов безопасности, выявленных в различных сетях;

3) компонент оперативного управления ИБ — реализует текущий мониторинг различных инцидентов безопасности, выявляемых в различных организациях;

4) компонент управления моделями обнаружения вторжений на основе ФО, состоящий из трех основных компонентов - выбора настроек ФО, агрегации данных и обнаружения атак на ФО;

5)глобальное хранилище событий и инцидентов безопасности — используется для хранения полного набора событий и инцидентов безопасности от всех агентов в интересах последующего централизованного анализа;

6) глобальная модель обнаружения вторжений — в общем случае представляет собой репозитории различных моделей обнаружения вторжений.

Компонент управления моделями обнаружения вторжений на основе ФО состоит из трех следующих компонентов: выбора настроек ФО, агрегации данных и обнаружения атак на ФО. Компонент выбора настроек ФО отвечает за общие настройки агентов СОВ, такие как схема анализируемых атрибутов, тип аналитической модели, ее архитектура, число раундов формирования глобальной модели, число локальных эпох обучения и т.д. Данный компонент на основе анализа конфигурации агента СОВ (а именно, в зависимости от доступных вычислительных ресурсов, объема локального хранилища, уровня доверия защищаемой сети) также определяет стратегию выбора клиентов в процессе обучения, функцию агрегирования данных и т.д. Таким образом, компонент как настраивает параметры ФО на сервере СОВ, так и передает параметры для выполнения локального обучения на агентах СОВ. Компонент агрегации данных выполняет вычисление глобальной модели на основе параметров локальной. На этапе инициализации для этого может быть использована модель, предобученная на некотором доступном наборе данных с похожими характеристиками: общими атрибутами, близкими вероятностями распределения их значений и т.д. Компонент обнаружения атак на ФО предназначен для выявления атак, направленных непосредственно на ФО и глобальную модель анализа. Поскольку ФО построено на взаимодействии некоторого множества агентов, то их присутствие рас-

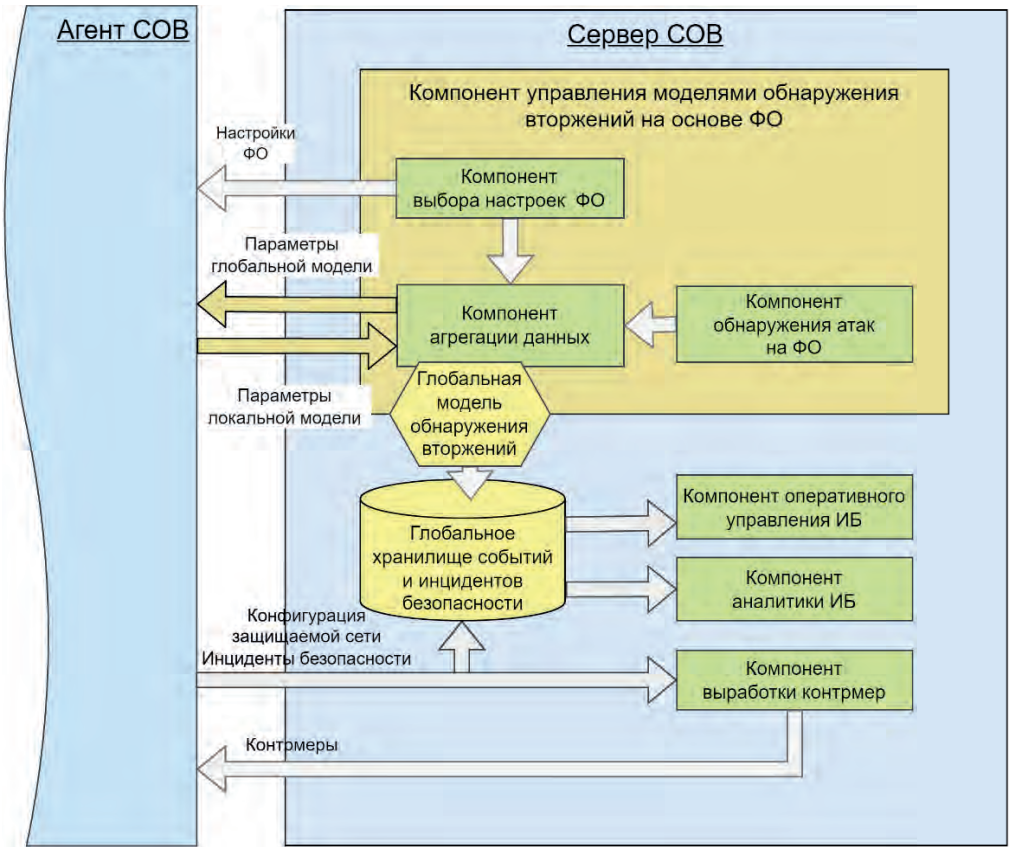

Рис. 5. Структурная схема сервера СОВ

ширяет поверхность вектора атак и актуализирует вопросы, связанные, в первую очередь, с защитой целостности и аутентичности данных, используемых при обучении. Атаки могут быть направлены на модификацию как данных, так и параметров передаваемой модели. Для выявления и противодействия таким атакам предложены различные подходы, в основе которых могут лежать следующие принципы: оценка расстояния между передаваемыми параметрами локальных моделей [35], исключение *k* самых больших и самых маленьких значений параметров модели [36], использование дополнительного тестового набора данных [37] и др.

4. Экспериментальная оценка

Для выполнения экспериментальной оценки компонента СОВ на основе ФО были решены следующие задачи: (1) построение экспериментального стенда; (2) моделирование разбиения данных между агентами СОВ; (3) определение метрик, позволяющих оценить как эффективность модели, обученной в федеративном режиме, так и определить требования к ресурсам агента СОВ для выполнения данной задачи.

Для организации федеративного обучения между агентами был выбран программный проект Flower [38]. Данный проект не требователен к вычислительным ресурсам и легко настраивается. Взаимодействие между клиентами и сервером ФО осуществляется на основе технологии gRPC. Проект предусматривает два режима запуска ФО — симуляционный и федеративный. В симуляционном режиме возможно запустить систему ФО (один сервер и несколько клиентов) на одной вычислительной машине. Имеется также возможность предварительной оценки производительности ФО на основе средств мониторинга системных ресурсов, обеспечивающих определение загрузки ЦПУ, потребления оперативной памяти и объема передаваемого сетевого трафика. В федеративном режиме система разворачивается на реальных физических устройствах. Кроме того, фреймворк проекта имеет хорошо описанные программные интерфейсы для подключения собственных алгоритмов агрегирования локальных моделей и на текущий момент поддерживает различные алгоритмы агрегирования, устойчивые к неидентично распределенным данным [39,40]. Например, в него включены недавно предложенные стратегии для гетерогенных и неидентичных данных:

— распределенный алгоритм агрегации на основе расчета медианных значений для параметров модели, который использует только один раунд связи между клиентами, что позволяет более высокую эффективность передаче данных [41];
— адаптивная стратегия оптимизации на стороне сервера, учитывающая гетерогенность устройств [39];
— FedBN-стратегия оптимизации, выполняемая на стороне клиента, которая использует локальные слои пакетной нормализации для решения проблем сдвига в неидентично распределенных данных[40].

В литературе предложено два следующих варианта моделирования распределения данных между клиентами [42]:

— один набор данных распределяется между *N* клиентами так, чтобы каждый клиент отвечал за определенный тип атак;
— каждый клиент получает свой набор данных, у которых одинаковое количество атрибутов.

В настоящей работе был использован первый вариант моделирования распределения данных между клиентами. В качестве основного набора данных использовался CIC-IDS2017 [22]. Он содержит информацию о сетевых потоках за 5 дней функционирования небольшой компьютерной сети, состоящей из 10 рабочих станций, в виде описательных статистик различных параметров (например, длины пакетов). Логи первого дня соответствуют нормальному функционированию системы, а данные за остальные четыре дня содержат информацию о различных сетевых атаках. Для выполнения экспериментов набор CIC-IDS2017 был поделен на две части таким образом, чтобы в состав каждого набора входили данные о разных типах атак. В табл. 1 приведена структура обоих наборов данных, которые использовались в экспериментах; во всех экспериментах набор данных был разделен на обучающую и тестовую выборки в соотношении 80 к 20.

С учетом того, что в каждом наборе данных представлены разные типы атак, было принято решение сформулировать задачу обнаружения вторжений в виде задачи бинарной классификации — т.е. определения того, является ли сетевой поток нормальным или нет.

Структура сверточной нейронной сети, которая во всех экспериментах обучалась 5 эпох, представлена на рис. 6.

Таблица 1

Структура наборов данных, используемых в экспериментах

Класс	Число сетевых потоков
Набор данных (DS1)	
Норма	251547
Атака Brute Force FTP	7916
Атака Brute Force SSH	4928
Dos-атака GoldenEye	15146
Dos-атака Hulk	28216
Dos-атака Slowhttptest	5621
Dos-атака Slowris	6081
Атака Hearbleed port 444	2
Набор данных (DS2)	
Норма	251547
Атака на проникновение Cool disk (MAC OS)	2
Атака на проникновение Dropbox	10
Веб-атака с помощью sql инъекций	18
Веб-атака типа межсайтовый скриптинг (XSS-атака)	1324
Веб-атака методом прямого перебора	2700
Ботсеть ARES - sql	1470
DDoS -атака LOIT	90418
Сканирования портов (с межсетевым экраном)	728
Сканирования портов (без межсетевым экраном)	318756

Поскольку процесс ФО должен выполняться регулярно во время функционирования СОВ, то возникает необходимость оценить его влияние на функционирование самого агента; в данной работе в качестве такого параметра было выбрано время обучения и оценка этого параметра в зависимости от настроек ФО. Как результат, для оценки эффективности были использованы следующие метрики: точность глобальной модели (accuracy, precision and recall и F-мера), время обучения, потребление памяти и загрузка процессора.

Для оценки целесообразности применения ФО при построении аналитических моделей обнаружения

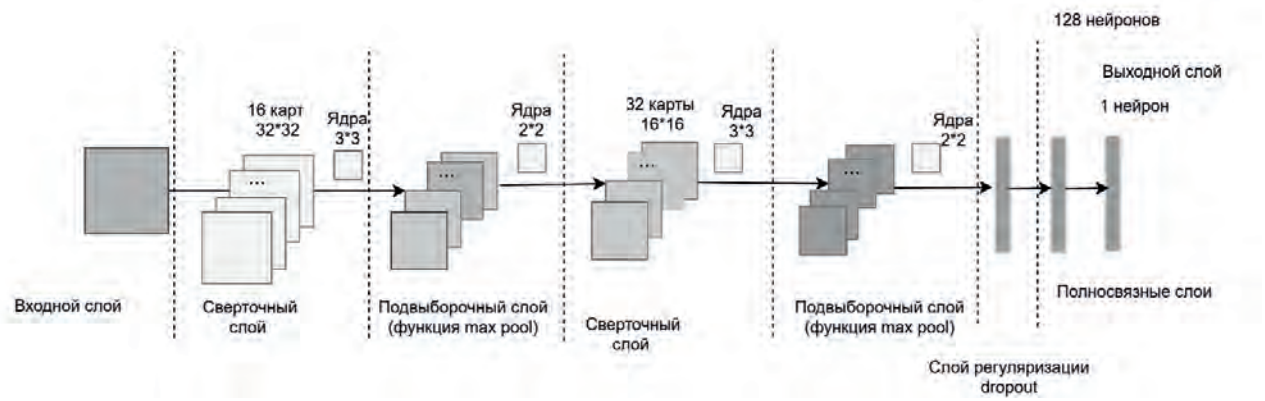

Рис. 6. Структура сверточной нейронной сети в экспериментах

Таблица 2

Точность обнаружения атак моделей, обученных только на локальных наборах данных

Обучающая выборка	Метрика	Тестовый набор данных	
		Набор данных DS1	Набор данных DS2
Набор данных DS1	Accuracy	0.99	0.48
	Recall	0.99	0.99
	Precision	0.99	0.42
	F-measure	0.99	0.59
Набор данных DS2	Accuracy	0.85	0.99
	Recall	0.99	0.99
	Precision	0.84	0.99
	F-measure	0.91	0.99

вторжений был разработан следующий сценарий эксперимента.

На первом этапе обучение модели осуществлялось на одном из наборов данных, а затем выполнялась оценка ее эффективности на втором наборе данных. Такая схема позволяет смоделировать ситуацию, когда некоторая обученная модель обнаружения «сталкивается» с новыми, ранее неизвестными ей типами атак, а полученные результаты позволяют судить об ее обобщающей способности. В этой серии экспериментов нейронная сеть обучалась 5 эпох. Полученные результаты представлены в табл. 2.

Очевидно, что точность детектирования сильно зависит от того, какие типы атак были представлены в обучающей выборке, и модель, обученная на наборе данных DS2 (который содержит более разнообразный набор атак), обнаруживает новые атаки более точно. Модель, которая обучалась на наборе данных DS1 (который содержит в основном DoS-атаки), обнаруживает атаки значительно хуже — ее точность составляет 48%, а низкое значение метрики precision (42%) говорит о высоком уровне ложноположительных срабатываний.

На втором этапе выполнялось обучение в федеративном режиме, моделировалось взаимодействие двух клиентов со следующими ресурсами: ЦПУ Intel Core i5-8 265U с тактовой частотой 1.80 ГГц и объемом оперативной памяти 8 ГБ. На одном клиенте в качестве обучающей выборки был использован набор данных DS1, а на втором - набор данных DS2.

Модель также обучалась 5 эпох, агрегация параметров локальных моделей выполнялась в следующих режимах: (1) каждый раунд; (2) каждые два раунда и (3) один раз в конце обучения. В качестве функции агрегации была использована функция FederatedAveraging. Результаты эксперимента приведены в табл. 3. Из нее следует, что точность модели, обученной в федеративном режиме, достаточно высокая на обоих наборах данных, благодаря объединению параметров локальных моделей, обученных

Таблица 3

Результаты обучения нейронной сети в федеративном режиме

Число раундов агрегации	Время обучения	Метрика	Тестовый набор данных	
			Набор данных DS1	Набор данных DS2
5 (после каждой эпохи обучения)	71.5 мин	Accuracy	0.94	0.99
		Recall	0.99	0.99
		Precision	0.93	0.99
		F-measure	0.96	0.99
3 (через каждые 2 эпохи)	80.0 мин	Accuracy	0.90	0.98
		Recall	0.99	0.99
		Precision	0.88	0.95
		F-measure	0.94	0.97
1 (в конце обучения)	73.1 мин	Accuracy	0.85	0.99
		Recall	0.99	0.99
		Precision	0.84	0.98
		F-measure	0.91	0.99

на каждом их них по отдельности. Следует отметить, что чем чаще происходило объединение моделей, т.е. чем выше было число раундов агрегации, тем выше точность модели была на обоих наборах данных. Длительность ФО в табл. 3 указана для агрегирующего сервера. В данном эксперименте зависимости длительности обучения от числа раундов агрегирования выявлено не было. Следует также отметить, что время локального обучения для двух клиентов было разным, для клиента с набором DS2 оно всегда было в 1.6 больше, чем с DS1, что закономерно, так как число записей в этом наборе в два раза больше числа записей в наборе DS1.

Средняя загрузка ЦПУ для обоих клиентов составила 40%, загрузка оперативной памяти составила 300-400МБ во время обучения.

Таким образом, можно сделать выводы, что, как и в случае классического машинного обучения, требования к ресурсам компонентов СОВ на основе ФО будут определяться объемом данных, которые используются для обучения, а также сложностью обучаемой модели. Соответственно, для систем с ограниченными вычислительными ресурсами возможно использование только легковесных и простых моделей МО. Повышение сложности аналитических моделей повлечет за собой повышение требований к вычислительным ресурсам, оперативной памяти и объему жесткого диска. Тем не менее целесообразность использования федеративного обучения для построения глобальных моделей обнаружения вторжений очевидна, оно естественным образом позволяет расширить множество детектируемых атак за счет увеличения обучающей выборки.

5. Заключение

В настоящее время в научном сообществе исследуются возможности федеративного обучения как механизма обмена знаниями об угрозах и атаках без обмена реальными данными. Предложенные решения, так и проведенные в данной работе эксперименты показывают эффективность его использования при построении моделей МО, предназначенных для выявления вторжений. Однако применение ФО в задачах обнаружения вторжений связано с решением многих практических задач, в частности, каким образом должны быть построены такие системы, как выполнять оценку их эффективности, как следует учитывать влияние ФО на функционирование всего компонента СОВ в целом, составным компонентом которого оно является.

В настоящей работе рассмотрена общая концепция ФО, предложена архитектура СОВ на основе ФО, представлены основные компоненты СОВ с описанием их функциональности. Также в работе приведены результаты экспериментальной оценки компонента СОВ, отвечающего за обнаружение вторжений. Дан-

ные оценки включают не только метрики точности выявления атак, но и характеристики потребления ресурсов на выполнение ФО.

В настоящий момент оценка влияния ФО ограничивается только оценкой длительности обучения, загрузкой ЦПУ и потреблением оперативной памяти, однако, она должна также включать данные по сетевому трафику для получения полноценного представления о необходимых и достаточных характеристиках компонента СОВ, отвечающего за локальное обучение на основе ФО. В связи с этом будущие работы включают в себя разработку системы мониторинга ФО, выполнения экспериментов с различными настройками ФО, включая оценку различных стратегий агрегирования. Отдельно следует выделить задачу по определению методики отбора данных для выполнения локального обучения, в том числе определения «эффективного» размера обучающей выборки.

Благодарность. *Исследование выполнено за счет гранта Российского научного фонда № 22-21-00724, https://rscf.ru/project/22-21-00724/.*

Рецензент: *Лаута Олег Сергеевич, доктор технических наук, профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, Санкт-Петербург, Россия.*

E-mail: laos-82@yandex.ru

Литература

1. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. 1335. DOI: 10.3390/s22041335.
2. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема // Вопросы кибербезопасности. 2023. № 3(55). С. 90-100. DOI: 10.21681/2311-3456-2023-3-90-100.
3. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 2. Алгоритм, модель и эксперимент // Вопросы кибербезопасности. 2023. № 4(56). С. 80-93. DOI: 10.21681/2311-3456-2023-4-80-93.
4. Котенко И.В., Саенко И.Б., Лаута О.С., Крибель А.М. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6 (98). С. 64-71. DOI: 10.22184/2070-8963.2021.98.6.64.70.
5. Котенко В.И., Саенко И.Б., Коцыняк М.А., Лаута О.С. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей // Труды СПИИРАН. 2017. № 6(55). С. 160-184. DOI: 10.15622/sp.55.7.
6. Branitskiy A., Kotenko I., Saenko I. Applying Machine Learning and Parallel Data Processing for Attack Detection in IoT // IEEE Transactions on Emerging Topics in Computing, 2021, vol. 9, no. 4. P. 1642-1653. DOI: 10.1109/TETC.2020.3006351.
7. Tushkanova O., Levshun D., Branitskiy A., Fedorchenko E., Novikova E., Kotenko I. Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation // Algorithms. 2023. 16(2):85. DOI: 10.3390/a16020085.
8. McMahan H. B., Moore E., Ramage D., Hampson S., Arcas B.A.Y. Communication-efficient learning of deep networks from decentralized data // International Conference on Artificial Intelligence and Statistics, 2016. URL: https://api.semanticscholar.org/CorpusID:14955348 (дата обращения: 20.08.2023).
9. Романов Н.Е., Израилов К.Е., Покусов В.В. Система поддержки интеллектуального программирования: машинное обучение feat. быстрая разработка безопасных программ // Информатизация и связь. 2021. № 5. С. 7-17. DOI: 10.34219/2078-8320-2021-12-5-7-16.
10. Astillo P.V., Duguma D.G., Park H., Kim J., Kim B., and You I.. Federated intelligence of anomaly detection agent in IoTmd-enabled diabetes management control system // Future Generation Computer Systems, 128. 2022. P.395–405. ISSN 0167-739X. DOI: 10.1016/j.future.2021.10.023.
11. Campos E.M., Saura P.F., Gonzalez-Vidal A., Hernandez-Ramos J., Bernabe J., Baldini G., and Skarmeta A. Evaluating federated learning for intrusion detection in internet of things: Review and challenges // Computer Networks, 2022. 203:108661. ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2021.108661.
12. Fedorchenko E., Novikova E., and Shulepov A. Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges // Algorithms, 15(7), 2022. ISSN 1999-4893. DOI: 10.3390/a15070247.
13. Friha O., Ferrag M. A., Shu L., Maglaras L., Choo K.-K., and Nafaa M. Felids: Federated learning-based intrusion detection system for agricultural internet of things // Journal of Parallel and Distributed Computing, 165, 2022. P.17–31. ISSN 0743-7315. DOI: 10.1016/j.jpdc.2022.03.003.
14. Bonawitz K., Ivanov V., Kreuter B., Marcedone A., McMahan H.B., Patel S., Ramage D., Segal A., and Seth K. Practical secure aggregation for privacy-preserving machine learning // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17, New York, NY, USA, 2017. Association for Computing Machinery. P.1175–1191. ISBN 9781450349468. DOI: 10.1145/3133956.3133982.
15. Stevens T., Skalka C., Vincent C., Ring J., Clark S., and Near J. Efficient differentially private secure aggregation for federated learning via hardness of learning with errors // 31st USENIX Security Symposium (USENIX Security 22). Boston, MA, August 2022. USENIX

Association. P.1379–1395. ISBN 978-1-939133-31-1. URL:https://www.usenix.org/conference/usenixsecurity22/ presentation/ stevens (дата обращения: 20.08.2023).
16. Aouedi O., Piamrat K., Muller G., and Singh K. Fluids: Federated learning with semi- supervised approach for intrusion detection system // 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC). 2022. P.523–524. DOI: 10.1109/ CCNC49033.2022.9700632.
17. Qin Y. and Kondo M. Federated learning-based network intrusion detection with a feature selection approach. // 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). 2021. P.1–6. DOI: 10.1109/ ICECCE52056.2021.9514222.
18. Fan Y., Li Y., Zhan M., Cui H., and Zhang Y. Iotdefender: A federated transfer learning intrusion detection framework for 5G IoT // 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE). 2020. P.88–95. DOI:10.1109/ BigDataSE50710.2020.00020.
19. Nguyen T.D., Marchal S., Miettinen M., Fereidooni H., Asokan N., and Sadeghi A.-R. Diot: A federated self-learning anomaly detection system for IoT // Proc. 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). 2019. P.756–767.
20. Rey V., Sanchez P.M.S., Celdran A.H., and Bovet G. Federated learning for malware detection in IoT devices // Computer Networks, 204:108693, 2022. ISSN 1389-1286. DOI: 10.1016/j.comnet.2021.108693.
21. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Shabtai A., Breitenbacher D., and Elovici Y. N-baiot—network-based detection of IoT botnet attacks using deep autoencoders // IEEE Pervasive Computing, 17(3). 2018. P.2–22, DOI: 10.1109/MPRV.2018.03367731.
22. Sharafaldin I., Lashkari A.H., and Ghorbani A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // Proc. of 4th International Conference on Information Systems Security and Privacy. 2018. P.108–116. DOI: 10.5220/0006639801080116.
23. Vaccari I., Chiola G., Aiello M., Mongelli M., Cambiaso E. MQTTset, a New Dataset for Machine Learning Techniques on MQTT // Sensors. 2020; 20(22):6578. https://doi.org/10.3390/s20226578.
24. Elsayed M. S., Le-Khac N.-A. and Jurcut A. D. InSDN: A Novel SDN Intrusion Dataset // IEEE Access, vol. 8. 2020. P.165263-165284. DOI: 10.1109/ACCESS.2020.3022633.
25. Rodrıguez-Barroso N., Stipcich G., Jimenez-Lopez D., Ruiz-Millan J.A., Martınez-Camara E., Gonzalez-Seco G., M. Luzon V., Veganzones M., and Herrera F. Federated learning and differential privacy: Software tools analysis, the sherpa.ai fl framework and methodological guidelines for preserving data privacy // Information Fusion, 64. 2020. P.270–292. ISSN 1566-2535. DOI: 10.1016/j. inffus.2020.07.009.
26. Sarhan M., Lo W.W., Layeghy S., and Portmann M. Hbfl: A hierarchical blockchain-based federated learning framework for a collaborative IoT intrusion detection, 2022. URL:https://arxiv.org/ abs/2204.04254 (дата обращения: 20.08.2023).
27. Moustafa N. The BoT-IoT dataset, 2019. URL https://dx.doi.org/10.21227/r7v2-x988 (дата обращения: 20.08.2023).
28. Abdel-Basset M., Moustafa N., Hawash H., Razzak I., Sallam K., and Elkomy O. Federated intrusion detection in blockchain-based smart transportation systems // IEEE Transactions on Intelligent Transportation Systems, 23(3). 2022. P.2523–2537. DOI: 10.1109/ TITS.2021.3119968.
29. Liu H., Zhang S., Zhang P., Zhou X., Shao X., Pu G., and Zhang Y. Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing // IEEE Transactions on Vehicular Technology, 70(6), 2021. P.6073–6084. DOI: 10.1109/ TVT.2021.3076780.
30. Chai H., Leng S., Chen Y., and Zhang K. A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles // IEEE Transactions on Intelligent Transportation Systems, 22(7), 2021. P.3975–3986. ISSN 1524-9050. DOI:10.1109/ TITS.2020.3002712.
31. Novikova E., Doynikova E., and Golubev S. Federated learning for intrusion detection in the critical infrastructures: Vertically partitioned data use case // Algorithms, 15(4), 2022. ISSN 1999-4893. doi:10.3390/a15040104.
32. Saputra F.A., Salman M., Hasim J.N., Nadhori I.U., Ramli K. The next-generation NIDS platform: Cloud-based snort NIDS using containers and big data // Big Data and Cognitive Computing, 6(1), 2022. ISSN 2504-2289. doi:10.3390/bdcc6010019.
33. Gong C., Zheng Z., Wu F., Shao Y., Li B., and Chen G.. To store or not? online data selection for federated learning with limited storage // Proc. of the ACM Web Conference 2023, WWW '23. New York, NY, USA, 2023. Association for Computing Machinery. P.3044–3055. ISBN 9781450394161. DOI: 10.1145/3543507.3583426.
34. Jiang C., Xia C., Liu Z., and Wang T. Feddroidmeter: A privacy risk evaluator for fl- based android malware classification systems. Entropy, 25(7), 2023. ISSN 1099-4300. DOI: 10.3390/e25071053.
35. Blanchard P., El Mhamdi E.M., Guerraoui R., and Stainer J. Machine learning with adversaries: Byzantine tolerant gradient descent // Proc. of the 31st International Conference on Neural Information Processing Systems, NIPS'17. Red Hook, NY, USA. Curran Associates Inc. 2017. P.118–128. ISBN 9781510860964.
36. Yin D., Chen Y., Kannan R., and Bartlett P. Byzantine-robust distributed learning: Towards optimal statistical rates // Proc. of the 35th International Conference on Machine Learning, volume 80 of Proceedings of Machine Learning Research. PMLR, 10–15 Jul 2018. P.5650–5659.
37. Cao X., Fang M., Liu J., and Gong N.J. Fltrust: Byzantine-robust federated learning via trust bootstrapping. CoRR, abs/2012.13995, 2020. URL: https://arxiv.org/abs/2012.13995. (дата обращения: 20.08.2023).
38. Flower — фреймворк для федеративного обучения. URL https://flower.dev/. (дата обращения: 20.08.2023).
39. Li X., Jiang M., Zhang X., Kamp M., and Dou Q. Fedbn: Federated learning on non-iid features via local batch normalization. CoRR, abs/2102.07623, 2021. (дата обращения: 20.08.2023).
40. Reddi S.J., Charles Z., Zaheer M., Garrett Z. , Rush K., Konecny J., Kumar S., and McMahan H.B. Adaptive federated optimization. CoRR, abs/2003.00295, 2020. (дата обращения: 20.08.2023).
41. Yin D., Chen Y., Ramchandran K., Bartlett P.L. Byzantine-Robust Distributed Learning: Towards Optimal Statistical Rates. International Conference on Machine Learning. 2018. URL: https://api.semanticscholar.org/CorpusID:3708326 (дата обращения: 20.08.2023).
42. Новикова Е.С., Федорченко Е.В., Котенко И.В., Холод И.И. Аналитический обзор подходов к обнаружению вторжений, основанных на федеративном обучении: преимущества использования и открытые задачи // Информатика и автоматизация, 22(5). С.1034–1082. DOI:10.15622/ia.22.5.4.

FEDERATED LEARNING BASED INTRUSION DETECTION: SYSTEM ARCHITECTURE AND EXPERIMENTS

Novikova E.S.[5], Kotenko I.V.[6], Meleshko A.V.7, Izrailov K.E.[8]

The goal of the investigation: *to develop an approach to building an intrusion detection system based on federated machine learning.*

Result: *the concept and architecture of an intrusion detection system based on federated machine learning is developed. The proposed architecture includes new components responsible for the organization of federated learning, such as components of data selection, local model training, sensitive information risk assessment, detection of federated learning attacks, and also defines their links with other functional elements of the system. To perform experimental evaluation of the components of the intrusion detection system based on federated learning, the metrics for evaluating their performance are formulated, they allow one to estimate, among other things, the requirements for the computational resources of the system. An approach to modeling the data distribution between the interacting components is proposed, and experimental evaluations of the intrusion detection performance using machine learning models trained in federated mode are obtained.*

Scientific novelty: *literature analysis has shown that the use of federated learning for building intrusion detection systems is associated with a number of open practical problems; in particular, there is no general methodology for building and evaluating the effectiveness of such systems. This paper proposes an architecture of the intrusion detection system that takes into account the practical features of using federated learning, and also presents the results of experimental evaluation of the effectiveness of intrusion detection models trained in federated mode.*

Contribution: *Novikova E.S. and Kotenko I.V. — the general concept and architecture of an intrusion detection system using federated learning, data collection methodology for researching the security of cyber-physical systems; Novikova E.S. and Izrailov K.E. — development of the functionality of individual components of the intrusion detection system, Meleshko A.V. — performing experiments.*

Keywords: *cybersecurity, cyberphysical systems, detection of anomalies and cyberattacks, distributed machine learning, convolutional neural network, performance assessment.*

References

1. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches . Sensors. 2022. Vol. 22. Iss. 4. pp. 1335. DOI: 10.3390/s22041335.
2. Izrailov K., Buinevich M. [A method for detecting attacks of different genesis on complex objects based on state information. Part 1. Prerequisites and scheme] Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема. Cybersecurity issues [Вопросы кибербезопасности]. 2023. No 3(55). pp. 90-100. DOI: 10.21681/2311-3456-2023-3-90-100. (in Russian)
3. Izrailov K., Buinevich M. [A method for detecting attacks of different genesis on complex objects based on state information. Part 2. Algorithm, model and experiment] Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 2. Алгоритм, модель и эксперимент. Cybersecurity issues [Вопросы кибербезопасности]. 2023. No 4(56). pp. 80-93.

5 Evgenia S. Novikova, Ph.D. (Technology), Associate Professor, Senior Researcher of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. ORCID: https://orcid.org/0000-0003-2923-4954. Scopus Author ID: 55415626100. E-mail: novikova@comsec.spb.ru.

6 Igor V. Kotenko, Honored Worker of Science of the Russian Federation, Dr.Sc. (Technology), Professor, Principal Researcher and Head of Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg. ORCID: 0000-0001-6859-7120. Scopus Author ID: 15925268000. E-mail: ivkote@comsec.spb.ru

7 Alexei V. Meleshko, Junior Researcher of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. ORCID: 0000-0002-1209-4230. Scopus Author ID: 57214672771. E-mail: meleshko.a@iias.spb.su.

8 Konstantin E. Izrailov, Ph.D. (Technology), Associate Professor, Senior Researcher of Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg. ORCID: 0000-0002-9412-5693. Scopus Author ID: 56123238800. E-mail: konstantin.izrailov@mail.ru.

DOI: 10.21681/2311-3456-2023-4-80-93. (in Russian)
4. Kotenko I., Saenko I., Lauta O., Kribel. [A method for early detection of cyberattacks based on the integration of fractal analysis and statistical methods] Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов. Pervaya milya [Первая миля]. 2021. № 6 (98). pp. 64-71. DOI: 10.22184/2070-8963.2021.98.6.64.70
5. Kotenko V.I., Saenko I.B., Kotsynyak M.A., Lauta O.S. [Assessment of Cyber-Resilience of Computer Networks based on Simulation of Cyber Attacks by the Stochastic Networks Conversion Method] Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей. SPIIRAS Proceedings [Труды СПИИРАН]. 2017. No 6(55). pp.160-184. DOI: https://doi.org/10.15622/sp.55.7.
6. Branitskiy A., Kotenko I., Saenko I. Applying Machine Learning and Parallel Data Processing for Attack Detection in IoT. IEEE Transactions on Emerging Topics in Computing, 2021, vol. 9, no. 4, pp. 1642-1653. DOI: 10.1109/TETC.2020.3006351.
7. Tushkanova O, Levshun D, Branitskiy A, Fedorchenko E, Novikova E, Kotenko I. Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation. Algorithms. 2023. 16(2):85. DOI: 10.3390/a16020085
8. McMahan H. B., Moore E., Ramage D., Hampson S., Arcas B.A.Y. Communication-efficient learning of deep networks from decentralized data. International Conference on Artificial Intelligence and Statistics, 2016. URL: https://api.semanticscholar.org/CorpusID:14955348 (accessed on: 20.08.2023).
9. Romanov N., Izrailov K., PokusovV. [Intelligent programming support system: machine learning feat. fast development of secure programs] Система поддержки интеллектуального программирования: машинное обучение feat. быстрая разработка безопасных программ. Informatization and communication [Информатизация и связь]. 2021. No 5. pp. 7-17. DOI: 10.34219/2078-8320-2021-12-5-7-16. (in Russian)
10. Astillo P.V., Duguma D.G., Park H., Kim J., Kim B., and You I. Federated intelligence of anomaly detection agent in IoTmd-enabled diabetes management control system. Future Generation Computer Systems, 128:395-405, 2022. ISSN 0167-739X. DOI: 10.1016/j.future.2021.10.023.
11. Campos E.M., Saura P.F., Gonzalez-Vidal A., Hernandez-Ramos J., Bernabe J., Baldini G., and Skarmeta A. Evaluating federated learning for intrusion detection in internet of things: Review and challenges. Computer Networks, 203:108661, 2022. ISSN 1389-1286. doi:https://doi.org/10.1016/j.comnet.2021.108661.
12. Fedorchenko E., Novikova E., and Shulepov A. Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges. Algorithms, 15(7), 2022. ISSN 1999-4893. DOI::10.3390/a15070247.
13. Friha O., Ferrag M. A., Shu L., Maglaras L., Choo K.-K., and Nafaa M. Felids: Federated learning-based intrusion detection system for agricultural internet of things. Journal of Parallel and Distributed Computing, 165:17–31, 2022. ISSN 0743-7315. DOI: 10.1016/j.jpdc.2022.03.003.
14. Bonawitz K., Ivanov V., Kreuter B., Marcedone A., McMahan H.B., Patel S., Ramage D., Segal A., and Seth K. Practical secure aggregation for privacy-preserving machine learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17, pp.1175–1191, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450349468. DOI:10.1145/3133956.3133982.
15. Stevens T., Skalka C., Vincent C., Ring J., Clark S., and Near J.. Efficient differentially private secure aggregation for federated learning via hardness of learning with errors. Proc. of 31st USENIX Security Symposium (USENIX Security 22), pp.1379–1395, Boston, MA, August 2022. USENIX Association. ISBN 978-1-939133-31-1. URL:https://www.usenix.org/conference/usenixsecurity22/ presentation/stevens (accessed on: 20.08.2023).
16. Aouedi O., Piamrat K., Muller G., and Singh K. Fluids: Federated learning with semi- supervised approach for intrusion detection system. 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), pp.523–524, 2022. DOI: 10.1109/CCNC49033.2022.9700632.
17. Qin Y. and Kondo M. Federated learning-based network intrusion detection with a feature selection approach. // 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), pp.1–6, 2021. DOI: 10.1109/ICECCE52056.2021.9514222.
18. Fan Y., Li Y., Zhan M., Cui H., and Zhang Y. Iotdefender: A federated transfer learning intrusion detection framework for 5G IoT . Proc. of 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), pp.88–95, 2020. DOI: 10.1109/BigDataSE50710.2020.00020.
19. Nguyen T.D., Marchal S., Miettinen M., Fereidooni H., Asokan N., and Sadeghi A.-R. Diot: A federated self-learning anomaly detection system for IoT. Proc. 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp.756–767, 2019.
20. Rey V., Sanchez P.M.S., Celdran A.H., and Bovet G. Federated learning for malware detection in IoT devices. Computer Networks, 204:108693, 2022. ISSN 1389-1286. DOI: 10.1016/j.comnet.2021.108693.
21. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Shabtai A., Breitenbacher D., and Elovici Y. N-baiot—network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3):12–22, 2018. DOI: 10.1109/MPRV.2018.03367731.
22. Sharafaldin I., Lashkari A.H., and Ghorbani A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. Proc. of 4th International Conference on Information Systems Security and Privacy. pp.108–116, 2018. DOI: 10.5220/0006639801080116.
23. Vaccari I., Chiola G., Aiello M., Mongelli M., Cambiaso E. MQTTset, a New Dataset for Machine Learning Techniques on MQTT . Sensors. 2020; 20(22):6578. https://doi.org/10.3390/s20226578.
24. Elsayed M. S., Le-Khac N. -A. and Jurcut A. D. InSDN: A Novel SDN Intrusion Dataset. IEEE Access, vol. 8, pp. 165263-165284, 2020. DOI: 10.1109/ACCESS.2020.3022633.
25. Rodrıguez-Barroso N., Stipcich G., Jimenez-Lopez D., Ruiz-Millan J.A., Martınez-Camara E., Gonzalez-Seco G., M. Luzon V., Veganzones M., and Herrera F. Federated learning and differential privacy: Software tools analysis, the sherpa.ai fl framework and methodological guidelines for preserving data privacy. Information Fusion, 64:270–292, 2020. ISSN 1566-2535. DOI: 10.1016/j.inffus.2020.07.009.
26. Sarhan M., Lo W.W., Layeghy S., and Portmann M. Hbfl: A hierarchical blockchain-based federated learning framework for a collaborative IoT intrusion detection, 2022. URL:https://arxiv.org/abs/2204.04254 (accessed on: 20.08.2023).
27. Moustafa N. The BoT-IoT dataset, 2019. URL https://dx.doi.org/10.21227/r7v2-x988 (accessed on: 20.08.2023).
28. Abdel-Basset M., Moustafa N., Hawash H., Razzak I., Sallam K., and Elkomy O. Federated intrusion detection in blockchain-based

smart transportation systems. IEEE Transactions on Intelligent Transportation Systems, 23(3):2523–2537, 2022. DOI: 10.1109/TITS.2021.3119968.
29. Liu H., Zhang S., Zhang P., Zhou X., Shao X., Pu G., and Zhang Y. Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. IEEE Transactions on Vehicular Technology, 70(6):6073–6084, 2021. DOI: 10.1109/TVT.2021.3076780.
30. Chai H., Leng S., Chen Y., and Zhang K. A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 22(7):3975–3986, jul 2021. ISSN 1524-9050. DOI: 10.1109/TITS.2020.3002712.
31. Novikova E., Doynikova E., and Golubev S. Federated learning for intrusion detection in the critical infrastructures: Vertically partitioned data use case. Algorithms, 15(4), 2022. ISSN 1999-4893. DOI: 10.3390/a15040104.
32. Saputra F.A., Salman M., Hasim J.N., Nadhori I.U., Ramli K. The next-generation NIDS platform: Cloud-based snort NIDS using containers and big data. Big Data and Cognitive Computing, 6(1), 2022. ISSN 2504-2289. DOI: 10.3390/bdcc6010019.
33. Gong C., Zheng Z., Wu F., Shao Y., Li B., and Chen G. To store or not? online data selection for federated learning with limited storage. Proc. of the ACM Web Conference 2023, WWW '23, page 3044–3055, New York, NY, USA, 2023. Association for Computing Machinery. ISBN 9781450394161. DOI: 10.1145/3543507.3583426.
34. Jiang C., Xia C., Liu Z., and Wang T. Feddroidmeter: A privacy risk evaluator for fl- based android malware classification systems. Entropy, 25(7), 2023. ISSN 1099-4300. DOI: 10.3390/e25071053..
35. Blanchard P., El Mhamdi E.M., Guerraoui R., and Stainer J. Machine learning with adversaries: Byzantine tolerant gradient descent. Proc. of the 31st International Conference on Neural Information Processing Systems, NIPS'17, pp.118–128, Red Hook, NY, USA, 2017. Curran Associates Inc. ISBN 9781510860964.
36. Yin D., Chen Y., Kannan R., and Bartlett P. Byzantine-robust distributed learning: Towards optimal statistical rates. Proc. of the 35th International Conference on Machine Learning, volume 80 of Proceedings of Machine Learning Research, pp.5650–5659. PMLR, 10–15 Jul 2018.
37. Cao X., Fang M., Liu J., and Gong N.J. Fltrust: Byzantine-robust federated learning via trust bootstrapping. CoRR, abs/2012.13995, 2020. URL: https://arxiv.org/abs/2012.13995. (accessed on: 20.08.2023).
38. Flower — a friendly framework for federated learning. URL https://flower.dev/. (accessed on: 20.08.2023).
39. Li X., Jiang M., Zhang X., Kamp M., and Dou Q.. Fedbn: Federated learning on non-iid features via local batch normalization. CoRR, abs/2102.07623, 2021. (accessed on: 20.08.2023).
40. Reddi S.J., Charles Z., Zaheer M., Garrett Z., Rush K., Konecny J., Kumar S., and McMahan H.B. Adaptive federated optimization. CoRR, abs/2003.00295, 2020. (accessed on: 20.08.2023).
41. Yin D., Chen Y., Ramchandran K., Bartlett P.L. Byzantine-Robust Distributed Learning: Towards Optimal Statistical Rates. International Conference on Machine Learning. 2018. URL: https://api.semanticscholar.org/CorpusID:3708326 (accessed on: 20.08.2023).
42. Novikova E., Fedorchenko E., Kotenko I.., Kholod I. [Analytical Review of Intelligent Intrusion Detection Systems Based on Federated Learning: Advantages and Open Challenges] Аналитический обзор подходов к обнаружению вторжений, основанных на федеративном обучении: преимущества использования и открытые задачи. Informatics and Automation [Информатика и автоматизация]. 2023. No 22 (5). pp.1034–1082. DOI: DOI:10.15622/ia.22.5.4 (in Russian)

МЕТОДИКА ОЦЕНИВАНИЯ ИНФОРМАЦИОННОЙ УСТОЙЧИВОСТИ ГЕТЕРОГЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

Коноваленко С.А.[1]

Цель исследования: *определение уточненного семантического значения, показателя и критерия оценивания информационной устойчивости процесса функционирования гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также формирование на их основе целенаправленной последовательности действий для получения количественной оценки рассматриваемого аспекта устойчивости.*

Метод исследования: *системный анализ, системно-динамическое моделирование с использованием алгебраических выражений и логических условий.*

Результаты исследования: *определена необходимость разработки научно-методического аппарата оценивания информационной устойчивости процесса функционирования гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на этапе ее эксплуатации в условиях деструктивных воздействий, направленных на нарушение ее процесса функционирования и доступности. Проведен анализ понятийного аппарата и выявлена терминологическая нечеткость в исследуемой предметной области. Сформировано уточненное семантическое значение, показатель и критерий оценивания информационной устойчивости процесса функционирования рассматриваемого объекта в заданных условиях эксплуатации. На основе представления заданного объекта оценивания в виде кибернетической системы и системно-динамической модели разработана система ключевых показателей и целенаправленная последовательность действий для получения количественной оценки текущего уровня рассматриваемого аспекта устойчивости. Предложены направления развития разработанного научно-методического аппарата оценивания информационной устойчивости процесса функционирования рассматриваемого объекта.*

Научная новизна *заключается в предоставлении теоретически обоснованного формализованного подхода к оцениванию информационной устойчивости процесса функционирования гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, позволяющего, в отличии от известных, сформировать научно-технологический задел для получения комплексной оценки устойчивости заданного объекта и реализации предлагаемых научно-технических решение на практике.*

Ключевые слова: *кибернетическая система, системно-динамическая модель, скорость изменения информационного ресурса, уязвимость, компьютерная атака, процедуры функционально-параметрического управления, нарушение процесса функционирования, нарушение доступности.*

DOI: 10.21681/2311-3456-2023-6-67-80

Введение

В настоящее время обеспечение информационной безопасности (ИБ) объектов критической информационной инфраструктуры (КИИ) достигается путем эффективного функционирования гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГетСОПКА) [1-3]. При этом, процесс функционирования (ПФ) объектов КИИ и ГетСОПКА, как средства обеспечения их безопасного применения, осуществляется в условиях [2, 3]:

— физических воздействий естественно-природных факторов окружающей среды, независимых от человека;

1 Коноваленко Сергей 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: konovalenko_rcf@mail.ru

— неумышленных воздействий, вызванных ошибками или халатностью деятельности человека;
— умышленных воздействий, вызванных действиями со стороны потенциального злоумышленника, в условиях вооруженного или информационного конфликта.

Указанные условия эксплуатации объектов КИИ и ГетСОПКА, имея естественную или искусственную природу происхождения, проявляются в виде деструктивных преднамеренных (ДПВ) или непреднамеренных (ДНПВ) воздействий, оказывающих негативное влияние на ПФ и доступность рассматриваемых объектов, тем самым переводя их в неустойчивое состояние, в котором они не обеспечивают решение поставленных перед ними задач [2-4]. В свою очередь, для компенсации негативных последствий ДПВ и ДНПВ, направленных на нарушение ПФ и доступности объектов КИИ, в структуре ГетСОПКА выделены источники событий ИБ (ИСИБ), образующие подсистему ИСИБ (ПИСИБ), и специализированные средства (СС), образующие центральную подсистему сбора, хранения и корреляции событий ИБ (ЦПСХКСИБ), которые в общем реализуют набор определенных функций по контролю состояния защищенности объектов КИИ, по сбору, хранению и анализу событий ИБ (СИБ) с целью обнаружения инцидентов ИБ (ИИБ) на объектах КИИ и принятия решений по ликвидации их последствий [4, 5]. Кроме того, наряду с ПИСИБ и ЦПСХКСИБ, в структуре ГетСОПКА не выделена отдельная подсистема централизованного управления ПФ ИСИБ (СС) на этапе их эксплуатации в условиях ДПВ и ДНПВ, направленных на нарушение их ПФ и доступности, но решение рассматриваемой задачи осуществляется специалистами по ИБ в «ручном» режиме при отсутствии реализованных на практике комплексных технических решений, способных обеспечить автоматизацию рассматриваемого процесса, что свидетельствует о недостаточном уровне эффективности ПФ данного объекта в выделенных условиях эксплуатации [4, 5]. Стоит заметить, что вышеуказанная проблемная ситуация в практике применения ГетСОПКА обусловила необходимость проведения всестороннего анализа теоретических основ в заданной предметной области, в результате которого установлено, что необходимо разработать новый научно-методический аппарат функционально-параметрического управления (ФПУ) ПФ ИСИБ (СС) с учетом особенностей их построения, режимов функционирования (РжФ) и выделенных условий эксплуатации [4]. При этом, разработка указанного научно-методического аппарата должна включать последовательный синтез таких процедур, как адаптивный контроль состояния ПФ и оценивание информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в заданных режимах и условиях функционирования, а также синтез и реализация информационно-технического решения (ИТР) на ФПУ ее ПФ. Учитывая вышеуказанное, а также, что в работах [6-8] был разработан научно-методический аппарат адаптивного контроля состояния ПФ ГетСОПКА в условиях ДПВ и ДНПВ, направленных на нарушение ее ПФ и доступности, в данной работе решается актуальная научно-техническая задача разработки научно-методического аппарата оценивания информационной устойчивости ПФ рассматриваемого объекта в выделенных условиях эксплуатации, что в общем может стать основой для построения подсистемы централизованного ФПУ (ПФПУ) ПФ рассматриваемого объекта [4].

Анализ теоретических основ реализации процедуры оценивания информационной устойчивости ПФ ГетСОПКА

Практика реализации процедуры оценивания информационной устойчивости ПФ сложных технических систем (СТС), к которым относится ГетСОПКА, свидетельствует о том, что в настоящее время отсутствует единый структурированный подход к пониманию семантического значения и к определению показателей рассматриваемого аспекта устойчивости [9-11].

В существующих исследованиях под информационной устойчивостью ПФ СТС понимают способность СТС в динамике информационного конфликта своевременно, достоверно и скрытно реализовывать информационный обмен (передавать данные) между своими структурными элементами и осуществлять управление ими с учетом деструктивных воздействий, направленных на нарушение ПФ элементов СТС [9, 10]. Анализируя существующую интерпретацию понятия «информационная устойчивость ПФ СТС», выделим его терминологическую нечеткость:

1. Полный цикл ПФ любого структурного элемента СТС представляется в виде последовательного выполнения определенных операций, завершающей из которых является операция передачи результатов своего функционирования в адрес очередного структурного элемента СТС [12]. Свойства, в частности, своевременность, достоверность и скрытность, которые определяют качество операции передачи данных между структурными элементами системы и, как следствие, поведение СТС в целом, относятся к группе функциональных (операционных) свойств [12]. Указанное является

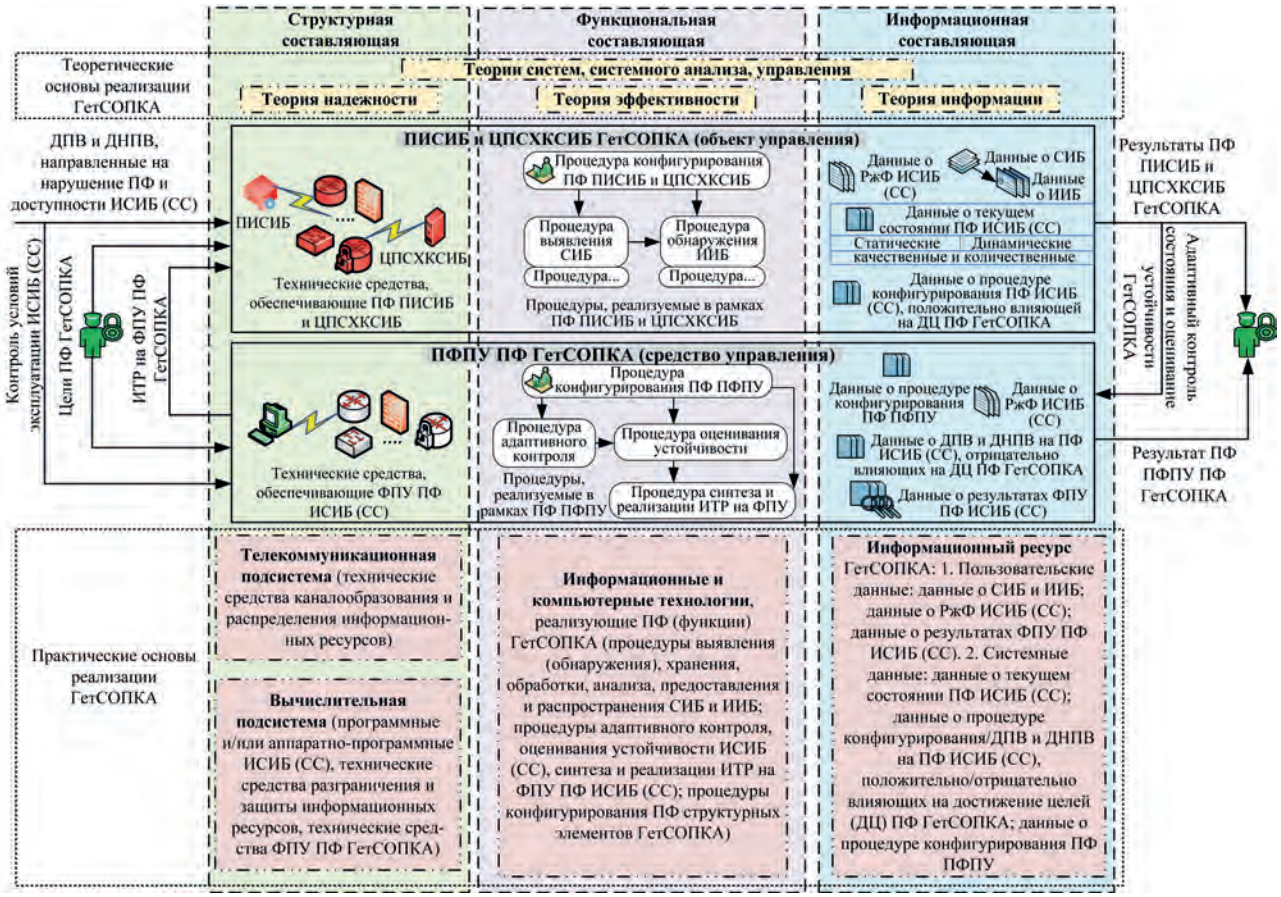

Рис. 1. Представление ГетСОПКА в виде кибернетической системы

свидетельством подмены понятий информационной и функциональной устойчивости ПФ СТС.

2. Оценивание информационной устойчивости ПФ СТС по степени управляемости структурными элементами СТС также не может в полной мере претендовать на адекватное решение так, как оба свойства «устойчивость» и «управляемость» одновременно являются общесистемными свойствами, определяющими принципиально разные аспекты качества ПФ СТС [12].

С учетом проведенного анализа понятийного аппарата и выявленной терминологической нечеткости в исследуемой предметной области возникает необходимость в уточнении семантического значения рассматриваемого понятия, а также определении его показателя и критерия оценивания с учетом особенностей построения ГетСОПКА, ее РжФ и условий эксплуатации.

Для определения семантического значения и показателя информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в заданном РжФ в условиях ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС), представим рассматриваемый объект в виде кибернетической системы (рис. 1) [9, 12, 13].

На рис. 1 ГетСОПКА описывается с трех точек зрения:

1. Структурная составляющая ГетСОПКА, представляющая собой совокупность разнотипных технических средств, с одной стороны входящих в состав телекоммуникационной или вычислительной подсистем рассматриваемой системы, а с другой стороны обеспечивающих реализацию ПФ объекта (ПИСИБ и ЦПСХКСИБ) и средства (ПФПУ) управления.

2. Функциональная составляющая ГетСОПКА, представляющая собой совокупность определенных процедур, выполняемых в рамках применяемых информационных и компьютерных технологий, реализующих ПФ объекта (ПИСИБ и ЦПСХКСИБ) и средства (ПФПУ) управления.

3. Информационная составляющая ГетСОПКА, представляющая собой совокупность пользовательских и системных данных, образующих информационный ресурс рассматриваемой системы, а также отражающих степень достижения целей и разнообразные свойства объекта (ПИСИБ и ЦПСХКСИБ) и средства (ПФПУ) управления на этапе их эксплуатации в штатном (ШРФ), усиленном (УРФ) или боевом (БРФ) РжФ при ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС).

Далее заметим, что в рамках данной работы рассмотрение структурной и функциональной составляющих ГетСОПКА и, как следствие, структурной и функциональной устойчивости ПФ рассматриваемого объекта в заданных режимах и условиях эксплуатации не предусмотрено.

Таким образом, основываясь на представлении рассматриваемого объекта в виде кибернетической системы (рис. 1), а в частности на его информационной составляющей, следует принять, что:

- под информационной устойчивостью ПФ ГетСОПКА понимается свойство ПФ ГетСОПКА, определяющее способность ПИСИБ и ЦПСХКСИБ на этапе их эксплуатации в произвольном (ζ) РжФ сохранять требуемый уровень информационного равновесия между факторами, положительно и отрицательно влияющими на достижение требуемого целевого эффекта (результата) их ПФ;
- показателем информационной устойчивости ПФ ГетСОПКА является скорость изменения набора (количества) данных (параметров) конфигурации (настройки) ПФ ПИСИБ и ЦПСХКСИБ в ζ-м РжФ при ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС) ($dY_{\zeta}^{\text{сопка/пдк}} / dt$);
- критерием оценивания информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в ζ-м РжФ при ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС), является:

$$dY_{\zeta}^{\text{сопка/пдк}} / dt \geq dY_{\zeta}^{\text{сопка/пдк/тр}} / dt \Big| \left(dY_{\zeta}^{\text{сопка/пдк/тр}} / dt\right) \geq 0, \ \zeta = \overline{1,3}, \quad (1)$$

где $dY_{\zeta}^{\text{сопка/пдк/тр}} / dt$ – допустимое значение скорости изменения набора (количества) данных (параметров) конфигурации (настройки) ПФ ПИСИБ и ЦПСХКСИБ в ζ-м РжФ, характеризующее требуемый уровень информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в условиях ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС);
$\zeta=1$, $\zeta=2$, $\zeta=3$ – соответственно ШРФ, УРФ, и БРФ ГетСОПКА.

Системно-динамическая модель ГетСОПКА

При оценивании информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в ζ-м РжФ при ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ИСИБ (СС), необходимо четко понимать особенности динамики ПФ рассматриваемого объекта и выделять множество факторов, положительно и отрицательно влияющих на достижение требуемого целевого эффекта (результата) его ПФ. В настоящее время наиболее адекватным методом, позволяющим обеспечить решение вышеуказанной задачи, является метод системно-динамического моделирования, которой направлен на изучение сложных динамических систем посредством исследования их состояния во времени в зависимости от особенностей построения их структурных элементов, взаимодействия между ними и влияния на них различного рода воздействий внешней среды и внутренних процессов [14, 15]. В основе метода системно-динамического моделирования находятся:

- системная потоковая диаграмма, строящаяся на основе типовых символов, представленных в табл. 1;
- система дифференциальных уравнений, которые позволяют рассчитать и представить в количественном выражении динамические изменения, происходящие в системе.

Далее на основе методологии системно-динамического моделирования рассмотрим ГетСОПКА как динамическую систему и представим ее с использованием системной потоковой диаграммы (рис. 2) [4, 14, 15].

Стоит еще раз отметить, что представление ГетСОПКА в виде кибернетической системы (рис. 1) и системно-динамической модели (рис. 2) возможно использовать не только для оценивания информационной устойчивости ПФ рассматриваемого объекта в заданных режимах и условиях эксплуатации, но и для оценивания ее структурной и функциональной устойчивости, порядок выполнения которого не приводится в данной работе в силу ранее введенного ограничения, связанного с рассмотрением только информационной составляющей ГетСОПКА.

С учетом системной потоковой диаграммы, описывающей системно-динамическую модель заданного объекта (рис. 2), а также особенностей его построения, как кибернетической системы (рис. 1), расчет текущего значения $dY_{\zeta}^{\text{сопка/пдк}} / dt$ выполним посредством аналитических методов (дифференциальных уравнений, алгебраических выражений и логических условий) при следующих общих допущениях [7, 16]:

- в состав ПИСИБ включено определенное ($\mu^{\text{писиб}}$) количество произвольных ($\rho^{\text{исиб}} = \overline{1, \mu^{\text{писиб}}}$) ИСИБ, а в состав ЦПСХКСИБ – определенное ($\varepsilon^{\text{цпсхксиб}}$) количество произвольных ($\varphi^{\text{сс}} = \overline{1, \varepsilon^{\text{цпсхксиб}}}$) СС;

Таблица 1.

Типовые символы, используемые в системной потоковой диаграмме

Графическое обозначение символа	Наименование символа	Назначение символа
	Уровень	Характеризует накопления внутри системы, возникающие в результате разности между входящими и исходящими потоками
	Темп	Обозначает скорость потока между уровнями в системе
	Потоковая связь	Соединяет уровни с уровнями, с истоками и стоками
	Информационная связь	Отражает информационные связи диаграммы
	Облако	Обозначает истоки и стоки потоков, которые не рассматриваются в модели
	Вспомогательная переменная	Специальный множитель (некоторая функция), влияющий на изменения моделируемых факторов

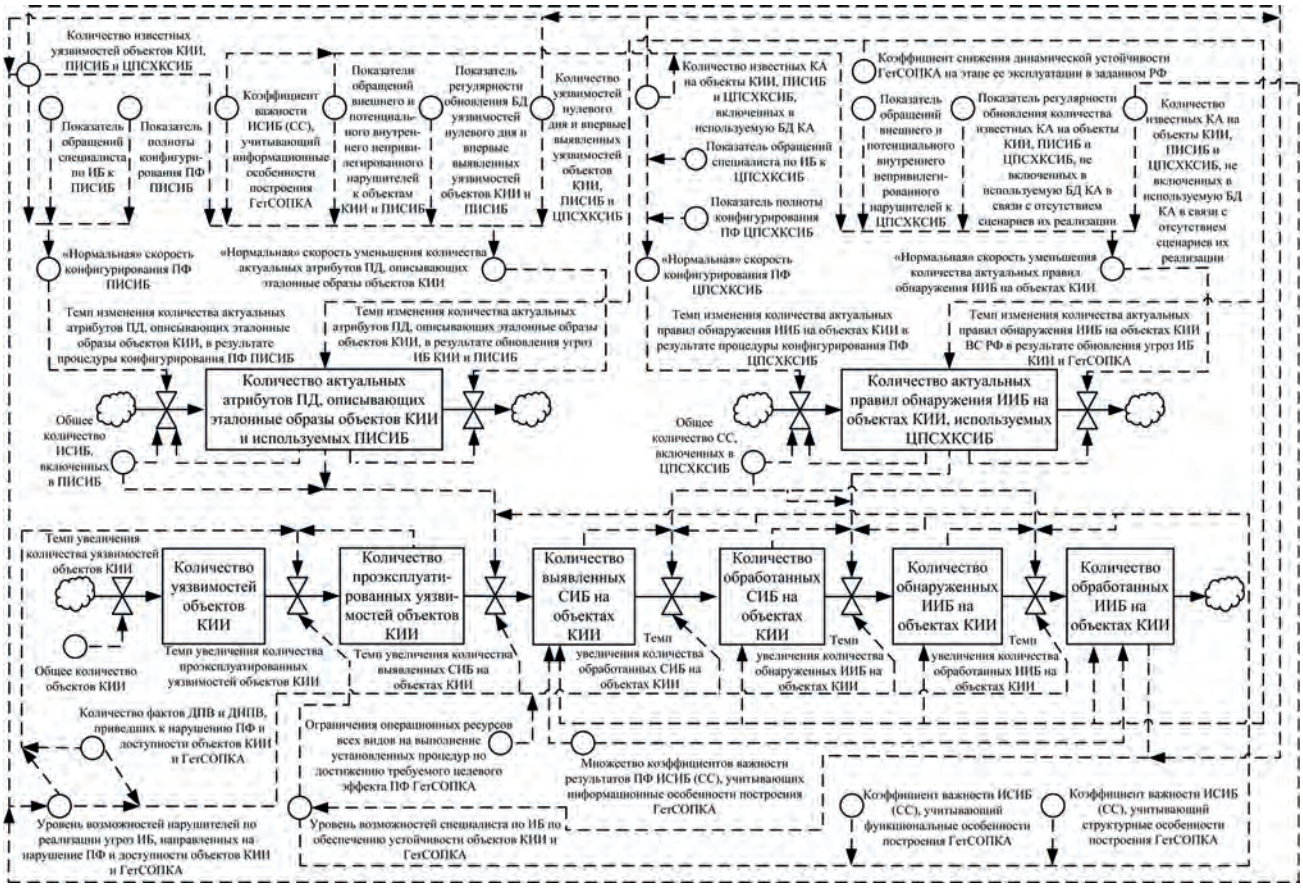

Рис. 2. Системная потоковая диаграмма, описывающая системно-динамическую модель ГетСОПКА

– ПФ $\rho^{\text{исиб}}$ направлен на выявление СИБ на определенных (контролируемых им) объектах КИИ и реализуется посредством контроля текущих значений атрибутов параметрических данных (ПД), описывающих эталонные образы соответствующих объектов;

– ПФ $\varphi^{\text{сс}}$ направлен на обнаружение ИИБ на определенных (контролируемых им) объектах КИИ и реализуется посредством автоматической обработки соответствующих СИБ, предоставляемых $\rho^{\text{исиб}}$, автоматического обнаружения ИИБ на основе применения предварительно заданных правил корреляции обработанных СИБ, а также с последующей обработкой обнаруженных ИИБ, в результате которой автоматически формируются соответствующие карточки ИИБ.

В дополнение к указанным общим допущениям для расчета текущего значения $dY_{\zeta}^{\text{сопка/пдк}} / dt$ введем следующие частные допущения:

1. Условно обозначим элементы системно-динамической модели ГетСОПКА (рис. 2), используемые при расчете текущего значения $dY_{\zeta}^{\text{сопка/пдк}} / dt$, в виде:

$Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ – количество актуальных атрибутов ПД, описывающих эталонные образы определенных объектов КИИ и используемых $\rho^{\text{исио}}$ на этапе его эксплуатации в ζ-м РжФ (единица измерения (ед. изм.) – число актуальных атрибутов ПД);

$Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ – количество актуальных правил обнаружения ИИБ на определенных объектах КИИ, используемых $\varphi^{\text{сс}}$ на этапе его эксплуатации в ζ-м РжФ (ед. изм. – число актуальных правил обнаружения ИИБ);

$IY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$, $BY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ – соответственно темп изменения $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ в результате процедуры конфигурирования ПФ $\rho^{\text{исиб}}$ и обновления угроз ИБ для определенных объектов КИИ и $\rho^{\text{исиб}}$ в ζ-м его РжФ (ед. изм. – число актуальных атрибутов ПД/ $\tau^{\text{оиу}}$, где $\tau^{\text{оиу}}$ – произвольный момент времени оценивания информационной устойчивости ПФ ГетСОПКА);

$DY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$, $PY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ – соответственно темп изменения $Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ в результате процедуры конфигурирования ПФ $\varphi^{\text{сс}}$ и обновления угроз ИБ для определенных объектов КИИ, $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – число актуальных правил обнаружения ИИБ/ $\tau^{\text{оиу}}$);

$\alpha_{\zeta}^{\rho^{\text{исио}}/\text{нск}}$, $\alpha_{\zeta}^{\varphi^{\text{сс}}/\text{нск}}$ – соответственно «нормальная» скорость конфигурирования ПФ $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ на этапе их эксплуатации в ζ-м РжФ (ед. изм. – соответственно число частей актуальных атрибутов ПД/ $\tau^{\text{оиу}}$ и число частей актуальных правил обнаружения ИИБ/ $\tau^{\text{оиу}}$);

$o_{\zeta}^{\rho^{\text{исио}}/\text{нсу}}$, $o_{\zeta}^{\varphi^{\text{сс}}/\text{нсу}}$ – соответственно «нормальная» скорость уменьшения $Y_{\zeta}^{\rho^{\text{исио}}/\text{пдк}}$ и $Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ (ед. изм. – соответственно число частей актуальных атрибутов ПД/ $\tau^{\text{оиу}}$ и число частей актуальных правил обнаружения ИИБ/ $\tau^{\text{оиу}}$);

$\delta_{\zeta_{\text{окии}}^{\text{киу}}}^{\rho^{\text{исиб}}}$, $\psi_{\zeta_{\text{окии}}^{\text{ика}}}^{\varphi^{\text{сс}}}$ – соответственно общее количество известных уязвимостей и компьютерных атак (КА) на объекты КИИ, контролируемые $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – соответственно число известных уязвимостей и число известных КА, включенных в используемые базы данных (БД);

$\beta_{\zeta}^{\rho^{\text{исиб}}/\text{пос}}$, $\beta_{\zeta}^{\varphi^{\text{сс}}/\text{пос}}$ – соответственно показатель обращений специалиста по ИБ к $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – безразмерная величина);

$\nu_{\zeta}^{\rho^{\text{исиб}}/\text{ппк}}$, $\nu_{\zeta}^{\varphi^{\text{сс}}/\text{ппк}}$ – соответственно показатель полноты процедуры конфигурирования ПФ $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – безразмерная величина);

$k_{\zeta}^{\rho^{\text{исиб}}/\text{виу}}$, $k_{\zeta}^{\varphi^{\text{сс}}/\text{виу}}$ – соответственно коэффициент важности $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ, учитывающий информационные особенности построения ГетСОПКА, в частности объем передаваемого $\rho^{\text{исиб}}$ в адрес $\varphi^{\text{сс}}$ и принимаемого $\varphi^{\text{сс}}$ от $\rho^{\text{исиб}}$, $\rho^{\text{исиб}} = \overline{1,\ \mu^{\text{писиб}}}$, сетевого трафика с результатами (информацией о состоянии определенных объектов КИИ) его ПФ (ед. изм. – безразмерная величина) [16];

$\omega_{\zeta_{\text{окии}}^{\text{пон}}}^{\rho^{\text{исиб}}}$, $\omega_{\zeta}^{\rho^{\text{исиб}}/\text{пон}}$, $\omega_{\zeta}^{\varphi^{\text{сс}}/\text{пон}}$ – соответственно показатель обращений внешнего и потенциального внутреннего непривилегированного нарушителей к определенным (контролируемым $\rho^{\text{исиб}}$) объектам КИИ, к $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – безразмерная величина);

$\gamma_{\zeta}^{\rho^{\text{исиб}}/\text{ронву}}$ – показатель регулярности обновления БД уязвимостей нулевого дня и впервые выявленных уязвимостей определенных (контролируемых $\rho^{\text{исиб}}$) объектов КИИ и $\rho^{\text{исиб}}$ в ζ-м его РжФ (ед. изм. – безразмерная величина);

$\vartheta_{\zeta_{\text{окии}}^{\text{кнву}}}^{\rho^{\text{исиб}}}$, $\vartheta_{\zeta}^{\rho^{\text{исиб}}/\text{кнву}}$ – соответственно количество уязвимостей нулевого дня и впервые выявленных уязвимостей определенных (контролируемых $\rho^{\text{исиб}}$) объектов КИИ и $\rho^{\text{исиб}}$ в ζ-м его РжФ, которые могли быть проэксплуатированы внешним и потенциальным внутренним непривилегированным нарушителем за интервал времени $\left[\tau^{\text{оиу}} - 1, \tau^{\text{оиу}}\right]$ (ед. изм. – число уязвимостей нулевого дня и впервые выявленных/ $\tau^{\text{оиу}}$);

$k_{\zeta}^{\text{сопка/снду}}$ – коэффициент снижения динамической (информационной) устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в ζ-м РжФ, значение кото-

рого определяется на основе подходов, описанных в [16] (ед. изм. – безразмерная величина);

$\gamma_{\zeta}^{\varphi^{cc}/\text{роика}}$ – показатель регулярности обновления количество известных КА на определенные (контролируемые $\rho^{\text{исиб}}$) объекты КИИ, на $\rho^{\text{исиб}}$ (взаимодействующие с φ^{cc}) и на φ^{cc} в ζ-м их РжФ, не включенных в используемую БД КА в связи с отсутствием сценариев их реализации (ед. изм. – безразмерная величина);

$h_{\zeta_{\text{окии}}^{\text{ика}}}^{\rho^{\text{исиб}}}$, $h_{\zeta}^{\rho^{\text{исиб}}/\text{ика}}$, $h_{\zeta}^{\varphi^{cc}/\text{ика}}$ – соответственно количество известных КА на определенные (контролируемые $\rho^{\text{исиб}}$) объекты КИИ, на $\rho^{\text{исиб}}$ (взаимодействующие с φ^{cc}) и на φ^{cc} в ζ-м их РжФ, не включенных в используемую БД КА в связи с отсутствием сценариев их реализации и которые могли быть проведены внешним и потенциальным внутренним непривилегированным нарушителем за интервал времени $\left[\tau^{\text{оиу}}-1,\tau^{\text{оиу}}\right]$ (ед. изм. – число известных КА, не включенных в используемую БД КА/ $\tau^{\text{оиу}}$).

2. Специалист по ИБ на этапах подготовки и непосредственной эксплуатации ГетСОПКА, реализуя процедуру конфигурирования ПФ $\rho^{\text{исиб}}$ и φ^{cc}, под каждую отдельную (произвольную) известную уязвимость и КА на определенные объекты КИИ, принадлежащие $\delta_{\zeta_{\text{окии}}^{\text{киу}}}^{\rho^{\text{исиб}}}$ и $\psi_{\zeta_{\text{окии}}^{\text{ика}}}^{\varphi^{cc}}$, соответственно выделяет один актуальный атрибут ПД, принадлежащий $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$, и формирует одно актуальное правило обнаружения ИИБ, принадлежащее $Y_{\zeta}^{\varphi^{cc}/\text{пдк}}$.

3. Значения $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ и $Y_{\zeta}^{\varphi^{cc}/\text{пдк}}$ могут соответствовать или быть меньше фактического (хранящегося в конфигурационных файлах $\rho^{\text{исиб}}$ и φ^{cc}) количества атрибутов ПД, описывающих эталонные образы определенных объектов КИИ, и правил обнаружения ИИБ на определенных объектах КИИ.

Методика оценивания информационной устойчивости ПФ ГетСОПКА

С учетом общих и частных допущений, введенных при построении системно-динамической модели ГетСОПКА (рис. 2), определим текущий уровень информационной устойчивости ПФ $\rho^{\text{исиб}}$ и φ^{cc} в $\tau^{\text{оиу}}$ момент времени на этапе их эксплуатации в ζ-м РжФ при ДПВ и ДНПВ, направленных на нарушение их ПФ и доступности, посредством расчета текущих значений скоростей изменения $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ и $Y_{\zeta}^{\varphi^{cc}/\text{пдк}}$ (соответственно $dY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}/d\tau^{\text{оиу}}$ и $dY_{\zeta}^{\varphi^{cc}/\text{пдк}}/d\tau^{\text{оиу}}$) в виде:

$$
\begin{cases}
\dfrac{dY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}}{d\tau^{\text{оиу}}}=k_{\zeta}^{\text{сопка/снду}}\cdot\left(IY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}})-BY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}})\right);\\
IY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}})=\alpha_{\zeta}^{\rho^{\text{исиб}}/\text{нск}}(\tau^{\text{оиу}})\cdot Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}}-1);\\
BY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}})=o_{\zeta}^{\rho^{\text{исиб}}/\text{нсу}}(\tau^{\text{оиу}})\cdot Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}}-1);\\
\alpha_{\zeta}^{\rho^{\text{исиб}}/\text{нск}}(\tau^{\text{оиу}})=1+\beta_{\zeta}^{\rho^{\text{исиб}}/\text{пос}}(\tau^{\text{оиу}})\cdot\nu_{\zeta}^{\rho^{\text{исиб}}/\text{ппк}}(\tau^{\text{оиу}})\cdot\dfrac{\delta_{\zeta_{\text{окии}}^{\text{двкиу}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}})}{\delta_{\zeta_{\text{окии}}^{\text{киу}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}}-1)};\\
o_{\zeta}^{\rho^{\text{исиб}}/\text{нсу}}(\tau^{\text{оиу}})=k_{\zeta}^{\rho^{\text{исиб}}/\text{виу}}(\tau^{\text{оиу}})\cdot\dfrac{\left(\begin{array}{l}\omega_{\zeta_{\text{окии}}^{\text{пон}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}})\cdot\vartheta_{\zeta_{\text{окии}}^{\text{кнву}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}})+\\+\omega_{\zeta}^{\rho^{\text{исиб}}/\text{пон}}(\tau^{\text{оиу}})\cdot\vartheta_{\zeta}^{\rho^{\text{исиб}}/\text{кнву}}(\tau^{\text{оиу}})\end{array}\right)}{\gamma_{\zeta}^{\rho^{\text{исиб}}/\text{ронву}}(\tau^{\text{оиу}})\cdot\delta_{\zeta_{\text{окии}}^{\text{киу}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}}-1)};\\
\zeta=\overline{1,3},\ \rho^{\text{исиб}}=\overline{1,\mu^{\text{писиб}}},
\end{cases}
\tag{2}
$$

$$\begin{cases} \dfrac{dY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}}{d\tau^{\text{оиу}}} = k_{\zeta}^{\text{сопка/снду}} \cdot \left(DY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}}) - PY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}}) \right); \\ DY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}}) = \alpha_{\zeta}^{\varphi^{\text{сс}}/\text{нск}}(\tau^{\text{оиу}}) \cdot Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}} - 1); \\ PY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}}) = o_{\zeta}^{\varphi^{\text{сс}}/\text{нсу}}(\tau^{\text{оиу}}) \cdot Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}} - 1); \\ \alpha_{\zeta}^{\varphi^{\text{сс}}/\text{нск}}(\tau^{\text{оиу}}) = 1 + \beta_{\zeta}^{\varphi^{\text{сс}}/\text{пос}}(\tau^{\text{оиу}}) \cdot \nu_{\zeta}^{\varphi^{\text{сс}}/\text{ппк}}(\tau^{\text{оиу}}) \cdot \dfrac{\psi_{\zeta_{\text{окии}}^{\text{двика}}}^{\varphi^{\text{сс}}}(\tau^{\text{оиу}})}{\psi_{\zeta_{\text{окии}}^{\text{ика}}}^{\varphi^{\text{сс}}}(\tau^{\text{оиу}} - 1)}; \\ o_{\zeta}^{\varphi^{\text{сс}}/\text{нсу}}(\tau^{\text{оиу}}) = k_{\zeta}^{\varphi^{\text{сс}}/\text{виу}}(\tau^{\text{оиу}}) \cdot \dfrac{\left(\begin{array}{l} \omega_{\zeta_{\text{окии}}^{\text{пон}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}}) \cdot h_{\zeta_{\text{окии}}^{\text{ика}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}}) + \omega_{\zeta}^{\rho^{\text{исиб}}/\text{пон}}(\tau^{\text{оиу}}) \cdot \\ \cdot h_{\zeta}^{\rho^{\text{исиб}}/\text{ика}}(\tau^{\text{оиу}}) + \omega_{\zeta}^{\varphi^{\text{сс}}/\text{пон}}(\tau^{\text{оиу}}) \cdot h_{\zeta}^{\varphi^{\text{сс}}/\text{ика}}(\tau^{\text{оиу}}) \end{array} \right)}{\gamma_{\zeta}^{\varphi^{\text{сс}}/\text{роика}}(\tau^{\text{оиу}}) \cdot \psi_{\zeta_{\text{окии}}^{\text{ика}}}^{\varphi^{\text{сс}}}(\tau^{\text{оиу}} - 1)}; \\ \zeta = \overline{1,3},\ \rho^{\text{исиб}} = \overline{1, \mu^{\text{писиб}}},\ \varphi^{\text{сс}} = \overline{1, \varepsilon^{\text{цпсхксиб}}}, \end{cases} \tag{3}$$

где $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}(\tau^{\text{оиу}} - 1)$, $Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}(\tau^{\text{оиу}} - 1)$ – соответственно значение $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$ и $Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ в момент времени $(\tau^{\text{оиу}} - 1)$, предшествующий $\tau^{\text{оиу}}$;

$\delta_{\zeta_{\text{окии}}^{\text{двкиу}}}^{\rho^{\text{исиб}}}$, $\psi_{\zeta_{\text{окии}}^{\text{двика}}}^{\varphi^{\text{сс}}}$ – соответственно количество известных уязвимостей и КА на объекты КИИ, контролируемые $\rho^{\text{исиб}}$ и $\varphi^{\text{сс}}$ в ζ-м их РжФ, дополнительно включенных в используемые БД за интервал времени $\left[\tau^{\text{оиу}} - 1, \tau^{\text{оиу}}\right]$ (ед. изм. – соответственно число известных уязвимостей/ $\tau^{\text{оиу}}$ и число известных КА/ $\tau^{\text{оиу}}$);

$\delta_{\zeta_{\text{окии}}^{\text{киу}}}^{\rho^{\text{исиб}}}(\tau^{\text{оиу}} - 1)$, $\psi_{\zeta_{\text{окии}}^{\text{ика}}}^{\varphi^{\text{сс}}}(\tau^{\text{оиу}} - 1)$ – соответственно значение $\delta_{\zeta_{\text{окии}}^{\text{двкиу}}}^{\rho^{\text{исиб}}}$ и $\psi_{\zeta_{\text{окии}}^{\text{двика}}}^{\varphi^{\text{сс}}}$ в момент времени $(\tau^{\text{оиу}} - 1)$, предшествующий $\tau^{\text{оиу}}$.

В целях решения (2, 3) и сокращения количества используемых аналитических выражений и логических условий введем следующие условные обозначения: $\beta_{\zeta}^{g/\text{пос}}$ – показатель, соответствующий $\beta_{\zeta}^{\rho^{\text{исиб}}/\text{пос}}$, либо $\beta_{\zeta}^{\varphi^{\text{сс}}/\text{пос}}$; $\nu_{\zeta}^{g/\text{ппк}}$ – показатель, соответствующий $\nu_{\zeta}^{\rho^{\text{исиб}}/\text{ппк}}$, либо $\nu_{\zeta}^{\varphi^{\text{сс}}/\text{ппк}}$; $k_{\zeta}^{g/\text{виу}}$ – коэффициент, соответствующий $k_{\zeta}^{\rho^{\text{исиб}}/\text{виу}}$, либо $k_{\zeta}^{\varphi^{\text{сс}}/\text{виу}}$; $\omega_{\zeta}^{g/\text{пон}}$ – показатель, соответствующий $\omega_{\zeta_{\text{окии}}^{\text{пон}}}^{\rho^{\text{исиб}}}$, либо $\omega_{\zeta}^{\rho^{\text{исиб}}/\text{пон}}$, либо $\omega_{\zeta}^{\varphi^{\text{сс}}/\text{пон}}$; $\gamma_{\zeta}^{g/\text{ро}}$ – показатель, соответствующий $\gamma_{\zeta}^{\rho^{\text{исиб}}/\text{ронву}}$, либо $\gamma_{\zeta}^{\varphi^{\text{сс}}/\text{роика}}$; $\vartheta_{\zeta}^{g/\text{кнву}}$ – количество, соответствующее $\vartheta_{\zeta_{\text{окии}}^{\text{кнву}}}^{\rho^{\text{исиб}}}$, либо $\vartheta_{\zeta}^{\rho^{\text{исиб}}/\text{кнву}}$; $h_{\zeta}^{g/\text{ика}}$ – количество, соответствующее $h_{\zeta_{\text{окии}}^{\text{ика}}}^{\rho^{\text{исиб}}}$, либо $h_{\zeta}^{\rho^{\text{исиб}}/\text{ика}}$, либо $h_{\zeta}^{\varphi^{\text{сс}}/\text{ика}}$.

Затем определим значения $\beta_{\zeta}^{g/\text{пос}}$, $\nu_{\zeta}^{g/\text{ппк}}$, $k_{\zeta}^{g/\text{виу}}$, $\omega_{\zeta}^{g/\text{пон}}$, $\gamma_{\zeta}^{g/\text{ро}}$, $\vartheta_{\zeta}^{g/\text{кнву}}$, $h_{\zeta}^{g/\text{ика}}$ в виде:

$$\beta_{\zeta}^{g/\text{пос}}(\tau^{\text{оиу}}) = \begin{cases} 1, \ \exists \left[\begin{array}{l} \left(\mathcal{J}_{\zeta}^{g/\text{кос}}(\tau^{\text{оиу}}) > 0 \right) \wedge \\ \wedge \left(\mathcal{X}_{\zeta_{\text{окии}}}^{g/\text{всо}}(\tau^{\text{оиу}}) = \mathcal{X}_{\zeta_{\text{окии}}}^{g/\text{во}}(\tau^{\text{оиу}}) \right) \end{array} \right]; \\ 0, \text{ иначе}, \end{cases} \tag{4}$$

$$\zeta = \overline{1,3},\ g = \overline{1,D},$$

где $\mathcal{J}_{\zeta}^{g/\text{кос}}$ – количество фактов (случаев) обращений специалиста по ИБ в интервале времени $\left[\tau^{\text{оиу}} - 1, \tau^{\text{оиу}}\right]$ к $\rho^{\text{исиб}}$, либо $\varphi^{\text{сс}}$ в целях конфигурирования их ПФ в ζ-м их РжФ (ед. изм. – число фак-

тов обращений специалиста по ИБ);

$\mathcal{X}_{\zeta_{\text{окии}}}^{g/\text{всо}}$, $\mathcal{X}_{\zeta_{\text{окии}}}^{g/\text{во}}$ – соответственно количество выполненных специалистом по ИБ и выпущенных соответствующим разработчиком обновлений БД известных уязвимостей объектов КИИ, либо обновлений используемой БД известных КА на объекты КИИ, контролируемые $\rho^{\text{исиб}}$, либо $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – соответственно число выполненных и выпущенных обновлений);

D – общее количество ИСИБ (СС), включенных в состав ГетСОПКА, причем $\mu^{\text{писиб}}+\varepsilon^{\text{цпсхксиб}}=D$;

$$\nu_{\zeta}^{g/\text{ппк}}(\tau^{\text{оиу}})=$$

$$\begin{cases} 1, \text{ при } \tau^{\text{оиу}}\geq\tau^{\text{окпк}}; \\ 0, \text{ при } \left[\left(\tau^{\text{оиу}}=\tau^{\text{оквсо}}\right)\vee\left(\tau^{\text{оквсо}}=\tau^{\text{окпк}}\right)\right]; \\ 1-\dfrac{\tau^{\text{окпк}}-\tau^{\text{оиу}}}{\tau^{\text{окпк}}-\tau^{\text{оквсо}}}, \text{ при } \tau^{\text{оквсо}}<\tau^{\text{оиу}}<\tau^{\text{окпк}}, \end{cases} \quad (5)$$

$$\zeta=\overline{1,3},\ g=\overline{1,D},$$

где $\tau^{\text{оквсо}}$ – момент времени окончания выполнения специалистом по ИБ всего количества обновлений БД известных уязвимостей объектов КИИ, либо обновлений используемой БД известных КА на объекты КИИ, контролируемые $\rho^{\text{исиб}}$, либо $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – в заданных единицах времени);

$\tau^{\text{окпк}}$ – момент времени окончания выполнения процедуры конфигурирования ПФ $\rho^{\text{исиб}}$, либо $\varphi^{\text{сс}}$ в ζ-м их РжФ, который определим в виде (ед. изм. – в заданных единицах времени):

$$\tau^{\text{окпк}}=\tau^{\text{оквсо}}+\bar{t}_{\zeta_{\text{окии}}}^{g/\text{одв}}\cdot\mathcal{L}_{\zeta_{\text{окии}}}^{g/\text{дв}}(\tau^{\text{оиу}}),$$
$$\zeta=\overline{1,3},\ g=\overline{1,D}, \quad (6)$$

где $\bar{t}_{\zeta_{\text{окии}}}^{g/\text{одв}}$ – среднее время, затрачиваемое специалистом по ИБ на обработку отдельной (произвольной) известной уязвимости, либо известной КА на определенные объекты КИИ, принадлежащих $\delta_{\zeta_{\text{двкиу}}\zeta_{\text{окии}}}^{\rho^{\text{исиб}}}$, либо $\psi_{\zeta_{\text{двика}}\zeta_{\text{окии}}}^{\varphi^{\text{сс}}}$, а также на выделение одного соответствующего актуального атрибута ПД, принадлежащего $Y_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}$, либо на формирование одного соответствующего актуального правила обнаружения ИИБ, принадлежащего $Y_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}$ (ед. изм. – в заданных единицах времени);

$\mathcal{L}_{\zeta_{\text{окии}}}^{g/\text{дв}}$ – число известных уязвимостей определенных объектов КИИ, либо известных КА на определенные объекты КИИ, образующих $\delta_{\zeta_{\text{двкиу}}\zeta_{\text{окии}}}^{\rho^{\text{исиб}}}$, либо $\psi_{\zeta_{\text{двика}}\zeta_{\text{окии}}}^{\varphi^{\text{сс}}}$;

$$k_{\zeta}^{g/\text{виу}}(\tau^{\text{оиу}})=\frac{\mathcal{I}_{\zeta}^{g/\text{ст}}(\tau^{\text{оиу}})}{\sum_{g=1}^{D}\mathcal{I}_{\zeta}^{g/\text{ст}}(\tau^{\text{оиу}})},$$
$$\zeta=\overline{1,3},\ g=\overline{1,D}, \quad (7)$$

где $\mathcal{I}_{\zeta}^{g/\text{ст}}$ – объем передаваемого $\rho^{\text{исиб}}$ в адрес $\varphi^{\text{сс}}$, либо принимаемого $\varphi^{\text{сс}}$ от $\rho^{\text{исиб}}$, $\rho^{\text{исиб}}=\overline{1,\ \mu^{\text{писиб}}}$ в ζ-м их РжФ за интервал времени $\left[\tau^{\text{оиу}}-1,\ \tau^{\text{оиу}}\right]$ сетевого трафика с результатами (информацией о состоянии определенных объектов КИИ) ПФ $\rho^{\text{исиб}}$ (ед. изм. – килобайт/мегабайт и т.п.);

$$\omega_{\zeta}^{g/\text{пон}}(\tau^{\text{оиу}})=\begin{cases}1,\ \mathcal{J}_{\zeta}^{g/\text{кон}}(\tau^{\text{оиу}})>0; \\ 0,\ \text{иначе},\end{cases} \quad (8)$$
$$\zeta=\overline{1,3},\ g=\overline{1,D},$$

где $\mathcal{J}_{\zeta}^{g/\text{кон}}$ – количество фактов (случаев) обращений внешнего и потенциального внутреннего непривилегированного нарушителей в интервале времени $\left[\tau^{\text{оиу}}-1,\ \tau^{\text{оиу}}\right]$ к определенным (контролируемым $\rho^{\text{исиб}}$) объектам КИИ, либо к $\rho^{\text{исиб}}$, либо к $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – число фактов обращений нарушителей);

$$\gamma_{\zeta}^{g/\text{ро}}(\tau^{\text{оиу}})=\left|\frac{\mathcal{B}_{\zeta}^{g/\text{всо}}(\tau^{\text{оиу}})}{\mathcal{B}_{\zeta}^{g/\text{во}}(\tau^{\text{оиу}})}\right|$$
$$\left[\begin{matrix}\left(\mathcal{B}_{\zeta}^{g/\text{всо}}(\tau^{\text{оиу}})\geq 1\right)\wedge \\ \wedge\left(\mathcal{B}_{\zeta}^{g/\text{во}}(\tau^{\text{оиу}})\geq 1\right)\end{matrix}\right], \quad (9)$$
$$\zeta=\overline{1,3},\ g=\overline{1,D},$$

где $\mathcal{B}_{\zeta}^{g/\text{всо}}$, $\mathcal{B}_{\zeta}^{g/\text{во}}$ – соответственно количество выполненных специалистом по ИБ и выпущенных соответствующим разработчиком обновлений БД уязвимостей нулевого дня и впервые выявленных уязвимостей определенных (контролируемых $\rho^{\text{исиб}}$) объектов КИИ и $\rho^{\text{исиб}}$ ζ-м его РжФ, либо обновлений количества известных КА на определенные (контролируемые $\rho^{\text{исиб}}$) объекты КИИ, на $\rho^{\text{исиб}}$ (взаимодействующие с $\varphi^{\text{сс}}$) и на $\varphi^{\text{сс}}$ в ζ-м их РжФ, не включенных в используемую БД КА в связи с отсутствием сценариев их реализации (ед. изм. – соответственно число выполненных и выпущенных обновлений);

$\mathcal{B}_{\zeta}^{g/\text{всо}}(\tau^{\text{оиу}}) \geq 1$, $\mathcal{B}_{\zeta}^{g/\text{всо}}(\tau^{\text{оиу}}) \geq 1$ – соответственно область допустимых значений $\mathcal{B}_{\zeta}^{g/\text{всо}}$ и $\mathcal{B}_{\zeta}^{g/\text{всо}}$ в $\tau^{\text{оиу}}$ момент времени, указывающая на то, что при расчете значения $\gamma_{\zeta}^{g/\text{ро}}(\tau^{\text{оиу}})$ учитывается, что на этапе подготовке к эксплуатации ГетСОПКА специалистом по ИБ выполнена первоначальная актуализация соответствующего набора исходных данных, требуемых для реализации процедуры конфигурирования ПФ $\rho^{\text{исиб}}$, либо $\varphi^{\text{сс}}$, в результате чего исходные значения $\mathcal{B}_{\zeta}^{g/\text{всо}}$ и $\mathcal{B}_{\zeta}^{g/\text{во}}$ принимаются равными 1, которые впоследствии могут увеличиваются с течением времени;

$$\begin{cases} \vartheta_{\zeta}^{g/\text{кнву}}(\tau^{\text{оиу}}) \Big| \exists \tau^{\text{вкнву}}: \\ \quad \Big[\left(\tau^{\text{вкнву}} \leq \tau^{\text{нон}}\right) \vee \\ \vee \left(\tau^{\text{нон}} < \tau^{\text{вкнву}} \leq \tau^{\text{оон}}\right)\Big] \leq \tau^{\text{оиу}}; \\ h_{\zeta}^{g/\text{ика}}(\tau^{\text{оиу}}) \Big| \exists \tau^{\text{вика}}: \\ \quad \Big[\left(\tau^{\text{вика}} \leq \tau^{\text{нон}}\right) \vee \\ \vee \left(\tau^{\text{нон}} < \tau^{\text{вика}} \leq \tau^{\text{оон}}\right)\Big] \leq \tau^{\text{оиу}}; \\ \zeta = \overline{1,3},\ g = \overline{1,D}, \end{cases} \quad (10)$$

где $\tau^{\text{вкнву}}$, $\tau^{\text{вика}}$ – соответственно момент времени выявления (выпуска соответствующим разработчиком) уязвимостей нулевого дня и впервые выявленных уязвимостей определенных (контролируемых $\rho^{\text{исиб}}$) объектов КИИ, либо $\rho^{\text{исиб}}$ в ζ-м его РжФ, либо известных КА на определенные (контролируемые $\rho^{\text{исиб}}$) объекты КИИ, либо на $\rho^{\text{исиб}}$ (взаимодействующие с $\varphi^{\text{сс}}$) или на $\varphi^{\text{сс}}$ в ζ-м их РжФ, не включенных в используемую БД КА в связи с отсутствием сценариев их реализации (ед. изм. – в заданных единицах времени);

$\tau^{\text{нон}}$, $\tau^{\text{оон}}$ – соответственно момент времени начала и окончания обращения внешнего и потенциального внутреннего непривилегированного нарушителей к определенным (контролируемым $\rho^{\text{исиб}}$) объектам КИИ, либо к $\rho^{\text{исиб}}$, либо к $\varphi^{\text{сс}}$ в ζ-м их РжФ (ед. изм. – в заданных единицах времени).

На основе (2-10) определим текущий уровень информационной устойчивости ПФ ПИСИБ и ЦПСХКСИБ на этапе их эксплуатации в ζ-м РжФ при ДПВ и ДНПВ, направленных на нарушение их ПФ и доступности, посредством расчета текущих значений скоростей изменения набора (количества) данных (параметров) конфигурации (настройки) их ПФ (соответственно $dY_{\zeta}^{\text{писиб/пдк}} / dt$ и $dY_{\zeta}^{\text{цпсхксиб/пдк}} / dt$) в виде:

$$\begin{cases} \dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt} = \min\limits_{\rho^{\text{исиб}}} \dfrac{dY_{\zeta}^{\rho^{\text{исиб}}/\text{пдк}}}{d\tau^{\text{оиу}}}; \\ \dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt} = \min\limits_{\varphi^{\text{сс}}} \dfrac{dY_{\zeta}^{\varphi^{\text{сс}}/\text{пдк}}}{d\tau^{\text{оиу}}}; \end{cases} \quad (11)$$

$$\zeta = \overline{1,3},\ \rho^{\text{исиб}} = \overline{1,\mu^{\text{писиб}}},\ \varphi^{\text{сс}} = \overline{1,\varepsilon^{\text{цпсхксиб}}}.$$

В завершении учитывая (1, 11), определим текущее значение $dY_{\zeta}^{\text{сопка/пдк}} / dt$ в виде:

$$\frac{dY_{\zeta}^{\text{сопка/пдк}}}{dt} = \quad (12)$$

$$= \begin{cases} \dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt} + \dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt}, \text{ при } \left[\left(\left(\dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt} \geq 0 \right) \wedge \left(\dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt} \geq 0 \right) \right) \vee \left(\left(\dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt} < 0 \right) \wedge \left(\dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt} < 0 \right) \right) \right]; \\ \min\left(\dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt}, \dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt} \right), \text{ при } \left[\left(\dfrac{dY_{\zeta}^{\text{писиб/пдк}}}{dt} < 0 \right) \vee \left(\dfrac{dY_{\zeta}^{\text{цпсхксиб/пдк}}}{dt} < 0 \right) \right]; \\ \zeta = \overline{1,3}. \end{cases} \quad (12)$$

Анализируя представленный научно-методический аппарат оценивания информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в условиях ДПВ и ДНПВ, направленных на нарушение ее ПФ и доступности, в качестве направлений дальнейшего его развития следует определить необходимость в разработке:

- имитационной модели ПФ ГетСОПКА (например, на базе программной среды AnyLogic), способной обеспечить определение степени зависимости текущего уровня информационной устойчивости ПФ рассматриваемого объекта от текущих значений выделенных ключевых показателей с последующим формированием рекомендаций специалисту по ИБ по порядку администрирования ИСИБ (СС) в различных их РжФ, например, по направлению определения и соблюдения времени $t_{\zeta_{\text{окии}}}^{g/\text{одв}}$;
- формализованных подходов к определению уточненного семантического значения, показателей и критериев оценивания структурной и функциональной устойчивости ПФ рассматриваемого объекта в заданных РжФ и условиях эксплуатации, что совместно с его информационной устойчивостью позволит обоснованно сформировать комплексную (интегральную) количественную оценку в заданной предметной области с учетом определенных исходных данных по составу структурных элементов ГетСОПКА, а также устаревания ПД о текущем состоянии ПФ ИСИБ (СС) в выделенном временном интервале их адаптивного итерационного контроля;
- программной модели системы комплексного оценивания устойчивости ГетСОПКА на этапе ее эксплуатации в заданных РжФ и условиях эксплуатации, позволяющей оперативно формировать обоснованные ИТР на ФПУ ПФ рассматриваемого объекта.

Выводы

В работе предложен формализованный подход к оцениванию информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации при ДПВ и ДНПВ, направленных на нарушение ПФ и доступности ее структурных элементов, в рамках которого:

1. На основе представления ГетСОПКА в виде кибернетической системы обосновано определено семантическое значение, показатель и критерий оценивания информационной устойчивости ПФ рассматриваемого объекта в заданных условиях эксплуатации, а также раскрыты и иные аспекты его устойчивости, в частности выделена структурная и функциональная устойчивость.

2. Приведено, что наиболее адекватным методом решения задачи оценивания информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации в заданных условиях является метод системно-динамического моделирования, посредством которого построена системно-динамическая модель рассматриваемого объекта. При этом, сформирована система ключевых показателей, обеспечивающая возможность получения количественной оценки текущего уровня рассматриваемого аспекта устойчивости ГетСОПКА, а также сделан научно-технологический задел для оценивания ее структурной и функциональной устойчивости и, как следствие, формирования на их основе комплексной (интегральной) оценки.

3. На основе представление ГетСОПКА в виде системно-динамической модели посредством применения аналитических методов (дифференциальных уравнений, алгебраических выражений и логических условий) сформирована целенаправленная последовательность действий для получения количественной оценки текущего уровня информационной устойчивости ПФ рассматриваемого объекта в заданных РжФ и условий эксплуатации.

4. Определены планируемые направления развития разработанного научно-методического аппарата оценивания информационной устойчивости ПФ ГетСОПКА на этапе ее эксплуатации, связанные с построением имитационной модели ПФ рассматриваемого объекта на базе программной среды AnyLogic, с формализацией подходов к комплексному оцениванию устойчивости ГетСОПКА с последующей разработкой соответствующей программной модели, обеспечивающей возможность практической реализации ПФПУ ПФ рассматриваемого объекта.

Литература

1. Котенко И.В., Саенко И.Б., Захарченко Р.И., Величко Д.В. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации // Вопросы кибербезопасности. 2023. № 1(53). С. 13–27. DOI:10.21681/2311-3456-2023-1-13-27.
2. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. профессора РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия – Телеком, 2022. 560 с.
3. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2023. 240 с.
4. Коноваленко С.А., Королев И.Д., Секунов В.Г. Моделирование системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Информационные системы и технологии. 2022. № 1(129). С. 105–113.
5. Устройство аудита информационной безопасности в автоматизированных системах: пат. 180789 Рос. Федерация / заявитель, патентообладатель Таразевич Е.С., Володина Н.И, Рыжов Б.С., Киселев В.В., Федеральное государственное бюджетное учреждение «4 Центральный научно-исследовательский институт» Министерства обороны Российской Федерации. – № 2017137955; заявл. 31.10.2017, опубл. 22.06.2018, Бюл. № 18. – 10 с.
6. Минаев В.А., Королев И.Д., Коноваленко С.А., Васильев Д.С., Секунов В.Г. Структурно-функциональная модель имитации компьютерных атак на автоматизированные системы // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ, управление. 2020. № 1. С. 3-16. DOI: 10.25586/RNU.V9187.20.01.P.003.
7. Коноваленко, С.А. Модель адаптивного контроля системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Информация и безопасность. 2022. Т. № 25. № 1. С. 141–154. DOI: 10.36622/VSTU.2022.25.1.012.
8. Коноваленко С.А. Функциональная модель синтеза скрипта контроля системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Вопросы защиты информации. 2022. № 2 (137). С. 3–12. DOI: 10.52190/2073-2600_2022_2_3.
9. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. 337 с.
10. Михайлов Р.Л., Макаренко С.И. Оценка устойчивости сети связи в условиях воздействия на нее дестабилизирующих факторов // Системы, сети и устройства телекоммуникаций. 2013. № 4. С. 69–79.
11. Мальцев В.А. Анализ устойчивости как комплексного функционального свойства системы технического обслуживания и ремонта военной техники // Известия ТулГУ. Технические науки. 2019. № 4. С. 215–221.
12. Цифровые двойники: монография / под ред. П.А. Созинова. – М.: Радиотехника, 2022. С. 113–232.
13. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Структурно-функциональная модель киберпространства // Вопросы кибербезопасности. 2021. № 4(44). С. 16–24. DOI:10.21681/2311-3456-2021-4-16-24.
14. Минаев В.А., Сычев М.П., Вайц Е.В., Киракосян А.Э. Имитационное моделирование эпидемий компьютерных вирусов // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2019. № 3. С. 3–12. DOI: 10.25586/RNU.V9187.19.03.P.003.

15. Минаев В.А., Сычев М.П., Вайц Е.В., Бондарь К.М. Системно-динамическое моделирование сетевых информационных операций // Инженерные технологии и системы. 2019. Т. № 29. № 1. С. 20–39. DOI: 10.15507/2658-4123.029.201901.020-039.
16. Коноваленко С.А. Модель системы комплексного оценивания устойчивости гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на этапе ее эксплуатации / Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2023. № 3-4 (177-178). С. 71–81. DOI: 10.53816/23061456_2023_3–4_71.

METHODOLOGY FOR ASSESSING THE INFORMATION STABILITY OF A HETEROGENEOUS COMPUTER ATTACK DETECTION SYSTEM

Konovalenko S.A.[21]

The purpose of the study: *to determine the refined semantic meaning, indicator and criterion for assessing the information stability of the process of functioning of a heterogeneous system for detecting, preventing and eliminating the consequences of computer attacks, as well as the formation on their basis of a targeted sequence of actions to obtain a quantitative assessment of the aspect of stability under consideration.*

Research method: *system analysis, system dynamic modeling using algebraic expressions and logical conditions.*

Research results: *the need to develop a scientific and methodological apparatus for assessing the information stability of the process of functioning of a heterogeneous system for detecting, preventing and eliminating the consequences of computer attacks at the stage of its operation under conditions of destructive influences aimed at disrupting its process of functioning and availability has been determined. An analysis of the conceptual apparatus was carried out and terminological vagueness in the subject area under study was identified. A refined semantic meaning, indicator and criterion for assessing the information stability of the process of functioning of the object under consideration under given operating conditions has been generated. Based on the representation of a given object of assessment in the form of a cybernetic system and a system-dynamic model, a system of key indicators and a targeted sequence of actions have been developed to obtain a quantitative assessment of the current level of the sustainability aspect under consideration. Directions for the development of the developed scientific and methodological apparatus for assessing the information stability of the process of functioning of the object under consideration are proposed.*

The scientific novelty *lies in the provision of a theoretically justified formalized approach to assessing the information stability of the process of functioning of a heterogeneous system for detecting, preventing and eliminating the consequences of computer attacks, which, unlike the known ones, allows us to form a scientific and technological basis for obtaining a comprehensive assessment of the stability of a given object and the implementation of the proposed scientific and technical solutions on practice.*

Keywords: *cybernetic system, system-dynamic model, rate of change of information resource, vulnerability, computer attack, functional-parametric control procedures, disruption of the functioning process, disruption of accessibility.*

References

1. Kotenko I.V., Saenko I.B., Zakharchenko R.I., Velichko D.V. Subsystem for preventing computer attacks on critical information infrastructure objects: analysis of functioning and implementation // Issues of cybersecurity. 2023. No. 1(53). pp. 13-27. DOI:10.21681/2311-3456-2023-1-13-27.
2. Cybersecurity of the digital industry. Theory and practice of functional resistance to cyber attacks / Ed. Professor of the Russian Academy of Sciences, Doctor of Technical Sciences D.P. Zegrzdy. – M.: Hotline – Telecom, 2022. 560 p.

21 Sergey A. Konovalenko, Ph.D. (Technology), Krasnodar Higher Military Order of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: konovalenko_rcf@mail.ru

3. Erokhin S.D., Petukhov A.N., Pilyugin P.L. Security management of critical information infrastructures. – M.: Hotline – Telecom, 2023. 240 p.
4. Konovalenko S.A., Korolev I.D., Sekunov V.G. Modeling a system for detecting, preventing and eliminating the consequences of computer attacks // Information systems and technologies. 2022. No. 1(129). pp. 105-113.
5. Information security audit device in automated systems: Pat. 180789 Ross. Federation / applicant, patent holder E.S. Tarazevich, N.I. Volodina, B.S. Ryzhov, V.V. Kiselev, Federal State Budgetary Institution "4th Central Research Institute" of the Ministry of Defense of the Russian Federation. – No. 2017137955; appl. 31.10.2017, publ. 22.06.2018, Bulletin. No. 18. – 10 p.
6. Minaev V.A., Korolev I.D., Konovalenko S.A., Vasiliev D.S., Sekunov V.G. Structural-functional model for simulating computer attacks on automated systems // Bulletin of the Russian New University. Series: Complex systems: models, analysis, control. 2020. No. 1. pp. 3-16. DOI: 10.25586/RNU.V9187.20.01.P.003.
7. Konovalenko, S.A. Model of adaptive control of a system for detecting, preventing and eliminating the consequences of computer attacks // Information and Security. 2022. Vol. No. 25. No. 1. pp. 141-154. DOI: 10.36622/VSTU.2022.25.1.012.
8. Konovalenko S.A. Functional model for the synthesis of a control script for a system for detecting, preventing and eliminating the consequences of computer attacks // Issues of information protection. 2022. No. 2 (137). pp. 3-12. DOI: 10.52190/2073-2600_2022_2_3.
9. Makarenko S.I. Models of a communication system under conditions of deliberate destabilizing influences and reconnaissance. Monograph. – St. Petersburg: High-tech technologies, 2020. 337 p.
10. Mikhailov R.L., Makarenko S.I. Assessing the stability of a communication network under the influence of destabilizing factors // Systems, networks and telecommunication devices. 2013. No. 4. pp. 69-79.
11. Maltsev V.A. Analysis of stability as a complex functional property of the system of maintenance and repair of military equipment // Izvestia of Tula State University. Technical science. 2019. No. 4. pp. 215-221.
12. Digital twins: monograph / ed. P.A. Sozinov. – M.: Radio engineering, 2022. pp. 113-232.
13. Starodubtsev Yu.I., Zakalkin P.V., Ivanov S.A. Structural-functional model of cyberspace // Issues of cybersecurity. 2021. No. 4(44). pp. 16-24. DOI:10.21681/2311-3456-2021-4-16-24.
14. Minaev V.A., Sychev M.P., Vaits E.V., Kirakosyan A.E. Simulation modeling of computer virus epidemics // Bulletin of the Russian New University. Series: Complex systems: models, analysis and control. 2019. No. 3. pp. 3-12. DOI: 10.25586/RNU.V9187.19.03.P.003.
15. Minaev V.A., Sychev M.P., Vaitz E.V., Bondar K.M. System-dynamic modeling of network information operations // Engineering technologies and systems. 2019. Vol. No. 29. No. 1. pp. 20-39. DOI: 10.15507/2658-4123.029.201901.020-039.
16. Konovalenko S.A. Model of a system for comprehensive assessment of the stability of a heterogeneous system for detecting, preventing and eliminating the consequences of computer attacks at the stage of its operation / Questions of defense technology. Episode 16: Technical means of countering terrorism. 2023. No. 3-4 (177-178). pp. 71-81. DOI: 10.53816/23061456_2023_3–4_71.

МАТЕМАТИЧЕСКИЕ МОДЕЛИ ДЛЯ ОЦЕНКИ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Соловьев С.В.[1], Язов Ю.К.[2], Теплинских А.А.[3]

Цель *исследования состоит в разработке математических моделей для количественной оценки показателей полноты, достоверности, актуальности и защищенности информационного обеспечения деятельности по организации и ведению технической защиты информации в органах власти, организациях и предприятиях.*

В результате исследования *предложены показатели оценки качества информационного обеспечения деятельности по технической защите информации: полноты, достоверности, своевременности (актуальности) и защищенности информации, необходимой для такого обеспечения, раскрыта взаимосвязь указанных показателей качества с комплексным показателем оценки эффективности информационного обеспечения. С учетом содержания модели предметной области технической защиты информации показано, что полнота, достоверность и актуальность информационного обеспечения защиты информации определяется множествами: функций, предусмотренных в модели предметной области и действительно реализуемых в информационной системе; задач, решение которых обеспечивает реализацию функций; информационных объектов и их атрибутов, подлежащих использованию в соответствии с моделью предметной области и реально используемых при решении задач защиты информации. Для оценки показателя защищенности информации, необходимой при информационном обеспечении деятельности по защите информации, предложено использование аппарата нечетких оценок вероятностей реализации угроз относительно системной и пользовательской информации, нарушение конфиденциальности, целостности или доступности которой может сорвать информационное обеспечение.*

Практическая ценность. *Разработаны аналитические соотношения для расчета показателей качества информационного обеспечения, что позволяет количественно обосновывать требования к информационному обеспечению деятельности по защите информации и к создаваемым системам информационного обеспечения для органов власти, организаций и предприятий.*

Ключевые слова: *информационная система, эффективность, предметная область, полнота, достоверность, актуальность, защищенность информации.*

DOI: 10.21681/2311-3456-2023-6-81-95

Введение

Информационное обеспечение деятельности по организации и ведению технической защиты информации (ТЗИ) в органах власти, организациях и предприятиях связано сегодня с предоставлением им такой информации, как [1]:

— состав и содержание актуальных нормативных правовых, организационно-распорядительных и методических документов государственного регулятора в области ТЗИ;

1 Соловьёв Сергей Вениаминович, кандидат технических наук, доцент, заместитель начальника Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. E-mail:sersol@mail.ru

2 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

3 Теплинских Александр Андреевич, научный сотрудник Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. E-mail:ma4karek48@yandex.ru

— сведения из реестра значимых объектов критической информационной инфраструктуры в части, касающейся информационной системы (ИС) субъекта деятельности по ТЗИ (органа власти, организации, предприятия) в случае, если ИС относится или может быть отнесена к таким объектам;
— акты, докладные, указания и сообщения, аналитические обзоры и иные информационные документы, присланные вышестоящими инстанциями или высланные им субъектом деятельности по ТЗИ;
— состав и характеристики ИС, функционирующей в субъекте деятельности по ТЗИ, требуемый класс (уровень) ее защищенности в соответствии с действующими документами;
— состав и характеристики мер и средств ТЗИ, применяемых в ИС, установленные для средств классы защиты и выданные на них сертификаты;
— состав и характеристики угроз безопасности информации, которые могут иметь место в данной ИС, а также уязвимостей системного и прикладного программного обеспечения функционирования ИС;
— результаты оценки рисков реализации угроз в данной ИС или в сходных с ней ИС;
— результаты контроля защищенности информации в ИС, выявления уязвимостей и нарушений безопасности информации и др.

Стремительно разрастающиеся объемы и сравнительно быстрые изменения содержания такой информации (например, связанные с разработкой и введением в действие новых нормативных и методических документов) приводят к значительным сложностям в ее подготовке, актуализации и предоставлении специалистам при организации и ведении ТЗИ, обусловливают необходимость автоматизации процессов информационного обеспечения (ИО) и создания в рамках организационно-технических систем защиты информации в органах власти, организациях и предприятиях специальных систем информационного обеспечения – СИО.

Однако для этого, как показано в [2], необходимо разработать соответствующее методическое обеспечение, то есть совокупность математических моделей и методик, которое сегодня только начинает развиваться применительно к предметной области ТЗИ. Важнейшей составляющей такого обеспечения является совокупность математических моделей количественной оценки эффективности информационного обеспечения деятельности по ТЗИ – эффективности функционирования СИО. При этом под эффективностью информационного обеспечения понимается [2-4] степень соответствия предоставляемых услуг в информационном обеспечении потребностям организации и ведения ТЗИ в субъекте деятельности по ТЗИ. В таком понимании эффективность информационного обеспечения является функцией частных показателей, характеризующих качество информационного обеспечения по его отдельным аспектам, таким как полнота, достоверность, своевременность (актуальность) и защищенность информации, требуемой при организации и ведении ТЗИ.

В [2] предложены аналитические соотношения, позволяющие с использованием линейной функции или мультипликативной функции Кобба-Дугласа [5, 6] свернуть указанные показатели в один комплексный показатель эффективности информационного обеспечения с учетом устанавливаемых для каждого частного показателя, например, с применением метода анализа иерархий[4] Т. Саати, коэффициентов важности. В частности, при использовании линейной функции соотношение для расчета комплексного показателя имеет вид:

$$\eta_1(t) = \alpha_{full} \cdot g_{full}(t) + \alpha_{rel} \cdot g_{rel}(t) + \\ + \alpha_{act} \cdot g_{act}(t) + \alpha_{prot} \cdot g_{prot}(t), \quad (1)$$

где $g_{full}(t)$, $g_{rel}(t)$, $g_{act}(t)$, $g_{prot}(t)$ – частные показатели полноты, достоверности, своевременности (актуальности) и защищенности информационного обеспечения при оценке в момент времени t;

α_{full}, α_{rel}, α_{act} и α_{prot} – коэффициенты важности частных показателей соответственно.

Вместе с тем в работе [2] не раскрывались методы и модели оценки самих частных показателей. В связи с изложенным цель данной статьи состоит в разработке математических моделей количественной оценки указанных частных показателей полноты, достоверности, актуальности и защищенности информационного обеспечения деятельности по организации и ведению ТЗИ в органах власти, организациях и предприятиях.

1. Математическая модель для оценки полноты информационного обеспечения деятельности по технической защите информации

Под полнотой информационного обеспечения понимается степень соответствия состава выполняемых услуг информационного обеспечения составу услуг, которые должны предоставляться в соответствии с мо-

4 Т. Саати. Метод анализа иерархий. М.: «Радио и связь». 1993 г.

делью предметной области ТЗИ и уровнем развития методического обеспечения организации и ведения ТЗИ [2, 7]. В связи с этим оценка полноты информационного обеспечения существенно зависит от содержания предметной области ТЗИ, в рамках которой осуществляется деятельность по ТЗИ. В соответствии с [7] модель предметной области ТЗИ формально описывается совокупностью множеств:

$$M(t)=\{F(t),Z(t),L(t),O(t),V(t),R(t)\} \quad (2)$$

где $F(t)=\{f_i(t)|i=\overline{1,I}\}$ – множество функций, реализуемых при организации и ведении ТЗИ. К таким функциям относятся, например, выявление актуальных угроз безопасности информации в ИС, формирование замысла защиты и т.д.;

$Z(t)=\{z_j(t)|j=\overline{1,J}\}$ – множество задач (процедур), решение (выполнение) которых обеспечивает реализацию функций множества F. К таким задачам (процедурам) относятся, например, выявление подлежащей защите информации, определение класса (уровня) защищенности ИС и др.;

$L(t)=\{l_k(t)|k=\overline{1,K}\}$ – множество пользователей защищаемой ИС;

$O(t)=\{o_m(t)|m=\overline{1,M}\}$ – множество информационных объектов, используемых при решении задач ТЗИ. К этому множеству относятся файлы с текстовой и иной информацией, файлы баз данных и т.д., содержащие совокупности сведений и данных, необходимых для организации и ведения ТЗИ, например, сведения о составе и характеристиках ИС, об угрозах безопасности информации и технических каналах утечки, о требованиях правовых нормативных документов, о методическом обеспечении решения задач ТЗИ и т.д.;

$V(t)=\{V_l(t)|l=\overline{1,L}\}$ – множество информационных элементов (атрибутов информационных объектов). Это множество содержит сведения об информационных объектах;

$R(t)=\{r_n(t)|n=1,N\}$ – множество отношений (взаимосвязей) между компонентами модели предметной области $F(t),Z(t),L(t),O(t),V(t)$.

Элементы указанных множеств, кроме множества отношений, представляют собой фреймы, содержащие определенные слоты описания результатов выполнения соответствующих функций.

С учетом содержания модели предметной области ТЗИ полнота информационного обеспечения деятельности по ТЗИ в рамках, например, одной ИС определяется: множеством функций, предусмотренных в модели предметной области $F(t)=\{f_i(t)|i=\overline{1,I}\}$ и действительно реализуемых при организации и ведении ТЗИ $F^{(ИС)}(t)=\{f_i^{(ИС)}(t)|i=\overline{1,I_{ИС}}\}$;;

множеством $Z(t)$ задач (процедур), решение (выполнение) которых обеспечивает реализацию функций множества F, то есть $Z_i(t)=\{z_{ij}(t)|i=\overline{1,I};\ j=\overline{1,J_i}\}$, при этом $J=\sum_{i=1}^{I}J_i$, и множества $Z_i^{(ИС)}(t)$ задач (процедур), решение которых обеспечивает реализацию функций множества $F_{ИС}$, то есть $Z_i^{(ИС)}(t)=\{z_{ij}^{(ИС)}(t)|i=\overline{1,I^{(ИС)}};\ j=\overline{1,J_i^{(ИС)}}\}$, при этом $J^{(ИС)}=\sum_{i=1}^{I}J_i^{(ИС)}$;

множеством $O_{ij}(t)=\{o_{ijn}(t)|i=\overline{1,I};\ j=\overline{1,J_i};\ n=\overline{1,N_{ij}}\}$ информационных объектов, подлежащих использованию в соответствии с моделью предметной области, при этом $N=\sum_{i=1}^{I}\sum_{j=1}^{J_i}N_{ij}$, и множеством $O_{ij}^{(ИС)}(t)=\{o_{ijn}^{(ИС)}(t)|i=\overline{1,I};\ j=\overline{1,J_i};\ n=\overline{1,N_{ij}^{(ИС)}}\}$ информационных объектов, используемых реально при решении задач ТЗИ, при этом $N^{(ИС)}=\sum_{i=1}^{I}\sum_{j=1}^{J_i}N_{ij}^{(ИС)}$;

множеством $V_{ijn}(t)=\{v_{ijnk}(t)|i=\overline{1,I};\ j=\overline{1,J_i};\ n=\overline{1,N_{ij}};k=\overline{1,K_{ijn}}\}$ информационных элементов, атрибутов информационных объектов, в соответствии с моделью предметной области, при этом $K=\sum_{i=1}^{I}\sum_{j=1}^{J_i}\sum_{n=1}^{N_{ij}}K_{ijn}$, и множеством $V_{ijn}^{(ИС)}(t)$ информационных элементов, реально используемых при организации и ведении ТЗИ, $V_{ijn}^{(ИС)}(t)=\{v_{ijnk}^{(ИС)}(t)|i=\overline{1,I};\ j=\overline{1,J_i};\ n=\overline{1,N_{ij}};k=\overline{1,K_{ijn}^{(ИС)}}\}$, при этом $K^{(ИС)}=\sum_{i=1}^{I^{(ИС)}}\sum_{j=1}^{J_i^{(ИС)}}\sum_{n=1}^{N_{ij}^{(ИС)}}K_{ijn}^{(ИС)}$.

Полнота информационного обеспечения характеризует, по сути, охват подлежащих реализации указанных множеств. С учетом изложенного данный показатель может быть рассчитан по следующей формуле:

$$g_{full}(t)=\frac{\sum_{i=1}^{I^{(ИС)}}\delta_{ИС}\left\{f_i^{(ИС)}(t)\right\}\cdot\sum_{j=1}^{J_i^{(ИС)}}\delta_{ИС}\left\{z_{ij}^{(ИС)}(t)\right\}\cdot\sum_{n=1}^{N_{ij}^{(ИС)}}\delta_{ИС}\left\{o_{ijn}^{(ИС)}(t)\right\}\cdot\sum_{k=1}^{K_{ijn}^{(ИС)}}\delta_{ИС}\left\{v_{ijnk}^{(ИС)}(t)\right\}}{\sum_{i=1}^{I}\delta\left\{f_i(t)\right\}\sum_{j=1}^{J_i}\delta\left\{z_{ij}(t)\right\}\sum_{n=1}^{N_{ij}}\delta\left\{o_{ijn}(t)\right\}\sum_{k=1}^{K_{ijn}}\delta\left\{v_{ijnk}(t)\right\}},\quad(3)$$

где

$\delta\{\bullet\}$ – единичная функция, равная единице, если функция (задача, информационный объект или его атрибут) предусмотрена в модели предметной области, и нулю – в противоположном случае;

$\delta_{ИС}\{\bullet\}$ – единичная функция, равная единице, если функция (задача, информационный объект или его атрибут) реально применяются (решаются) при организации и ведении ТЗИ, и нулю – в противоположном случае.

Таким образом, алгоритм оценки показателя полноты информационного обеспечения сводится к последовательному определению состава функций, задач, информационных объектов и информационных элементов, которые предусматриваются при организации и ведении ТЗИ в разработанной модели предметной области ТЗИ и которые реально решаются субъектом деятельности по ТЗИ.

2. Математическая модель для оценки достоверности информационного обеспечения деятельности по технической защите информации

Снижение достоверности информационного обеспечения организации и ведения ТЗИ обусловливается преимущественно ошибками прогноза характеристик предметной области ТЗИ, записываемых в соответствующие базы данных и, прежде всего, ошибками прогноза значений информационных элементов – атрибутов информационных объектов, не измененных к заданному моменту времени. Такие ошибки могут быть оценены следующим образом.

Пусть I – общее количество функций, которые должны выполняться при организации и ведении ТЗИ в соответствии с содержанием предметной области, из которых $I^{(err)}$ к данному моменту времени имеют ошибки в прогнозе значений атрибутов информационных объектов и, в зависимости от размеров ошибок, могут быть неадекватны обстановке, и аналогично J_i и $J_i^{(err)}$ – по решаемым задачам при реализации i-й функции, N_{ij} и $N_{ij}^{(err)}$ – по составу информационных объектов при решении j-й задачи и реализации i-й функции, K_{ijn} и $K_{ijn}^{(err)}$ – по информационным элементам в составе каждого n-го информационного объекта при решении j-й задачи и реализации i-й функции.

Тогда для оценки значения суммарной среднеквадратической ошибки прогноза численных значений[5] атрибутов информационных объектов в ИС имеет место соотношение:

$$\sigma_{\Sigma}^{(v)}(t)=\sqrt{\sum_{i=1}^{I^{(err)}}\delta\left\{f_i(t)\right\}\left[\sum_{j=1}^{J_i^{(err)}}\delta\left\{z_{ij}(t)\right\}\left[\sum_{n=1}^{N_{ij}^{(err)}}\delta\left\{o_{ijn}(t)\right\}\left[\sum_{k=1}^{K_{ijn}^{(num,err)}}\sigma_l^2(t)\,\delta\left\{v_{ijnk}^{(num)}(t)\right\}\right]\right]\right]},\quad(4)$$

где $\sigma_l(t)$ – средняя квадратическая ошибка прогноза значения l-й характеристики (атрибута информационного объекта);

$\delta(\bullet)$ – единичная функция, равная 1, если функция, задача, информационный объект используются при организации и ведении ТЗИ, а информационный элемент не приводит к срыву выполнения задачи или функции, и равна 0 в противоположном случае;

$K_{ijn}^{(num)}$, $K_{ijn}^{(num,err)}$ – общее количество числовых (количественных) атрибутов в составе каждого n-го информационного объекта при решении j-й задачи и реализации i-й функции и количество таких атрибутов, которые имеют ошибки в прогнозе значений, соответственно.

При этом имеют место следующие равенства:

$$J=\sum_{i=1}^{I}J_i,\quad J^{(err)}=\sum_{i=1}^{I^{(err)}}J_i^{(err)},\quad N=\sum_{i=1}^{I}\sum_{j=1}^{J_i}N_{ij},$$
$$N^{(err)}=\sum_{i=1}^{I^{(err)}}\sum_{j=1}^{J_i^{(err)}}N_{ij}^{(err)},K^{(num)}=\sum_{i=1}^{I}\sum_{j=1}^{J_i}\sum_{n=1}^{N_{ij}}K_{ijn}^{(num)},\quad(5)$$

5 В их состав не входят атрибуты, имеющие вербальные описания.

$$K^{(num,err)} = \sum_{i=1}^{I^{(err)}} \sum_{j=1}^{J_i^{(err)}} \sum_{n=1}^{N_{ij}^{(err)}} K_{ijn}^{(num,err)}, \qquad (5)$$

$$K^{(num)} + K^{(num,err)} = K_{IIC}^{(num)} .$$

Следует отметить, что в качестве показателя достоверности ИО может быть использована суммарная среднеквадратическая ошибка прогноза значений атрибутов всех информационных объектов в ИС, однако более адекватным является вероятностная оценка, основанная на расчете вероятности превышения отклонения суммы числовых значений атрибутов информационных объектов, при это суть расчета сводится к следующему.

Суммарное математическое ожидание числовых значений атрибутов информационных объектов рассчитывается по формуле:

$$\overline{k_{\Sigma}^{(v)}(t)} = \frac{\sum_{i=1}^{I^{(err)}} \delta\{f_i(t)\} \left[\sum_{j=1}^{J_i^{(err)}} \delta\{z_{ij}(t)\} \left[\sum_{n=1}^{N_{ij}^{(err)}} \delta\{o_{ijn}(t)\} \left[\sum_{k=1}^{K_{ijn}^{(num,err)}} v_{ijnk}^{(num)}(t) \delta\{v_{ijnk}^{(num)}(t)\} \right] \right] \right]}{K^{(num,err)}}. \qquad (6)$$

Сумма большого количества в общем случае случайных значений количественных атрибутов информационных объектов $\xi(t)$, определяемая к моменту времени t, распределена по нормальному закону[6]:

$$w_{\xi}(x,t) = \frac{1}{\sigma_{\Sigma}^{(v)}\sqrt{2\pi}} \cdot \exp\left\{ -\frac{1}{2} \cdot \left[\frac{x - \overline{k_{\Sigma}^{(v)}(t)}}{\sigma_{\Sigma}^{(v)}(t)} \right]^2 \right\}. \qquad (7)$$

Тогда вероятность того, что ошибка в оценке суммы значений числовых атрибутов информационных объектов $\xi(t)$ не превысит заданного значения a_{lim}, используемая в качестве показателя оценки достоверности информационного обеспечения в ИС, рассчитывается по формуле:

$$g_{rel}^{(num)}(t) = \int_0^{a_{lim}} w_{\xi}(x,t)dx = \Phi_0\left[\frac{a_{lim} - \overline{k_{\Sigma}^{(v)}(t)}}{\sigma_{\Sigma}^{(v)}(t)} \right] - \frac{1}{2}, \qquad (8)$$

где $\Phi_0(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-z^2} dz$ – табулированная функция нормального распределения.

Если атрибуты информационных объектов имеют вербальные описания, то наличие ошибок в их прогнозе определяется путем сравнения слотов их описаний и экспертной оценки существенности таких ошибок. Пусть $K_{ijn}^{(w)}$ и $K_{ijn}^{(w,err)}$ – общее количество атрибутов с вербальным описанием в составе каждого n-го информационного объекта при решении j-й задачи и реализации i-й функции и количество таких атрибутов, для которых имеются ошибки в прогнозе значений, соответственно. Ориентировочно уровень недостоверности ИО по таким атрибутам может быть оценен как отношение количества вербально описанных атрибутов, по которым имеются существенные отклонения в результате ошибок прогнозирования, что может отрицательно повлиять на организацию и ведение ТЗИ, к общему количеству вербально описанных атрибутов. Тогда показатель достоверности ИО по вербально описанным атрибутам оценивается как величина, дополняющая показатель недостоверности до единицы, то есть следующим образом:

$$g_{rel}^{(w)}(t) = 1 - \frac{\sum_{i=1}^{I^{(err)}} \delta\{f_i(t)\} \left[\sum_{j=1}^{J_i^{(err)}} \delta\{z_{ij}(t)\} \left[\sum_{n=1}^{N_{ij}^{(err)}} \delta\{o_{ijn}(t)\} \left[\sum_{k=1}^{K_{ijn}^{(w,err)}} \delta\{v_{ijnk}^{w}(t)\} \right] \right] \right]}{\sum_{i=1}^{I} \delta\{f_i(t)\} \left[\sum_{j=1}^{J_i} \delta\{z_{ij}(t)\} \left[\sum_{n=1}^{N_{ij}} \delta\{o_{ijn}(t)\} \left[\sum_{k=1}^{K_{ijn}^{(w)}} \delta\{v_{ijnk}(t)\} \right] \right] \right]} \qquad (9)$$

При этом имеют место соотношения:

$$\sum_{i=1}^{I^{(w)}} \sum_{j=1}^{J_i^{(w)}} \sum_{n=1}^{N_{ij}^{(w)}} K_{ijn}^{(w)} = K^{(w)}; \sum_{i=1}^{I^{(w)}} \sum_{j=1}^{J_i^{(w)}} \sum_{n=1}^{N_{ij}^{(w)}} K_{ijn}^{(w,err)} = K^{(w,err)}; \; K^{(w)} + K^{(w,err)} = K_{IIC}^{(w)}. \qquad (10)$$

Для оценки достоверности ИО применительно к совокупности как вербальных, так и числовых атрибутов информационных объектов предлагается использовать следующее соотношение:

$$g_{rel}(t) = \frac{g_{rel}^{(w)}(t) \cdot K^{(w,err)} + g_{rel}^{(num)}(t) \cdot K^{(num,err)}}{K^{(w,err)} + K^{(num,err)}}. \qquad (11)$$

6 Справочник по теории вероятностей и математической статистике / В.С.Королюк, Н.И.Портенко, А.В.Скороход, А.Ф.Турбин – М.: «Наука». Главная редакция физико-математической литературы. 1985 г., 640 с.

Полученные соотношения впервые позволяют оценить достоверность информационного обеспечения организации ТЗИ на объектах информатизации.

3. Математическая модель для оценки актуальности информационного обеспечения деятельности по технической защите информации

Вероятность того, что информационное обеспечение станет неактуальным по всей совокупности информации, практически отсутствует. Однако некоторая информация, включенная в описание предметной области, может быть не предусмотрена в ходе прогнозирования или устарела к моменту решения задач организации или ведения ТЗИ и не будет соответствовать реалиям. В связи с этим актуальность информационного обеспечения рассматривается как соответствие информации, применяемой в субъекте деятельности по ТЗИ, реальному состоянию развития предметной области ТЗИ к заданному моменту времени.

Пусть, как и при расчете показателя достоверности, I – общее количество функций, которые должны выполняться при организации и ведении ТЗИ в соответствии с содержанием предметной области, из которых $I^{(act)}$ к данному моменту времени адекватны обстановке, то есть не устарели по сравнению с имеющимися в описании предметной области прогнозными значениями, и аналогично J_i и $J_i^{(act)}$ – то же, но по решаемым задачам при реализации i-й функции, N_{ij} и $N_{ij}^{(act)}$ – по информационным объектам при решении j-й задачи и реализации i-й функции, K_{ijn} и $K_{ijn}^{(act)}$ – по информационным элементам в составе каждого n-го информационного объекта, используемого при решении j-й задачи и реализации i-й функции. При этом имеют место соотношения:

$$K_{ИС}=\sum_{i=1}^{I}\sum_{j=1}^{J_i}\sum_{n=1}^{N_{ij}}K_{ijn},\quad K_{ИС}^{(act)}=\sum_{i=1}^{I^{(act)}}\sum_{j=1}^{J_i^{(act)}}\sum_{n=1}^{N_{ij}^{(act)}}K_{ijn}^{(act)}. \quad (12)$$

Кроме того, положим, что возможно появление новых функций $f_i^{(new)}(t), i=\overline{1,I^{(new)}}$, задач $z_{ij}^{(new)}(t), j=\overline{1,J_i^{new}}, i=\overline{1,I^{(new)}}$, и соответствующим им информационных объектов $o_{ijn}^{(new)}(t), n=\overline{1,N_{ij}^{(new)}}, j=\overline{1,J_i^{new}}, i=\overline{1,I^{(new)}}$ и информационных элементов $v_{ijnk}^{(new)}(t), k=\overline{1,K_{ijnk}^{(new)}}, n=\overline{1,N_{ij}^{(new)}}, j=\overline{1,J_i^{new}}, i=\overline{1,I^{(new)}}$. Пусть известны (заданы экспертным путем или получены на основе обработки статистических данных за предыдущие годы) вероятности появления к моменту времени t новых функций $P_{fi}^{(new)}$ и задач $P_{zij}^{(new)}$. Пример шкалы оценок этих вероятностей приведен в табл. 1. Тогда общее количество новых атрибутов информационных элементов может быть оценено следующим образом:

$$K_{ИС}^{(new)}=\sum_{i=1}^{I^{new}}P_{fi}^{(new)}\delta\left\{f_i^{(new)}(t)\right\}\left[\sum_{j=1}^{J_i^{new}}P_{zij}^{(new)}\delta\left\{z_{ij}^{(new)}(t)\right\}\times\left[\sum_{n=1}^{N_j^{new}}\delta\left\{o_{ijn}^{(new)}(t)\right\}\left[\sum_{k=1}^{K_{ijn}^{new}}\delta\left\{v_{nijk}^{(new)}(t)\right\}\right]\right]\right]. \quad (13)$$

При этом степень актуальности информационного обеспечения деятельности по ТЗИ может быть оценена по формуле:

$$g_{акт}(t)=1-\frac{K_{ИС}-K_{ИС}^{(act)}+K_{ИС}^{(new)}}{K_{ИС}+K_{ИС}^{(new)}}=\frac{K_{ИС}^{(act)}}{K_{ИС}+K_{ИС}^{(new)}}. \quad (14)$$

Полученное соотношение впервые позволяет рассчитать показатель актуальности информационного ТЗИ и количественно оценить, насколько в действующей модели предметной области учтены возможные инновации.

4. Математическая модель для оценки защищенности информационного обеспечения деятельности по технической защите информации

Защищенность информационного обеспечения деятельности по ТЗИ достигается парированием (нейтрализацией) возможных угроз функционированию ИС, используемой в органе, организации, на предприятии для автоматизации этой деятельности, угроз нарушения конфиденциальности, целостности и доступности прикладных программ и данных, необходимых для организации и ведения ТЗИ.

Указанные угрозы могут реализовываться на сетевом (при передаче защищаемой информации по сети), системном (на уровне операционной системы) и прикладном (на уровне прикладных программ и данных) системно-технических уровнях[7] [8]. При этом угрозы на сетевом уровне реализуются путем перехвата трафика, а на системном и прикладном – путем проникновения в операционную среду ИС. Состав актуальных угроз определяется в частной модели угроз, которая должна составляться для каждой ИС.

Состав мер и средств защиты, которые должны

7 Угрозы на микропрограммном уровне в данной работе не рассматриваются.

Таблица 1

Экспертная шкала оценок возможности возникновения новых функций и задач, подлежащих учету при организации и ведении ТЗИ

Критерий возникновения новой функции	Вербальная оценка возможности возникновения новой функции	Вероятность возникновения новой функции	Критерий возникновения новой задачи	Вербальная оценка возможности возникновения новой задачи	Вероятность возникновения новой задачи
Имеются публикации, подтверждающие возможность появления инноваций: новых технологий обработки информации, новых угроз безопасности, новых нормативных и методических документов, новых мер и средств защиты информации и т.д.	Высокая	$P_{fi}^{(new)} > 0.8$	Путем решения известных задач невозможно выполнить новую функцию, необходимо решать для ее выполнения новые задачи	Высокая	$P_{zij}^{(new)} > 0.8$
			Решением известных задач частично можно выполнить новую функцию, однако для решения некоторых из задач, возможно, потребуется новое методическое обеспечение или новые исходные данные	Средняя	$0.4 < P_{zij}^{(new)} \le 0.8$
			Предположительно возможно обеспечить выполнение новой функции путем решения известных задач	Низкая	$P_{zij}^{(new)} \le 0.4$
Имеются сведения, свидетельствующие лишь о возможности разработки инноваций	Средняя	$0.4 < P_{fi}^{(new)} \le 0.8$	Путем решения известных задач невозможно выполнить новую функцию, необходимо решать для ее выполнения новые задачи	Высокая	$P_{zij}^{(new)} > 0.8$
			Решением известных задач частично можно выполнить новую функцию, однако для решения некоторых из задач, возможно, потребуется новое методическое обеспечение или новые исходные данные	Средняя	$0.4 < P_{zij}^{(new)} \le 0.8$
			Предположительно возможно обеспечить выполнение новой функции путем решения известных задач	Низкая	$P_{zij}^{(new)} \le 0.4$
Сведения, свидетельствующие о сроках появления инноваций весьма неопределенные или отсутствуют	Низкая	$P_{fi}^{(new)} \le 0.4$	Путем решения известных задач невозможно выполнить новую функцию, необходимо решать для ее выполнения новые задачи	Высокая	$P_{zij}^{(new)} > 0.8$
			Решением известных задач частично можно выполнить новую функцию, однако для решения некоторых из задач, возможно, потребуется новое методическое обеспечение или новые исходные данные	Средняя	$0.4 < P_{zij}^{(new)} \le 0.8$
			Предположительно возможно обеспечить выполнение новой функции путем решения известных задач	Низкая	$P_{zij}^{(new)} \le 0.4$

применяться в интересах парирования угроз, определяется классом защищенности ИС и соответствующим этому классу составом мер защиты, регламентированным нормативными документами ФСТЭК России. Чем выше класс защищенности, тем меньше вероятность того, что принятая мера может быть преодолена в ходе реализации той или иной угрозы.

Для парирования возможности перехвата трафика, поступающего в ИС органа власти, организации, предприятия или передаваемого с защищаемой ИС в вышестоящие инстанции или другим органам власти, организациям и предприятиям, как правило, применяются частные виртуальные сети с криптографической защитой, реализуемой с применением сертифицированных ФСБ России криптографических средств, при этом считается, что такая защита является достаточной.

В связи с этим оценку защищенности целесообразно проводить только относительно угроз на системном и прикладном уровнях, то есть относительно угроз, реализация которых связана с проникновением в операционную среду ИС, в том числе с внедрением вредоносных программ. Особенности такой оценки заключаются в следующем.

1. Оценка защищенности от угроз нарушения конфиденциальности, целостности и доступности защищаемой информации должна быть привязана к самой информации, то есть к пользовательским программам и данным, и охватывать всю защищаемую информацию, циркулирующую в ИС. До сих пор оценка защищенности не проводилась относительно всего объема подлежащей защите информации, а выбирались лишь отдельные файлы и применительно к каждому из них оценивалась возможность реализации угрозы без мер защиты и в условиях применения мер защиты. Поскольку объемы защищаемой информации даже в одном компьютере весьма велики, крайне сложной оказывается и оценка защищенности информационного обеспечения деятельности по ТЗИ, то есть защищенности всей информации, необходимой для организации и ведения ТЗИ. Более того, даже подход к такой оценке фактически не разрабатывался.

2. При оценке защищенности информационного обеспечения от угроз, связанных с проникновением в операционную среду, необходимо учитывать то, что для разных угроз несанкционированные (деструктивные) действия, определяющие содержание угрозы, различны. Так, угрозы нарушения конфиденциальности информации реализуются путем несанкционированного копирования соответствующих файлов с записью в выбранные области постоянной памяти с последующей их передачей (возможно скрытной) по нужному сетевому адресу или на отчуждаемый носитель. Угрозы нарушения целостности информации реализуются путем полного или частичного уничтожения (стирания) информации, полной или частичной ее подмены. Угрозы нарушения доступности пользовательской информации реализуются путем изменения пути к файлам с такой информацией (несанкционированной перезаписи файлов в иные каталоги и директории), нарушения таблиц дескрипторов файлов и др. [8 – 11]. При этом, во-первых, имеется существенная неопределенность, относительно какой защищаемой информации и какое конкретно будет выполняться несанкционированное действие с защищаемой информацией. Во-вторых, при реализации всех таких угроз сначала осуществляется проникновение в операционную среду. Таким образом, при оценке защищенности необходимо в первую очередь оценить возможность проникновения в операционную среду в условиях применения мер защиты, а затем – возможность выполнения какого-либо из несанкционированных действий или совокупности таких действий, направленных на нарушение конфиденциальности, целостности или доступности информации.

3. Для количественной оценки защищенности информационного обеспечения необходимо иметь математические модели процессов реализации угроз безопасности информации, используемой для организации и ведения ТЗИ. Некоторые из таких моделей разработаны, например, в [8, 11 – 13]. Однако применительно к оценке защищенности информационного обеспечения в условиях огромного разнообразия угроз безопасности информации и мер защиты от них таких моделей сегодня явно не хватает, поэтому применительно к рассматриваемой проблеме в данной работе был предложен метод, основанный на использовании нечетких оценок вероятностей реализации угроз безопасности информации[8]. Однако применительно к проблеме ИО деятельности по ТЗИ до сих пор не рассматривался. Суть этого метода сводится к следующему.

Пусть в условиях отсутствия мер защиты вероятности реализации угроз безопасности как системной,

8 Например, в статье Язова Ю.К., Середы О.А. «Комплексная оценка эффективности защиты от угроз безопасности с использованием аппарата теории нечетких множеств» // Региональный научный вестник «Информация и безопасность» / ВГТУ Воронеж, 2001 г. Вып.2., в монографии Корченко А.Г. «Построение систем защиты информации на нечетких множествах. Теория и практическое решение»/ Киев: «МК-Пресс», 2006. – 216 с. и др.

так и прикладной информации близки к единице. Тогда ее защищенность может быть оценена нечетким значением показателя g_{prot}, соответствующего нечеткой вероятности того, что угрозы не могут быть реализованы в ИС, рассчитываемым по формуле:

$$g_{prot} = 1 - P_{imp} \cdot \left\{ \gamma_1 \cdot P_{syst} + \gamma_2 \cdot P_{app} \right\}, \quad (15)$$

где P_{imp} – нечеткая оценка вероятности проникновения в операционную среду ИС в условиях применения адекватных мер защиты;

$$P_{imp} = \pi_1 P_{imp.1} + \pi_2 P_{imp.2}, \quad (16)$$

π_1 и π_2 – априорные вероятности реализации первого и второго варианта проникновения соответственно, $\pi_1 + \pi_2 = 1$;

P_{imp1} и P_{imp2} – нечеткие оценки вероятности проникновения при действиях внешнего и внутреннего нарушителя соответственно;

P_{syst} – нечеткая оценка условной вероятности выполнения несанкционированных (деструктивных) действий файлов операционной системы, то есть относительно системной информации, приводящих к отказу в обслуживании пользователей, при условии проникновения в операционную среду и при наличии мер защиты;

P_{app} – нечеткая оценка условной вероятности выполнения несанкционированных действий относительно текстовых, графических, видео- и аудиофайлов, а также исполняемых файлов прикладных программ пользователей[9], то есть относительно пользовательской информации, при условии проникновения в операционную среду и при наличии мер защиты;

γ_1 и γ_2 – априорные вероятности того, что после проникновения будут выполняться действия, направленные на нарушение безопасности системной информации с отказом функционирования ИС (угрозы отказа ИС в обслуживании), или действия, направленные на нарушения целостности, конфиденциальности или доступности пользовательской информации, при этом имеет место условие $\gamma_1 + \gamma_2 = 1$.

Для определения вероятности проникновения учитываются первоочередные меры разграничения доступа такие как:

- межсетевое экранирование;
- идентификация и аутентификация;
- антивирусная защита;
- обнаружение вторжений, в том числе незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама);
- выявление нарушений целостности, доступности и работоспособности программного обеспечения и средств защиты информации, отклонения параметров его настройки от номинальных;
- контроль состава технических средств, в том числе средств защиты информации и сигнализация о выявленных нарушениях;
- прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.

Полагается, что у нарушителя имеется достаточно времени для реализации любой угрозы и, таким образом, оценивается потенциальная возможность такой реализации без учета ее динамики [8, 12].

Если применяются адекватные меры защиты, то угроза проникновения в операционную среду возможна в случае эксплуатации неизвестной ранее уязвимости системного программного обеспечения и внедрения вредоносной программы, обеспечивающей такое проникновение. В настоящее время большинство угроз проникновения реализуются с применением вредоносных программ, при этом имеется два варианта проникновения: первый – из внешней сети, второй – путем проведения сетевой атаки с одного из компьютеров ИС этого органа, организации, предприятия, при этом возможна реализация несанкционированных действий и относительно информации, находящейся на этом компьютере.

При использовании аппарата нечетких множеств [14] наиболее удобным является использование треугольных нечетких чисел. Пример представления нечеткого треугольного числа, например, для вероятности проникновения в операционную среду приведен на рис.1.

На рисунке $\mu_{P_{imp}}(x)$ – функция принадлежности нечеткого числа P_{imp} заданному множеству значений (в данном случае интервалу значений от 0.25 до 0.7). В аналитическом виде функция принадлежности, показанная на рис.1, записывается следующим образом: $\mu_{P_{imp}}(x) = \left\{ \frac{0}{0.25}; \frac{1}{0.4}; \frac{0}{0.7} \right\}$, где в числителях указываются значения функции принадлежности, а в знаменателях значения нечеткого числа.

9 Здесь не рассматриваются маловероятные случаи, когда угрозы одновременно направлены как на нарушение безопасности прикладной информации, так и на отказ в обслуживании пользователей операционной системы.

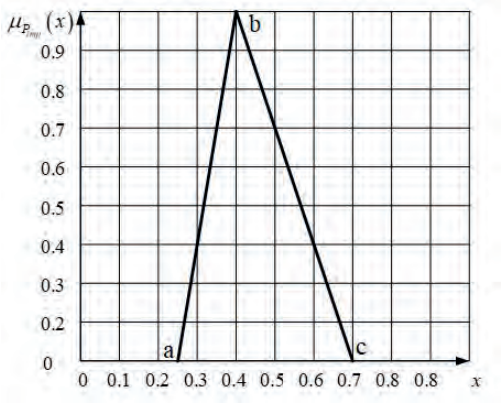

Рис.1. Пример представления треугольного нечеткого числа при оценке вероятности проникновения в операционную среду

Аналогичным образом описывается само нечеткое число, равное примерно 0.4:

$$P_{imp} = \left\{ \begin{array}{c|c|c|c} \mu_{P_{imp}}(x) & 0 & 1 & 0 \\ \hline x & 0.25 & 0.4 & 0.7 \end{array} \right\} \equiv \left\{ \frac{0}{0.25}, \frac{1}{0.4}, \frac{0}{0.7} \right\}$$

Сумма и произведение K треугольных нечетких чисел вида $A_k = \left\{ \frac{0}{a_k}; \frac{1}{b_k}; \frac{0}{c_k} \right\}, k = \overline{1,K}$, представляют собой нечеткие числа следующего вида:

$$\sum_{k=1}^{K} A_k = \left\{ \frac{0}{\sum_{k=1}^{K} a_k}; \frac{1}{\sum_{k=1}^{K} b_k}; \frac{0}{\sum_{k=1}^{K} c_k} \right\},$$

$$\prod_{k=1}^{K} A_k = \left\{ \frac{0}{\prod_{k=1}^{K} a_k}; \frac{1}{\prod_{k=1}^{K} b_k}; \frac{0}{\prod_{k=1}^{K} c_k} \right\}. \quad (17)$$

Последовательно можно рассчитать функции принадлежности для любого числа перемножаемых нечетких чисел. Если необходимо возвести в степень нечеткое число $A = \left\{ \frac{0}{a}; \frac{1}{b}; \frac{0}{c} \right\}$, то из (17) следует:

$$A^K = \left\{ \frac{0}{a^K}; \frac{1}{b^K}; \frac{0}{c^K} \right\}. \quad (18)$$

Наконец, важным моментом арифметики нечетких чисел в случае, когда рассматриваются нечеткие вероятности, является определение дополнения нечеткой вероятности до 1, то есть, если задана вероятность в виде нечеткого треугольного числа $P = \left\{ \frac{0}{a}, \frac{1}{b}, \frac{0}{c} \right\}$, то нечеткое треугольное число $1 - P$ определяется следующим образом:

$$1 - P = \left\{ \frac{0}{1-c}; \frac{1}{1-b}; \frac{0}{1-a} \right\}. \quad (19)$$

Использование аппарата нечетких множеств позволяет учесть неопределенности, которые возникают у специалистов при проведении анализа защищенности ИО деятельности по ТЗИ от угроз безопасности информации.

Вероятность P_{syst} выполнения несанкционированного (деструктивного) действия относительно системной информации, то есть относительно любого из файлов (исполняемых, файлов дескрипторных таблиц и др.), нарушение целостности, уничтожение или модификация которых приводит к нарушению функционирования ИС в условиях применения мер защиты, определяется возможностью запуска и выполнения соответствующих команд операционной системы. Пусть в операционной системе имеется K_{sys} таких файлов, нечеткая оценка вероятности уничтожения, модификации, подмены каждого k-го файла составляет величину $P^{(F)}_{syst.k}$, тогда нечеткая оценка условной вероятности выполнения несанкционированных (деструктивных) действий относительно файлов операционной системы, приводящих к отказу в обслуживании пользователей, при условии проникновения в операционную среду и при наличии мер защиты находится из соотношения:

$$P_{syst} = 1 - \prod_{k=1}^{K_{sys}} \left[1 - P^{(F)}_{syst.k} \right]. \quad (20)$$

Если вместо $P^{(F)}_{syst.i}$ использовать усредненное нечеткое значение вероятности

$$\overline{P^{(F)}_{syst.}} = \frac{1}{K_{sys}} \cdot \sum_{k=1}^{K_{sys}} P^{(F)}_{syst.k}, \quad (21)$$

то

$$P_{syst} = 1 - \left[1 - \overline{P^{(F)}_{syst}} \right]^{K_{sys}}. \quad (22)$$

Далее проводится дефаззификация, то есть получение четкого значения этой вероятности. При этом может быть использованы разные методы, такие как методы среднего максимума, «центра тяжести», центра сумм и т.д. [13].

Наиболее корректным из них является метод центра тяжести, при этом, если получено треугольное число в виде: $P_{syst} = \left\{ \frac{0}{a_{syst}}; \frac{1}{b_{syst}}; \frac{0}{c_{syst}} \right\}$, то четкое значение этой вероятности рассчитывается следующим образом:

$$P_{syst} = \frac{\int_{a_{syst}}^{b_{syst}} x \cdot \mu_{P_{syst}}(x)\,dx + \int_{b_{syst}}^{c_{syst}} x \cdot \mu_{P_{syst}}(x)\,dx}{\int_{a_{syst}}^{b_{syst}} \mu_{P_{syst}}(x)\,dx + \int_{b_{syst}}^{c_{syst}} \mu_{P_{syst}}(x)\,dx}, \quad (23)$$

откуда

$$P_{syst} = \frac{b_{syst}^2 - a_{syst}b_{syst} - a_{syst}^2 - b_{syst}c_{syst} + 2c_{syst}^2}{3\left(c_{syst} - a_{syst}\right)} \quad (24)$$

Например, если $P_{syst} = \left\{ \frac{0}{0.6}; \frac{1}{0.8}; \frac{0}{0.9} \right\}$, то после дефаззификации $P_{syst} = 0.77$.

Нечеткая оценка условной вероятности P_{app} выполнения несанкционированных действий относительно пользовательской информации находится следующим образом.

Пусть в ИС имеются K_{conf} файлов, содержащих защищаемую информацию конфиденциального характера, K_{int} файлов, содержащих информацию, целостность которой не должна быть нарушена, и K_{acc} файлов, доступность к которым должна быть обеспечена. Тогда нечеткая оценка вероятности выполнения несанкционированных действий относительно указанных файлов определяется из соотношения:

$$P_{app} = \theta_{conf} \cdot P_{conf} + \theta_{int} \cdot P_{int} + \theta_{acc} \cdot P_{acc}, \quad (25)$$

где $P_{conf}, P_{int}, P_{acc}$ – нечеткие оценки вероятностей выполнения действий, направленных на нарушение конфиденциальности, целостности и доступности хотя бы одного из соответствующих файлов с пользовательской информацией;

θ_{conf}, θ_{int}, θ_{acc} – априорные вероятности того, что будет выбрано действие, направленное на нарушение конфиденциальности, целостности или доступности пользовательской информации соответственно;

K_j – количество файлов, защищаемых от j-го несанкционированного действия, $j = \overline{1,3}$, при этом $K_1 \equiv K_{conf}, K_2 \equiv K_{\text{int}}, K_3 \equiv K_{acc}$;

θ_j – априорная вероятность того, что будет выбрано для выполнения j-е несанкционированное действие, направленное на нарушение или конфиденциальности, или целостности или доступности информации, $\sum_{j=1}^{3} \theta_j = 1$.

Если рассматривается наиболее жесткая оценка защищенности, когда считается, что недопустимо нарушение конфиденциальности, целостности или доступности ни одного из файлов с пользовательской информацией в системе, то

$$P_{conf} = 1 - \prod_{k=1}^{K_{conf}} \left[1 - P_{conf.k} \right];$$
$$P_{int} = 1 - \prod_{k=1}^{K_{int}} \left[1 - P_{int.k} \right]; P_{acc} = 1 - \prod_{k=1}^{K_{acc}} \left[1 - P_{acc.k} \right], \quad (26)$$

где $P_{conf.k}, P_{int.k}, P_{acc.k}$ – нечеткие оценки вероятностей выполнения действий, направленных на нарушение конфиденциальности, целостности или доступности k-го файла соответственно.

Если рассматривается менее жесткая оценка защищенности, когда считается, что недопустимо нарушение сразу всех рассматриваемых файлов пользовательской информации, то

$$P_{conf} = \prod_{k=1}^{K_{conf}} P_{conf.k}; P_{int} = \prod_{k=1}^{K_{int}} P_{int.k}; P_{acc} = \prod_{k=1}^{K_{acc}} P_{acc.k}. \quad (27)$$

Если использовать усредненную оценку нечетких значений вероятностей по каждому из возможных несанкционированных действий, то формула (25) преобразуется к виду:

$$P_{app} = \theta_{conf} \cdot \left[1 - (1 - \overline{P_{conf}})^{K_{conf}} \right] + \\ + \theta_{int} \cdot \left[1 - (1 - \overline{P_{int}})^{K_{int}} \right] + \theta_{acc} \cdot \left[1 - (1 - \overline{P_{acc}})^{K_{acc}} \right], \quad (28)$$

где $\overline{P_{conf}}, \overline{P_{\text{int}}}, \overline{P_{acc}}$ – средние вероятности выполнения несанкционированных действий, направленных соответственно на нарушение конфиденциальности, целостности и доступности информации,

$$\overline{P_{conf}} = \frac{1}{K_{conf}} \cdot \sum_{k=1}^{K_{conf}} P_{conf.k};$$
$$\overline{P_{int}} = \frac{1}{K_{int}} \cdot \sum_{k=1}^{K_{int}} P_{int.k}; \overline{P_{acc}} = \frac{1}{K_{acc}} \cdot \sum_{k=1}^{K_{acc}} P_{acc.k}; \quad (29)$$

$\theta_{conf}, \theta_{int}, \theta_{acc}$ – априорные вероятности вы-

Таблица 2

Шкала перевода количественных значений показателя защищенности информационного обеспечения в качественные суждения

Количественные значения показателя защищенности g_{prot}	$g_{prot} > 0.99$	$0.99 \geq g_{prot} > 0.8$	$g_{prot} < 0.8$
Качественные суждения об уровне защищенности	Высокий	Средний	Низкий

бора несанкционированных действий, $\theta_{conf} \equiv \theta_1, \theta_{int} \equiv \theta_2, \theta_{acc} \equiv \theta_3$;

$P_{conf.k}, P_{int.k}, P_{acc.k}$ – вероятности выполнения несанкционированного действия относительно k-го файла, направленного на нарушение соответственно конфиденциальности, целостности или доступности содержащейся в нем информации.

Рассчитанный по формуле (15) показатель защищенности информационного обеспечения может быть переведен в качественные суждения по шкале, указанной в табл. 2.

Пример. Пусть количество системных файлов, реализация угрозы нарушения целостности или доступности которых приводит к отказу в обслуживании (например, к «зависанию» операционной системы) составляет $K_{syst} = 50$. Угрозы могут реализованы как по сети, так и с одного из компьютеров ИС, при этом возможности проникновения в операционную среду ИС в условиях мер защиты как по первому, так и по второму варианту проникновения равны, то есть вероятности $P_{imp}^{(1)} = P_{imp}^{(2)} = \left(\frac{0}{7\cdot10^{-3}}, \frac{1}{10^{-2}}, \frac{0}{3\cdot10^{-2}}\right)$ и $\pi_1 = \pi_2 = 0.5\cdot10^{-2}$. Априорные вероятности того, что угроза будет реализована относительно системной или пользовательской информации равны соответственно $\gamma_{syst} = 0.6$ и $\gamma_{app} = 0.4$, а нечеткая оценка вероятности того, что относительно одного системного файла будет выполнено несанкционированное действие, составляет величину $P_{syst.k}^{(F)} = \left(\frac{0}{0.01}, \frac{1}{0.02}, \frac{0}{0.03}\right)$, одинаковую для всех системных файлов.

Пусть количество файлов пользовательской информации, относительно которых могут быть реализованы угрозы нарушения конфиденциальности, целостности и доступности, равны соответственно $K_{conf} = 10, K_{int} = 20, K_{acc} = 7$, а априорные вероятности выбора действий $\theta_{conf} = 0.6, \theta_{int} = 0.3, \theta_{acc} = 0.1$. Нечеткие значения вероятностей выполнения несанкционированных действий относительно файлов с пользовательской информацией в случае нарушения конфиденциальности, целостности и доступности одинаковы для соответствующих файлов

$$P_{conf.k} = \left(\frac{0}{0.2}, \frac{1}{0.3}, \frac{0}{0.4}\right),$$

$$P_{int.k} = \left(\frac{0}{0.88}, \frac{1}{0.96}, \frac{0}{0.99}\right),$$

$$P_{acc.k} = \left(\frac{0}{10^{-3}}, \frac{1}{10^{-2}}, \frac{0}{10^{-1}}\right).$$

Необходимо оценить защищенность информации, используемой в деятельности по ТЗИ.

Усредненное нечеткое значение вероятности реализации угроз относительно системных файлов рассчитывается по формуле (20): $\overline{P_{syst.}^{(F)}} = P_{syst}^{(F)} = \left(\frac{0}{0.01}, \frac{1}{0.02}, \frac{0}{0.03}\right)$, при этом дополнение до 1 этой вероятности представляет собой нечеткое число: $1 - P_{syst}^{(F)} = \left(\frac{0}{0.97}, \frac{1}{0.98}, \frac{0}{0.99}\right)$.

Отсюда в соответствии с формулами (17), (18) и (21) получаем $P_{syst} = \left(\frac{0}{0.4}, \frac{1}{0.64}, \frac{0}{0.78}\right)$.

Применительно к пользовательской информации находим аналогично:

$$P_{conf} = \left(\frac{0}{0.89}, \frac{1}{0.97}, \frac{0}{0.994}\right);$$

$$P_{\text{int}} = \left(\frac{0}{0.12}, \frac{1}{0.15}, \frac{0}{0.2}\right);$$

$$P_{acc} = \left(\frac{0}{0.007}, \frac{1}{0.07}, \frac{0}{0.52}\right).$$

По формуле (27) находим нечеткую оценку вероятности выполнения несанкционированных действий относительно указанных файлов: $P_{app} = \left(\frac{0}{0.57}, \frac{1}{0.63}, \frac{0}{0.7}\right)$. Далее по формуле (15) оценивается нечеткое значение показателя защищенности $g_{prot} = \left(\frac{0}{0.98}, \frac{1}{0.993}, \frac{0}{0.997}\right)$.

В результате дефаззификации по формуле, аналогичной формуле (24), получаем $g_{prot} = 0.98$. В соответствии с табл. 2 уровень защищенности информационного обеспечения – средний.

Выводы

1. Разработаны математические модели для количественной оценки показателей полноты, достоверности, актуальности и защищенности информационного обеспечения деятельности по организации и ведению ТЗИ в органах власти, организациях и предприятиях и показана их связь с комплексным показателем эффективности такого обеспечения. Модели необходимы при построении систем информационного обеспечения деятельности по ТЗИ и позволяют перейти от качественных к количественным оценкам его эффективности и тем самым, во-первых, существенно повысить обоснованность требований к СИО, во-вторых, автоматизировать процессы информационного обеспечения деятельности по ТЗИ в органах власти, организациях и предприятиях.

2. Предложенные показатели качества информационного обеспечения и аналитические соотношения для их расчета использованы при построении и сопровождении функционирования информационно-аналитической системы ФСТЭК России, а также в ходе аудита при проверке информационного обеспечения деятельности по ТЗИ в органах власти, организациях и предприятиях.

Литература:

1. Ю.К.Язов. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К.Язов, С.В.Соловьев. Воронеж: Кварта, 2018. – 588 с.
2. Соловьев С. В. Информационное обеспечение деятельности по технической защите информации / С.В. Соловьев, Ю.К. Язов / Вопросы кибербезопасности. 2021, №1 (41), с. 69–79. DOI: 10.21681/2311-3456-2021-1-69-79
3. Сюнтюренко О.В. Информационное обеспечение: факторы развития, управление, эффективность. Научно-техническая информация. Серия 2: Информационные процессы и системы. 2016. №6. С 7–15.
4. Трояновская М. А. Информационное обеспечение деятельности органов государственного управления: понятие и значение. Международный научно-исследовательский журнал. 2020. №5-2(95). С.100-103.
5. Чернов В. А. Теория экономического анализа. Изд-во ООО «Проспект». – М.: 2017.
6. Сазанова Л. А. Анализ особенностей производственной функции Кобба-Дугласа. В сборнике: Актуальные тенденции и инновации в развитии российской науки / сборник научных статей. Москва. 2020. С. 120–123.
7. Колесникова, Е. В. Моделирование развития информационного обеспечения организационно-технических систем технической защиты информации с учетом прогноза изменений предметной области / Е. В. Колесникова // Сборник докладов международной конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий – РЭУС-2016», Российское научно-техническое общество радиотехники, электроники и связи им. А. С. Попова. – 2016. – том 2 – С. 564–569.
8. Язов Ю. К. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Санкт-Петербург: Наукоемкие технологии, 2023. – 258 с.
9. Васильев В. И., Вульфин А. М., Кириллова А. Д., Кучкарова Н. В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. № 3. С. 110–134. DOI: 10.24412/2410-9916-2021-3-110-134.
10. Бутрик Е.Е. Подход к определению актуальных угроз безопасности информации в автоматизированных системах управления технологическими процессами с применением банка данных угроз безопасности информации ФСТЭК России / Е.Е.Бутрик, С.В.Соловьев // Информация и безопасность. – Воронеж,2018. – Выпуск 19 (2). – с.203 – 210.
11. Олифер, В.Г. Безопасность компьютерных систем / В.Г.Олифер, Н.А.Олифер – М.: Горячая линия – Телеком, 2017.– 644 с.: илл.
12. Язов, Ю.К. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах: монография / Ю. К. Язов, А. В. Анищенко. – Воронеж: Кварта,2020. 173 с.
13. Рубцова, И.О. Об оценке эффективности защиты электронного документооборота с применением аппарата сетей Петри-Маркова [Текст] / И. О. Рубцова, Ю. К. Язов, О.С. Авсентьев, А.О. Авсентьев // Труды СПИИРАН, №5(25) – 2019.
14. Пегат, А. Нечеткое моделирование и управление / А.Пегат; пер. с англ.– 2-е изд. – М.: БИНОМ. Лаборатория знаний, 2015. – 798 с.: ил. – (Адаптивные интеллектуальные системы).

MATHEMATICAL MODELS FOR ASSESSING QUALITY INDICATORS OF INFORMATION SUPPORT OF TECHNICAL INFORMATION PROTECTION ACTIVITIES

Soloviev S.V.[10], Yazov Yu.K.[11], Teplinskikh A.A.[12]

The purpose of the research *is to develop mathematical models for quantitative assessment of indicators of completeness, reliability, relevance and security of information support for organizing and maintaining technical information protection in government agencies, organizations and enterprises*

The methods of research are: *mathematical apparatus of factor analysis, methods of set theory, fuzzy number theory and probability theory.*

The result of the research: *indicators for assessing the quality of information support for technical information protection activities are proposed: completeness, reliability, relevance and security of information necessary for such support; the correlation of these quality indicators with a comprehensive indicator for assessing the effectiveness of information support is revealed. Taking into account the content of the subject area model of technical information protection, it is shown that the completeness, reliability and relevance of security information support is determined by the sets of: functions provided for in the subject area model and actually implemented in the information system; tasks, the solution of which ensures the implementation of functions; information objects and their attributes to be used in accordance with the domain model and actually used in solving information security problems. To assess the indicator of information security required for information support of information protection activities, it is proposed to use a device for fuzzy estimates of the probabilities of the implementation of threats regarding system and user information, violation of the confidentiality, integrity or availability of which can disrupt the information support.*

Analytical relations have been developed to calculate the quality indicators of in-formation support, makes it possible to quantify the requirements for information support of information protection activities and for the created information support systems for government agencies, organizations and enterprises.

Keywords: *information system, effectiveness, subject area, completeness, reliability, relevance, information protection.*

References

1. Ju.K.Jazov. Organizacija zashhity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa: monografija / Ju.K.Jazov, S.V.Solov'ev. Voronezh: Kvarta, 2018. – 588 s.
2. Solov'ev S. V. Informacionnoe obespechenie dejatel'nosti po tehnicheskoj zashhite informacii / S.V. Solov'ev, Ju.K. Jazov / Voprosy kiberbezopasnosti. 2021, №1 (41), s. 69–79. DOI: 10.21681/2311-3456-2021-1-69-79
3. Sjuntjurenko O.V. Informacionnoe obespechenie: faktory razvitija, upravlenie, jeffektivnost'. Nauchno-tehnicheskaja informacija. Serija 2: Informacionnye processy i sistemy. 2016. №6. S 7–15.
4. Trojanovskaja M. A. Informacionnoe obespechenie dejatel'nosti organov gosudarstvennogo upravlenija: ponjatie i znachenie. Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. 2020. №5-2(95). S.100-103.
5. Chernov V. A. Teorija jekonomicheskogo analiza. Izd-vo 000 «Prospekt». – M.: 2017.
6. Sazanova L. A. Analiz osobennostej proizvodstvennoj funkcii Kobba-Duglasa. V sbornike: Aktual'nye tendencii i innovacii v razvitii rossijskoj nauki / sbornik nauchnyh statej. Moskva. 2020. S. 120–123.
7. Kolesnikova, E. V. Modelirovanie razvitija informacionnogo obespechenija organizacionno-tehnicheskih sistem tehnicheskoj zashhity informacii s uchetom prognoza izmenenij predmetnoj oblasti / E. V. Kolesnikova // Sbornik dokladov mezhdunarodnoj konferencii

10 Sergey V. Soloviev, Ph.D. (Technology), Associate Professor, Deputy Head ofof the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control of Russia, Voronezh, Russian Federation. E-mail:sersol@mail.ru

11 Yuri K. Yazov, Dr.Sc. (Technology), Professor, Principal Researcher at the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control of Russia, Voronezh, Russian Federation. E-mail:yazoff_1946@mail.ru

12 Alexander A. Teplinskikh, Researcher of the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control of Russia, Voronezh, Russian Federation. E-mail:ma4karek48@yandex.ru

«Radiojelektronnye ustrojstva i sistemy dlja infokommunikacionnyh tehnologij – RJeUS-2016», Rossijskoe nauchno-tehnicheskoe obshhestvo radiotehniki, jelektroniki i svjazi im. A. S. Popova. – 2016. – tom 2 – S. 564–569.
8. Jazov Ju. K. Metodologija ocenki jeffektivnosti zashhity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa: monografija / Ju.K. Jazov, S.V. Solov'ev. – Sankt-Peterburg: Naukoemkie tehnologii, 2023. – 258 s.
9. Vasil'ev V. I., Vul'fin A. M., Kirillova A. D., Kuchkarova N. V. Metodika ocenki aktual'nyh ugroz i ujazvimostej na osnove tehnologij kognitivnogo modelirovanija i Text Mining // Sistemy upravlenija, svjazi i bezopasnosti. 2021. № 3. S. 110–134. DOI: 10.24412/2410-9916-2021-3-110-134.
10. Butrik E.E. Podhod k opredeleniju aktual'nyh ugroz bezopasnosti informacii v avtomatizirovannyh sistemah upravlenija tehnologicheskimi processami s primeneniem banka dannyh ugroz bezopasnosti informacii FSTJeK Rossii / E.E.Butrik, S.V.Solov'ev // Informacija i bezopasnost'. – Voronezh,2018. – Vypusk 19 (2). – s.203 – 210.
11. Olifer, V.G. Bezopasnost' komp'juternyh sistem / V.G.Olifer, N.A.Olifer – M.: Gorjachaja linija – Telekom, 2017.– 644 s.: ill.
12. Jazov, Ju.K. Seti Petri-Markova i ih primenenie dlja modelirovanija processov realizacii ugroz bezopasnosti informacii v informacionnyh sistemah: monografija / Ju. K. Jazov, A. V. Anishhenko. – Voronezh: Kvarta,2020. 173 s.
13. Rubcova, I.O. Ob ocenke jeffektivnosti zashhity jelektronnogo dokumentooborota s primeneniem apparata setej Petri-Markova [Tekst] / I. O. Rubcova, Ju. K. Jazov, O.C. Avsent'ev, A.O. Avsent'ev // Trudy SPIIRAN, №5(25) – 2019.
14. Pegat, A. Nechetkoe modelirovanie i upravlenie / A.Pegat; per. s angl.– 2-e izd. – M.: BINOM. Laboratorija znanij, 2015. – 798 s.: il. – (Adaptivnye intellektual'nye sistemy).

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ ПРОЦЕССОВ И МЕР, ОБЕСПЕЧИВАЮЩИХ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ СИСТЕМЫ С ГРАФОВОЙ СУБД

Карапетьянц Марк[1], Плаксий К.В.[2], Никифоров А.А.[3]

Аннотация

Цель: *Исследование популярных процессов и мер информационной безопасности в информационных системах с графовой СУБД и оценка их применимости с использованием инструментов сканирования уязвимостей и методов тестирования безопасности.*

Методы. *Теория графов, системный анализ, защита от инъекций, фильтрация ввода, Brute force.*

Результаты: *Выявлены основные угрозы и уязвимости для графовой СУБД. Проведённый анализ используемых процессов и мер защиты информации для SQL СУБД позволил определить перечень мер, наиболее подходящих для применения в графовых СУБД. В ходе исследования производилось тестирование безопасности Neo4j посредством использования перечня программных средств и утилит для раскрытия уязвимостей, которые в дальнейшем были устранены выявленными процессами и мерами защиты информации. В заключение проведена проверка и оценка защищенности комбинации средств защиты графовой СУБД. Полученные результаты имеют практическую значимость для различных информационных систем, внедряющих графовую СУБД в бизнес-процессы. Они также могут быть использованы для разработки основных критериев, необходимых при создании или улучшении графовых систем управления базами данных.*

Научная новизна. *Новизна исследования заключается в доказательстве применимости процессов и мер, обеспечивающих информационную безопасность информационной системы с графовой СУБД.*

Ключевые слова: *графовые СУБД, процессы и меры, информационная безопасность, Acunetix, Nmap, OWASP ZAP proxy, Burp Suite, Neo4j, угрозы, уязвимости, сканер уязвимости.*

DOI: 10.21681/2311-3456-2023-6-96-111

Введение

Базы данных NoSQL стали известны с 2009 года, и за последние несколько лет понятие «NoSQL» приобрело очень большую огласку по всему миру, это дало толчок к активному развитию и продвижению на рынке от разных производителей систем управления базами данных (СУБД). Первоначальное использование этих технологий стимулировало прогресс в развитии web-технологий и социальных сервисов. Это также привело к пересмотру множества подходов к хранению и обработке данных. На это развитие также повлияла проблема, связанная с использованием традиционных SQL СУБД, которые для поставленных задач были дорогостоящими или имели низкую производительность. Примером начала применения нереляционных СУБД является использование технологии Больших данных, которые на сегодняшний день имеют большую корреляцию с рассматриваемыми СУБД[4].

Одной из разновидностей NoSQL являются графовые СУБД, которые имеют немалую популярность среди пользователей, так как хранение в традиционных табличных формах не всегда отвечают их требованиям. NoSQL базы данных отличаются высокой произво-

4 Keith D. Foote. Graph Databases: An Overview. Datavetsity.2019 [Электронный ресурс] // Режим доступа к ресурсу: https://www.dataversity.net/graph-databases-an-overview (Дата обращения: 10.01.2023).

1 Карапетьянц Марк, аспирант Национального исследовательского ядерного университета «МИФИ», Москва, Россия. E-mail: Mkarapetyants@mephi.ru, ORCID: 0009-0002-3262-1138.

2 Плаксий Кирилл Владимирович, старший преподаватель Национального исследовательского ядерного университета «МИФИ», Москва, Россия. E-mail: KVPlaksii@mephi.ru, ORCID: 0000-0002-8949-6772.

3 Никифоров Андрей Александрович, старший преподаватель Национального исследовательского ядерного университета «МИФИ», Москва, Россия. E-mail: andreinikiforov993@gmail.com, ORCID: 0000-0002-2726-0000.

дительностью и скоростью. Распределенная архитектура СУБД обеспечивает простое масштабирование, позволяет автоматически распределять данные между несколькими серверами и повышает скорость чтения данных. На данный момент самым популярным решением в этой области является Neo4j, которая занимает первое место среди графовых СУБД (рис. 1).

Несмотря на то, что графовые СУБД способны обрабатывать большой поток информации, обладая такими свойствами, как гибкость, масштабируемость и производительность, появляется проблема, связанная с плохой безопасностью данных в них, что может негативно сказаться на деятельности компании [1].

Обеспечение информационной безопасности графовых СУБД начинается с определения и устранения существующих уязвимостей. Для ликвидации уязвимостей необходимо использование комплексного подхода к защите данных в графовых СУБД. Также для создания эффективной системы обеспечения ИБ СУБД необходимо оценить актуальные угрозы ИБ, которые существуют на сегодняшний день.

Данное исследование продолжает работу, начатую авторами в [2], и ставит своей целью дополнить основной перечень уязвимостей и угроз ИБ для графовых СУБД, применить выработанный перечень методов защиты данных, используемых для устранения выявленных уязвимостей, и провести тестирование безопасности графовой СУБД на примере Neo4j [3]. Для выполнения поставленной цели решаются следующие задачи: актуализировать список угроз и уязвимостей графовых СУБД, применить средства тестирования СУБД для поиска существующих уязвимостей Neo4j, использовать перечень процессов и мер защиты информации для устранения уязвимостей СУБД, провести повторное тестирование после внедрения процессов и мер для оценки защищенности системы.

1. Угрозы, уязвимости и методы защиты данных в графовых СУБД

Исследований в области уязвимостей и угроз для графовых СУБД не так много по той причине, что данные системы только набирают популярность в IT-отрасли. Но, основываясь на предыдущих работах авторов и на других трудах в этой области, был дополнен основной перечень угроз и уязвимостей (табл. 1) и подобраны к ним соответствующие меры для их устранения[5].

Для противодействия данным угрозам был определен актуальный перечень процессов и мер, которые позволяют устранить выявленные уязвимости в графовой СУБД Neo4j [4].

Rank Jan 2023	Rank Dec 2022	Rank Jan 2022	DBMS	Database Model	Score Jan 2023	Score Dec 2022	Score Jan 2022
1.	1.	1.	Neo4j	Graph	55.84	-1.49	-2.19
2.	2.	2.	Microsoft Azure Cosmos DB	Multi-model	37.96	+0.01	-2.08
3.	3.	3.	Virtuoso	Multi-model	5.88	-0.07	+0.50
4.	4.	4.	ArangoDB	Multi-model	5.07	-0.27	+0.34
5.	5.	5.	OrientDB	Multi-model	4.48	-0.09	-0.07
6.	↑ 7.	↑ 7.	Amazon Neptune	Multi-model	2.81	-0.09	+0.18
7.	↓ 6.	↑ 8.	JanusGraph	Graph	2.64	-0.35	+0.25
8.	8.	↓ 6.	GraphDB	Multi-model	2.53	+0.06	-0.33
9.	9.	9.	TigerGraph	Graph	2.20	+0.13	+0.18
10.	↑ 11.	↑ 11.	Dgraph	Graph	1.80	+0.08	+0.29
11.	↓ 10.	↑ 12.	Fauna	Multi-model	1.77	-0.11	+0.41
12.	12.	↓ 10.	Stardog	Multi-model	1.62	-0.04	-0.27
13.	↑ 14.	13.	Giraph	Graph	1.53	+0.13	+0.22
14.	↑ 16.	↑ 15.	NebulaGraph	Graph	1.51	+0.37	+0.37
15.	↓ 13.	↓ 14.	AllegroGraph	Multi-model	1.39	-0.03	+0.15
16.	↓ 15.	↑ 18.	TypeDB	Multi-model	1.34	+0.07	+0.58
17.	↑ 18.	↑ 20.	Memgraph	Graph	1.32	+0.27	+0.94
18.	↓ 17.	↓ 16.	Blazegraph	Multi-model	1.13	-0.01	+0.17
19.	19.	↓ 17.	Graph Engine	Multi-model	1.07	+0.06	+0.22
20.	20.	↓ 19.	InfiniteGraph	Graph	0.61	+0.06	+0.14

Рис.1. Рейтинг DB-engines графовых хранилищ [6]

5 Hostingdata. List of NoSQLdatabase management systems [Электронный ресурс] // Режим доступа к ресурсу: https://hostingdata.co.uk/nosql-database/ (Дата обращения: 09.01.2023).

6 DB-Engines Рейтинг графовых БД. URL: https://db-engines.com/en/ranking/graph+dbms (дата обращения: 15.10.2020).

Таблица 1

Меры устранения уязвимостей графовых СУБД

Угрозы	Уязвимости	Процессы и меры устранения уязвимостей
Угроза обхода некорректно настроенных механизмов аутентификации	Уязвимость в системе аутентификации	Использование средств разграничения доступа: — Active Directory, OpenLDAP на основе сетевых протоколов аутентификации LDAP (Lightweight Directory Access Protocol) и Kerberos; — аутентификация с помощью токенов; использование компонентов экосистемы Apache Hadoop.
Угроза использования механизмов авторизации для повышения привилегий	Уязвимость в системе авторизации	
Угроза несанкционированного создания учётной записи пользователя	Уязвимость, связанная с недостатками разграничения доступа	Использование внутренней системы разграничения доступа для пользователей
Угроза несанкционированного удаления защищаемой информации		
Угроза повышения привилегий		
Угроза несанкционированного копирования защищаемой информации	Нешифрованный текст	Использование средств шифрования: — алгоритм шифрования AES (Advanced Encryption Standard); — использование HTTPS для шифрования сетевого взаимодействия; — использование компонента экосистемы Apache Hadoop, Cloudera, обеспечивающего шифрование данных HDFS-файлов (Hadoop Distributed File System).
Угроза приведения системы в состояние «отказ в обслуживании»	Уязвимость переполнения буфера и отказа в обслуживании	Использование резервных копий или сторонних продуктов Apache Hadoop для хранения данных: — Распределенная между узлами вычислительного кластера файловая система HDFS (Hadoop Distributed File System); — MapReduce для распределенных операций предварительной обработки
Угроза несанкционированной модификации защищаемой информации	Инъекции в регулярных выражениях	— Проверка входных данных; — использование компонента экосистемы Apache Hadoop Native Auditing, журналов аудита периметра на шлюзе Knox, мониторинга запросов доступа, операций обработки и изменения данных; — ограничение использования регулярных выражений и REST-интерфейса.
Угроза межсайтового скриптинга	Инъекции кода, манипуляции с REST-интерфейсом	
Угроза межсайтовой подделки запроса		
Угроза внедрения кода или данных	Уязвимость контроля доступа к файлам СУБД	Использование внутреннего разграничения доступа в ОС путём присваивания прав neo4j, а также обеспечивая выполнение функций: чтение, изменение и запуск, только от имени «neo4j»
Угроза доступа к защищаемым файлам с использованием обходного пути		
Угроза несанкционированного доступа к аутентификационной информации		
Угроза удаления аутентификационной информации		
Угроза использования слабостей кодирования входных данных	Уязвимость программного кода	Поддержка постоянного обновления ПО, так как данная уязвимость образуется на этапе разработки ПО
Угроза исследования механизмов работы программы		

2. Инструменты тестирования безопасности графовой СУБД на примере Neo4j

Необходимость в проведении тестирования заключается в том, что нужно определить, где у системы имеются недостатки или какие-либо уязвимости в конфигурации безопасности. Результаты проведенного тестирования позволят в дальнейшем снизить риски и смягчить последствия нежелательного доступа к БД [5]. Регулярные проверки безопасности также необходимы для защиты конфиденциальных данных организации от злоумышленников.

Процесс тестирования безопасности включает в себя 4 этапа:

1. Подготовка среды;
2. Проведение теста;
3. Оценка результатов;
4. Точная отчетность.

Выделяют основные типы проведения тестирования БД:

— Тест на проникновение – это процесс имитации кибератаки на сеть, компьютерную систему или веб-приложение для обнаружения в них любых уязвимостей;
— Сканер уязвимостей – это использование программы для сканирования системы на наличие известных уязвимостей с целью их устранения и исправления;
— Аудит безопасности – это процесс оценки реализации и соответствия политик и стандартов безопасности организации;
— Оценка рисков – это процесс определения и анализа потенциальных угроз и возможных негативных последствий для достижения целей или выполнения задач.

На сегодняшний день для проверки безопасности в большинстве случаев используют инструменты, которые за счет быстрого выполнения своих задач существенно экономят время. Для проверки безопасности и проведения тестирования существуют разнообразные решения, включая как корпоративные, так и решения с открытым исходным кодом. Каждое из них предлагает свой уникальный набор функций, которые имеют различную специализацию и применимость. Это позволяет выявить ошибки и уязвимости в программном обеспечении перед его эксплуатацией [6].

В ходе исследования были использованы следующие варианты ПО:

— Burp Suite. Burp Suite — это интегрированная платформа для тестирования безопасности веб-приложений как в ручном, так и в автоматическом режимах. Программа кроссплатформенна и за счет наличия различных инструментов имеет возможность проводить процесс тестирования начиная от составления карты сайта до эксплуатации найденной уязвимости[7].
— Zed Attack Proxy. OWASP Zed Attack Proxy (ZAP) — это один из самых популярных бесплатных инструментов безопасности, он активно поддерживается сотнями волонтёров со всего мира. Он может помочь автоматически найти уязвимости безопасности в веб-приложениях во время разработки и тестирования. Этот инструмент также прекрасно подходит для опытных пентестеров, которые хотят проводить ручное тестирование безопасности.
— NMAP. Nmap или network mapper представляет собой набор инструментов функционального тестирования и тестирования на проникновение для всей сети, включая сканирование портов и обнаружение уязвимостей. Скрипты Nmap scripting engine (NSE) Script – одна из самых популярных и сильных возможностей Nmap. Данные скрипты сканирования уязвимостей Nmap имеют большую популярность у специалистов по тестированию на проникновение и злоумышленников для изучения общеизвестных уязвимостей.
— Acunetix. Acunetix (от Invicti) — это решение для сканирования кибербезопасности и веб-уязвимостей, предлагающее технологию автоматического тестирования веб-безопасности, которая позволяет организациям сканировать и проверять сложные, аутентифицированные веб-сайты с большим количеством HTML5 и JavaScript.

Выбор данных средств был сделан на основе доступности, результативности и надежности ПО. На сегодняшний день в связи с геополитической ситуацией в распоряжении у российских авторов находится небольшое количество инструментов для тестирования. При этом не существует полноценного теста безопасности гравофых СУБД, поэтому будут рассмотрены основные варианты, которые есть в открытых источниках.

3. Проверка безопасности Neo4j

На основе вышеописанных утилит и программ была проведена проверка безопасности графовой СУБД Neo4j без предварительного применения процессов и мер защиты информации. В тестах с Burp Suite происходит анализ защищенности графовой СУБД, кото-

7 SkillFactory. Burp Suite [Электронный ресурс] // Режим доступа к ресурсу: https://blog.skillfactory.ru/glossary/burp-suite/ (Дата обращения: 10.01.2023).

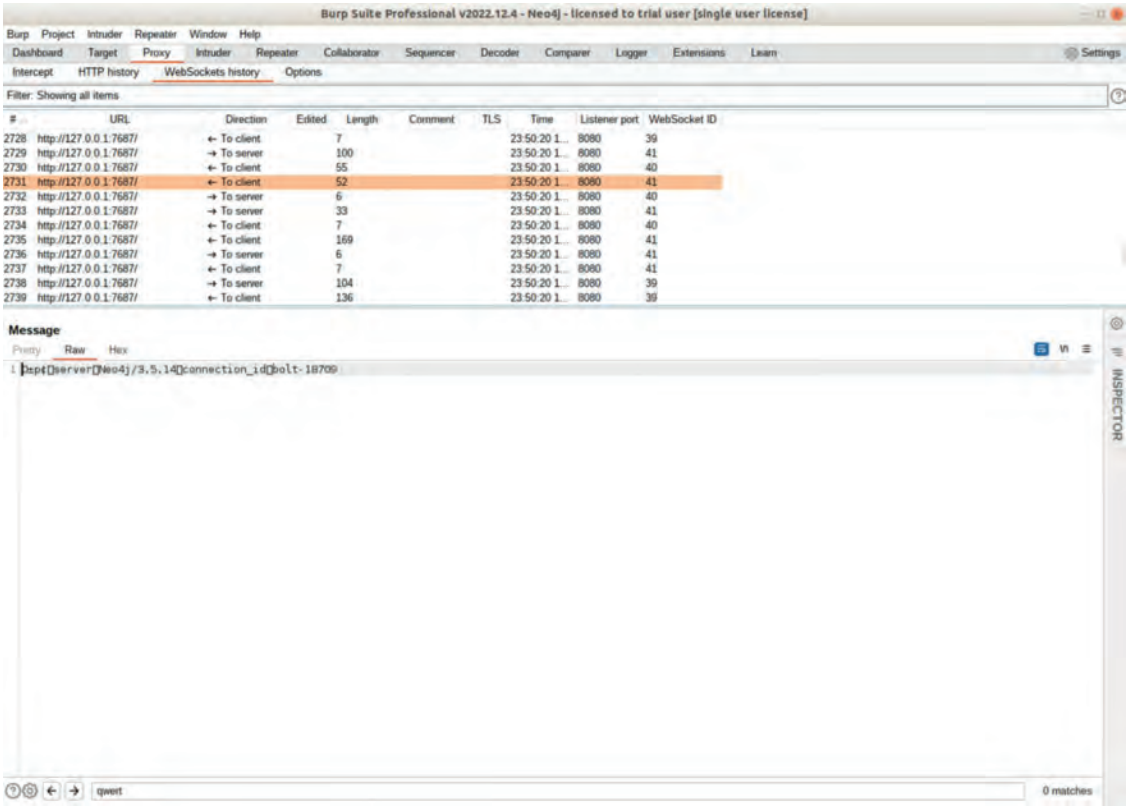

Рис.2. Отслеживание версии Neo4j

рая запускается по адресу «http://127.0.0.1:7474». Была поставлена задача выявить информацию, которая передается между клиентом и сервером. В большинстве веб-ресурсов плохо защищены поля ввода, из-за чего можно проводить атаку типа Brute force с помощью специальных утилит вроде Burp Suite. Но в данном случае провести такого типа атаку через интерфейс Neo4j не оказалось возможным [7].

При помощи утилиты удалось отследить передачу информации, отчетливо проследить запросы, которые передаются как серверу, так и к клиенту. В данном случае был произведен ввод корректной информации учетной записи, которая имеется в базе данных Neo4j. Удалось увидеть, как в открытом виде передаются данные логина и пароля. Это происходит по причине использования протокола http, который почти не шифрует данные при передаче. Помимо учетных данных, авторы выяснили версию установленной СУБД (рис.2), а также были перехвачены основные роли, которые присвоены пользователю.

С помощью программы Burp Suite Community можно отслеживать запросы, передаваемые между клиентом и сервером. Это может означать, что при изучении ИС злоумышленник может получить доступ к идентификационным данным пользователя, что позволит ему несанкционированно войти в систему.

Также с помощью Burp Suite можно сканировать веб-приложения на наличие уязвимостей. В ходе исследования сканер смог выявить 3 проблемы (рис. 3):

— Отправка пароля открытым текстом. Степень тяжести: высокая.
— Незашифрованные сообщения. Степень тяжести: низкая.
— Уязвимая зависимость библиотек JavaScript. Степень тяжести: низкая.

Следующим инструментом для проверки безопасности был взят OWASP ZAP [8] с возможностью проводить тестирование в режиме Атаки. Данная программа предлагает пользователю использовать как традиционный spider (инструмент, который предназначен для автоматического обнаружения новых URL-адресов на проверяемом сайте), так и ajax spider, который позволяет сканировать веб-приложения, написанные на AJAX. (рис. 4)

ZAP проводит полный перебор всевозможных полей на веб-приложении посредством использования spider. После завершения атаки происходит активное сканирование всего ресурса для обнаружения возможных уязвимостей. В случае проведенного сканирования были выявлены следующие проблемы в Neo4j:

— Content Security Policy (CSP): style-src небезопасный встроенный. Средняя степень тяжести.

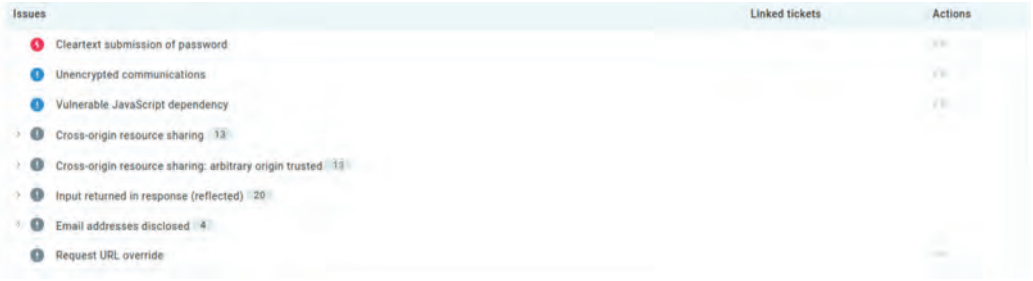

Рис.3. Результат сканирования Burp Suite

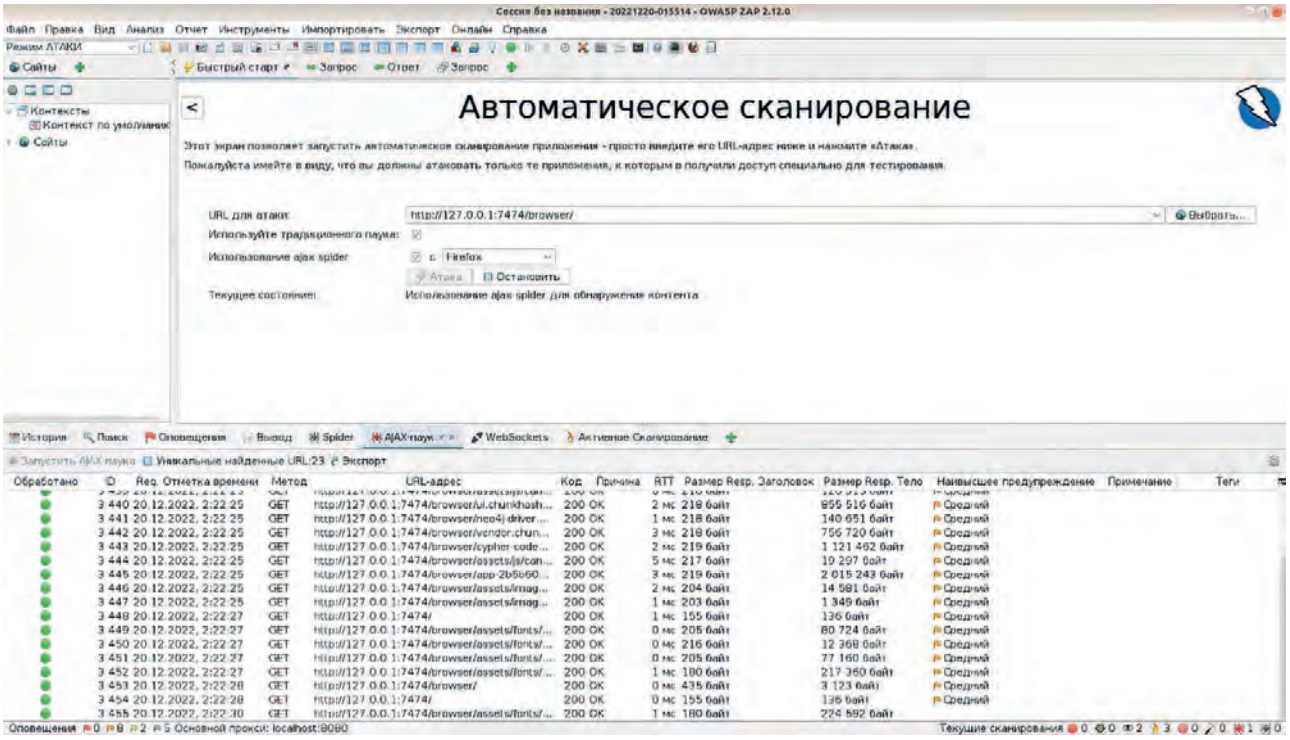

Рис.4. Результат сканирования ZAP

— CSP: Директива подстановочного знака. Средняя степень тяжести.
— CSP: скрипт-SRC небезопасный встроенный. Средняя степень тяжести.
— Заголовок CSP не задан. Средняя степень тяжести.
— Междоменная неправильная конфигурация. Средняя степень тяжести.
— Раскрытие ошибок приложения. Средняя степень тяжести.
— Недостаточно надежный метод. Средняя степень тяжести.
— Уязвимость JS Библиотеки. Средняя степень тяжести.
— Заголовок X-Content-Type-Options отсутствует. Низкая степень тяжести.
— Раскрытие отметки времени - Unix. Низкая степень тяжести.

Выявленные уязвимости в основном связаны с некорректной работой передачи данных между клиентом и сервером, а также с разметкой страницы, что может привести к негативным последствиям [9].

В ходе исследования был использован популярный сканер уязвимостей Acunetix. Данный сканер прост в использовании, достаточно ввести в качестве цели СУБД Neo4j по адресу «http://localhost:7474»[10]. После проведения сканирования системы Acunetix предоставляет полный перечень выявленных уязвимостей с возможностью выгрузить отчет (рис. 5). Вследствие проведения сканирования программа выявила следующие уязвимости:

— Базовая аутентификация через HTTP. Средняя степень тяжести.
— Clickjacking: отсутствует заголовок X-Frame-Options. Низкая степень тяжести.

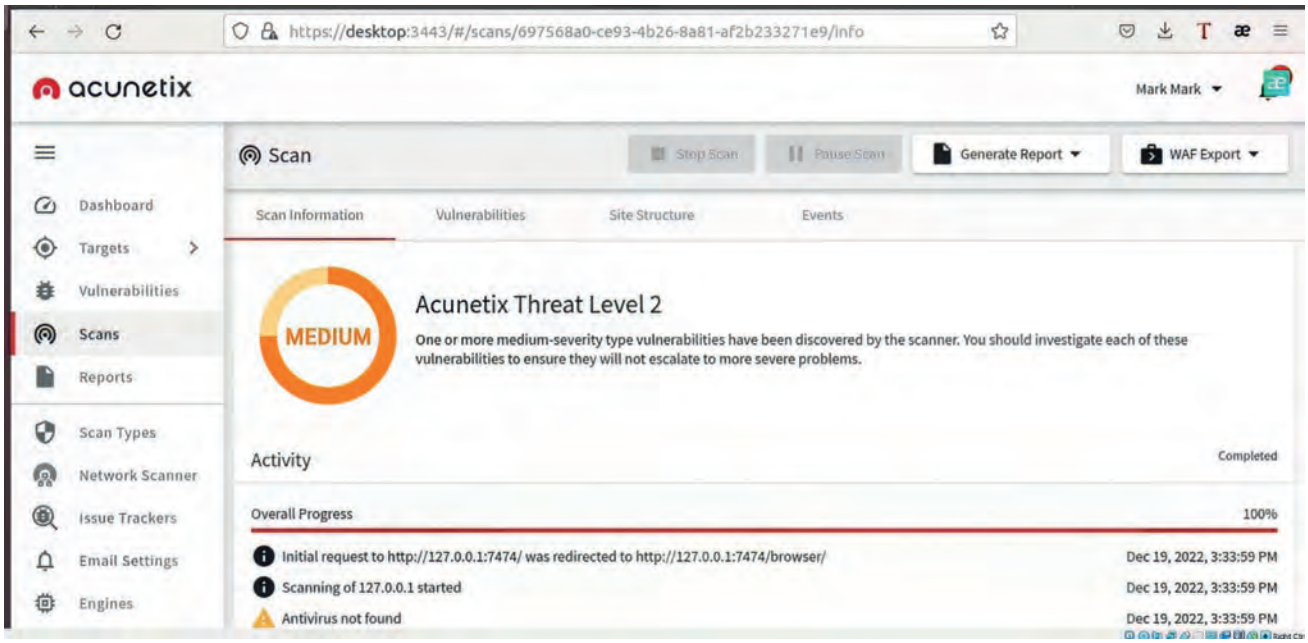

Рис.5. Результаты сканирования Acunetix

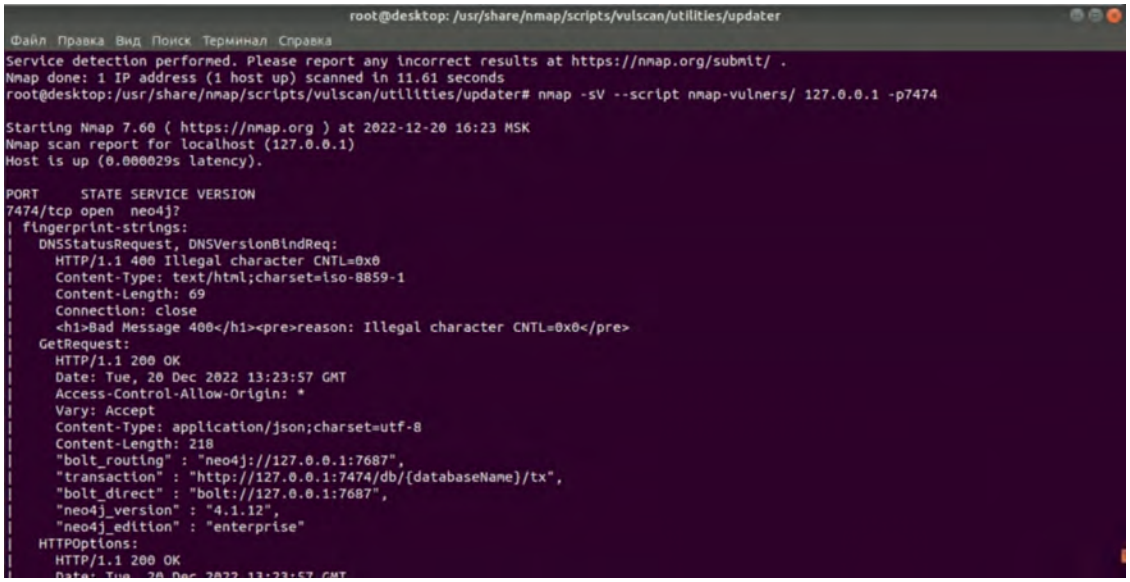

Рис.6. Результат сканирования скриптов Nmap

— Незашифрованное соединение. Низкая степень тяжести.
— Политика безопасности контента (CSP) не реализована. Низкая степень тяжести.

Были обнаружены аналогичные уязвимости, сходные с теми, которые были обнаружены при использовании предыдущих инструментов. Помимо вышеописанных программ в ходе исследования использовался встроенный инструмент для сканирования не только портов, но и уязвимостей Nmap. Самыми распространёнными и эффективными в поиске скриптами обнаружения уязвимостей являются Nmap-vulners, vulscan и vuln [11]. В основном они используют открытую базу знаний CVE. Данные скрипты позволяют исследовать и находить важную информацию об уязвимостях систем[8].

После запуска каждого из скриптов получен одинаковый результат, который не выявил критических уязвимостей кроме информации о версии СУБД Neo4j. Такие данные могут быть использованы злоумышлен-

8 Подвальчик Хакера. Основы Burp Suite. Что это и как им пользоваться [Электронный ресурс] // Режим доступа к ресурсу:https://hacker-basement.com/2021/01/11/osnovy-burp-suite/ (Дата обращения: 10.01.2023).

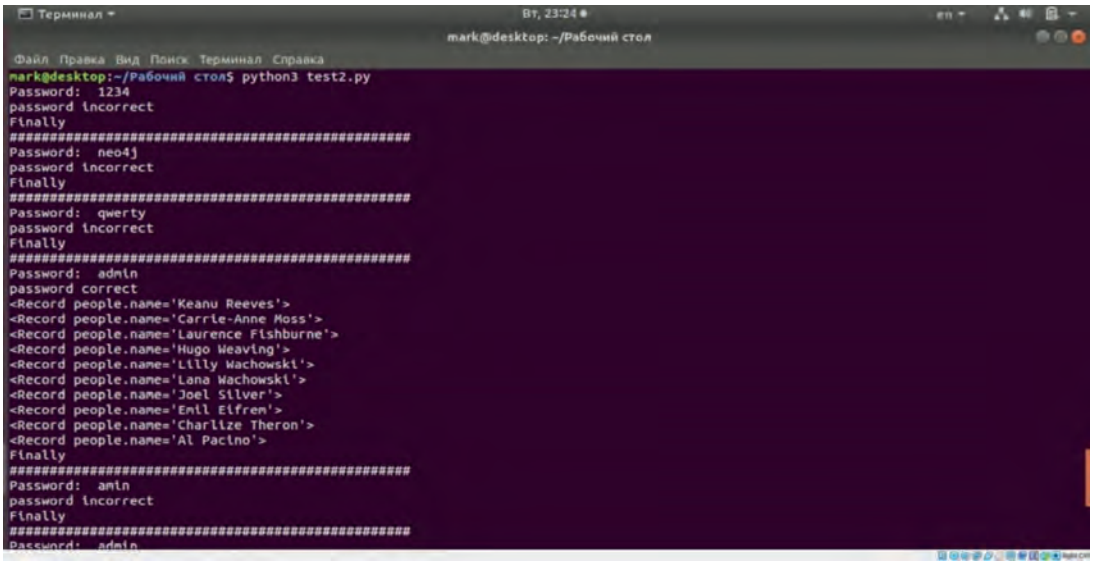

Рис.7. Результат программного кода

никами, которые в перспективе могут изучить уязвимости базы в открытых источниках. (рис.6)

В большинстве случаев ручное тестирование на безопасность проводится опытными специалистами для возможности определить уязвимости там, где не смог определить сканер, с учетом особенностей системы или ПО. Был рассмотрен вариант, когда злоумышленник может проникнуть в СУБД не только напрямую, но и косвенно через ОС, точнее через службы, которые в ней запущены.

Руководствуясь данным суждением, были выявлены следующие проблемы:

1. Доступ к файлам СУБД.

В процессе исследования были выявлены документы, которые либо не защищены, либо имеют недостаточно надежную систему защиты. Если основное устройство, на котором развернута система управления базами данных (СУБД), имеет парольную защиту, нет необходимости вводить пароль для чтения данных из файлов. Это указывает на низкую уровень безопасности системы. В качестве ценных файлов можно отметить следующие:

- Security.log. Журнал безопасности, который используется для отслеживания информации, связанной с безопасностью в компьютерной системе;
- Auth. Файл хранит аутентификационную информацию пользователя, зашифрованную посредством использования алгоритма SHA256;
- Roles. Файл хранит информацию о ролях пользователей.

2. Попытка проведения Brutforce-атаки.

В ходе исследования проведена атака по словарю. Данный метод реализован на языке программирования Python. Выбор сделан в его пользу по той причине, что остальные методы либо не реализуемы в нынешнем исследовании, либо не применимы, как, например, гибридный метод в связи со спецификой веб-сайта графовой СУБД Neo4j.

Реализовав программный код (рис. 7), можно наблюдать, что в случае некорректного ввода пароля выводится сообщение «password incorrect», в противном случае «password correct». Посредством перебора было рассмотрено 8 паролей, 6 из них вывели сообщение о неправильном пароле, а 2 вывели результат. В качестве результата были переданы первые 10 человек из БД, связанные с «Фильмом».

4. Применение процессов и мер обеспечения ИБ для графовой СУБД

В ходе проведения тестирования безопасности Neo4j выявлены уязвимости, которые нужно устранить. Для того, чтобы обеспечить надежную безопасность графовой СУБД, необходимо проверить применимость существующих процессов и мер СУБД посредством тестирования с помощью инструментов, описанных выше.

В основном, планируется использовать комбинацию ранее изученных средств, учитывая уже существующие процессы и меры обеспечения информационной безопасности реляционных баз данных, а также адаптированные методы защиты, применяемые в графовых СУБД [12].

1. Настройка конфигурации.

```
# Bolt connector
dbms.connector.bolt.enabled=true
dbms.connector.bolt.tls_level=REQUIRED
#dbms.connector.bolt.listen_address=:7687
#dbms.connector.bolt.advertised_address=:7687

# HTTP Connector. There can be zero or one HTTP connectors.
dbms.connector.http.enabled=true
#dbms.connector.http.listen_address=:7474
#dbms.connector.http.advertised_address=:7474

# HTTPS Connector. There can be zero or one HTTPS connectors.
dbms.connector.https.enabled=true
#dbms.connector.https.listen_address=:7473
#dbms.connector.https.advertised_address=:7473
```

Рис.8. Настройка защиты транспортного уровня

Основным файлом конфигурации СУБД Neo4j является neo4j.conf, который содержит в себе основные параметры конфигурации в Neo4j[9].

В качестве основных протоколов для безопасной передачи данных используют Bolt, который помогает обеспечить связь «клиент-сервер» в базе данных Neo4j, а также протокол https, позволяющий использовать сертификаты SSL для безопасной передачи данных[10].

Коннекторы настраиваются в формате dbms.connector.<connector-name>.<setting-suffix>> (рис. 8).

2. Разграничение доступа и защита полей.

Необходимой мерой для СУБД является определение ролей. Данная СУБД предоставляет встроенные роли и привилегии по умолчанию. Всего данных ролей 6: Public, Reader, Editor, Publisher, Architector, Admin.

Для обеспечения мер безопасности СУБД с использованием команды «drop» удален пользователь «neo4j». Перед проведением этой манипуляции заранее создан другой суперпользователь под именем «mark». Данное действие необходимо для того, чтобы злоумышленникам было труднее получить доступ в базу данных, используя атаку типа brute force.

3. Аутентификация пользователя.

У Neo4j есть собственный провайдер аутентификации, который хранит всю информацию о пользователях и ролях в system-базе. Аутентификация настраивается в конфигурационном файле при помощи параметра dbms.security.auth_enabled. По умолчанию аутентификация включена (рис. 9).

Дополнительно можно настроить параметры, такие как «dbms.security.auth_max_failed_attempts» и «dbms.security.auth_lock_time». В первом случае можно задать максимальное количество неудачных попыток при входе, что позволяет существенно помешать злоумышленнику подобрать учетные данные. Второй параметр позволяет настроить время блокировки после исчерпания количества неудачных попыток.

4. Выбор расширенной лицензии для получения поддержки и дополнительных мер безопасности, таких как журналирование.

Стоимость услуги является проблемой при использовании корпоративной лицензии, а лицензия сообщества не предоставляет основных параметров безопасности, таких как журнал. Это будет способствовать атакам и утечкам информации.

5. Ограничение диска.

Для обеспечения безопасности диска, где расположена графовая СУБД, необходимо определить корректный объем памяти. Посредством использования команды «neo4j-admin memrec» можно получить первоначальную рекомендацию о том, как распределить определенный объем памяти.

6. Использование журналов безопасности.

Neo4j предоставляет механизмы отслеживания и анализа состояния базы данных при помощи мониторинга. При этом есть возможность проверять выполняемые запросы[11].

9 Инструменты Kali Linux. Zaproxy [Электронный ресурс] // Режим доступа к ресурсу: https://kali.tools/?p=2299 (Дата обращения: 10.01.2023).

10 Anti-malware. Обзор Acunetix Premium 14, DAST-платформы контроля безопасности веб-приложений [Электронный ресурс] // Режим доступа к ресурсу: https://www.anti-malware.ru/reviews/Acunetix-Premium (Дата обращения: 10.01.2023).

11 Технологии баз данных и знаний. Система управления базы данных [Электронный ресурс] // Режим доступа к ресурсу: http://bseu.by/it/tohod/lekcii5_4.htm (Дата обращения: 10.01.2023).

```
# Whether requests to Neo4j are authenticated.
# To disable authentication, uncomment this line
dbms.security.auth_enabled=true
```

Рис.9. Настройка аутентификации

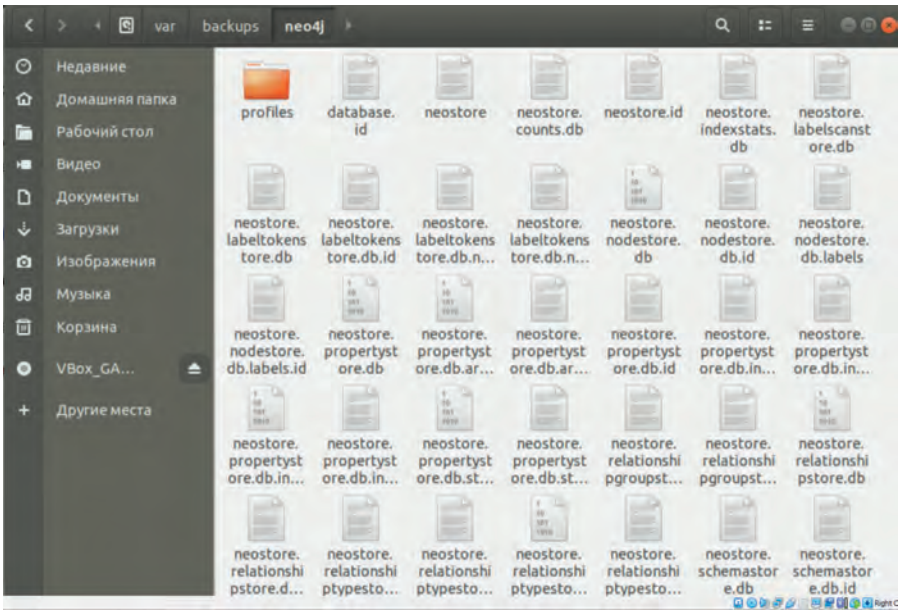

Рис.10. Директория резервной копии Neo4j

Все журналы, которые используются в графовой СУБД на дистрибутиве Linux, расположены по следующему адресу: «/var/log/neo4j». При этом настройка данных логов производится в параметре «dbms.directories.logs» [13].

В распоряжении администратора находятся 3 журнала, которые хранят в себе конфиденциальную информацию (табл. 2).

Таблица 2

Существующие журналы в графовой СУБД Neo4j

Название журнала	Описание
debug.log	Информация, полезная при отладке проблем с Neo4j.
query.log	Журнал выполненных запросов, которые занимают больше времени, чем указанный порог.
security.log	Журнал событий безопасности.

7. Резервное копирование.

В Neo4j резервная копия реализуется посредством использования команды «neo4j-admin backup». Она имеет дополнительные аргументы в виде директории сохранения и базы данных. Использование команды позволяет создать резервную копию в папке «var/backups» (рис. 10).

8. Защита передачи данных

В ходе исследования для создания собственного сертификата SSL была использована утилита mkcert. Основные параметры настройки SSL конфигурации находятся в «SSL policy configuration». В данном разделе большая часть полей закомментирована и не работает по умолчанию. Были указаны прямые ссылки на расположение открытого и закрытого ключей и при этом выставлены параметры «dbms.ssl.policy.bolt.enabled» в значении «true» [14] (рис. 11).

После внесения изменения и сохранения данных появилась возможность войти в интерфейс СУБД через защищенный канал связи по выделенному порту 7473. (рис. 12)

9. Разграничение прав доступа к файлам

Нельзя забывать, что СУБД не является отдельно работающим ПО. Доступ к основным файлам можно получить через командную строку ОС, на которой Neo4j расположена. Neo4j рекомендует[12] производить разграничения прав доступа на следующие директории:

— Conf
— Import
— Bin
— Lib

12 Neo4j. Default file locations URL: https://neo4j.com/docs/operations-manual/current/configuration/file-locations/ (accessed: 10.01.2023).

```
# Bolt SSL configuration
dbms.ssl.policy.bolt.enabled=true
dbms.ssl.policy.bolt.base_directory=/var/lib/neo4j/certificates/bolt
dbms.ssl.policy.bolt.private_key=/var/lib/neo4j/certificates/bolt/localhost-key.pem
dbms.ssl.policy.bolt.public_certificate=/var/lib/neo4j/certificates/bolt/localhost.pem
dbms.ssl.policy.bolt.client_auth=NONE

# Https SSL configuration
dbms.ssl.policy.https.enabled=true
dbms.ssl.policy.https.base_directory=/var/lib/neo4j/certificates/https
dbms.ssl.policy.https.private_key=/var/lib/neo4j/certificates/https/localhost-key.pem
dbms.ssl.policy.https.public_certificate=/var/lib/neo4j/certificates/https/localhost.pem
dbms.ssl.policy.https.client_auth=NONE
```

Рис.11. Настройка SSL конфигурации

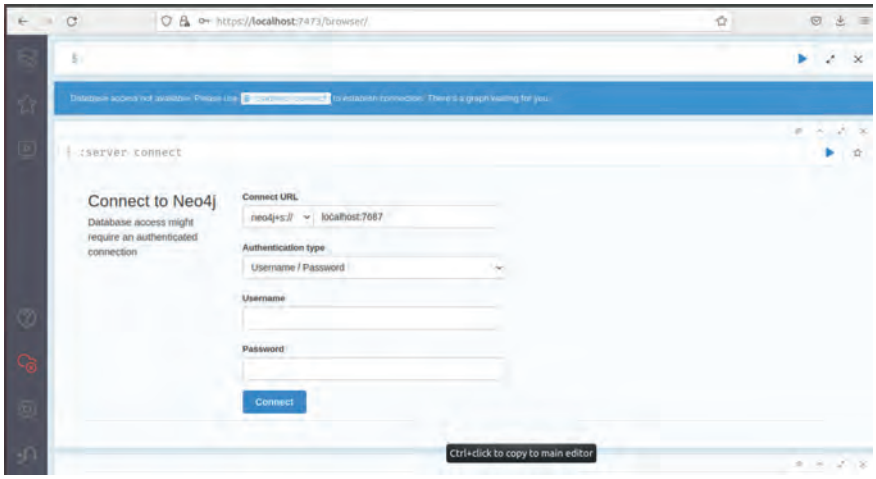

Рис.12. Подключение к Neo4j через протокол https

— Plugins
— Data
— Log

Для коррекции доступа к файлам Neo4j были использованы команды Linux «chmod» и «chown». Первая функция позволяет изменить права доступа к файлу, а вторая изменить владельца или группу. Необходимо, чтобы у всех важных файлов Neo4j были права чтения, изменения и запуска только для суперпользователя. При помощи команды «chmod 700 neo4j.conf» присваиваются права только пользовательскому администратору. Для передачи прав администратора neo4j нужно выполнить команду «chown neo4j:neo4j neo4j.conf».

5. Проверка защищенности методов защиты данных в Neo4j

Для определения эффективности предлагаемых методов защиты, требуется осуществить проверку защищенности графовой СУБД путем использования соответствующих процессов и мер, обеспечивающих информационную безопасность. Кроме того, необходимо повторно применить эти процессы и меры на защищенной СУБД с помощью специальных инструментов тестирования. Это позволит оценить степень применимости предлагаемых методов защиты.

Посредством использования инструмента Burp Suite была проведена попытка отследить передаваемые аутентификационные данные через клиент-серверное подключение. В данном случае инструмент не отслеживает передачу информации, то есть нельзя отследить данные, так как они передаются в зашифрованном виде, а при этом сам факт отслеживания попытки входа в графовую СУБД отслеживается. (рис. 13)

В итоге можно сказать, что инструмент Burp Suite не выявил критических уязвимостей у графовой СУБД после применения методов защиты.

Что касается проверки через Zed attack Proxy, то было проведено тестирование на безопасность с использованием данного инструментария, что позволило выявить 10 потенциальных уязвимостей. (рис. 14)

Если осуществлять сравнение проведенного сканирования с прошлым вариантом без применения методов защиты, то были выявлены те же уязвимости. В этом случае есть предположение, что предлагаемые процессы и меры не влияют на данные уязвимости,

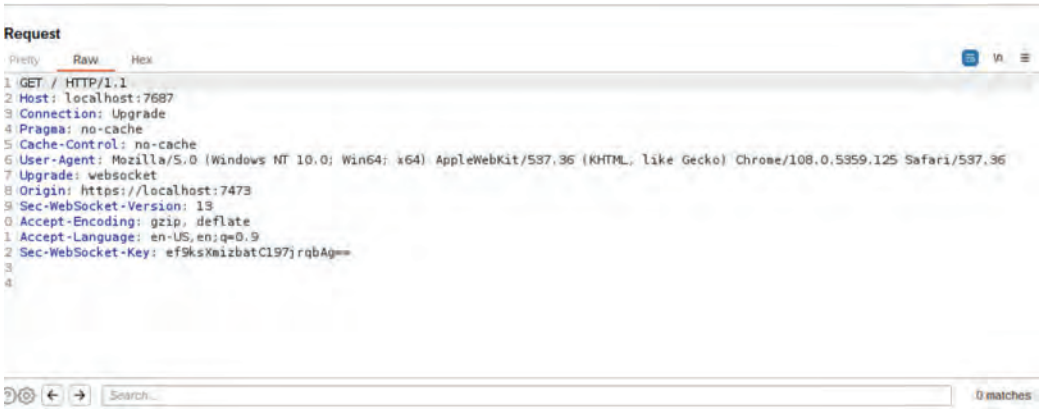

Рис.13. Отслеживание попытки входа в графовую СУБД

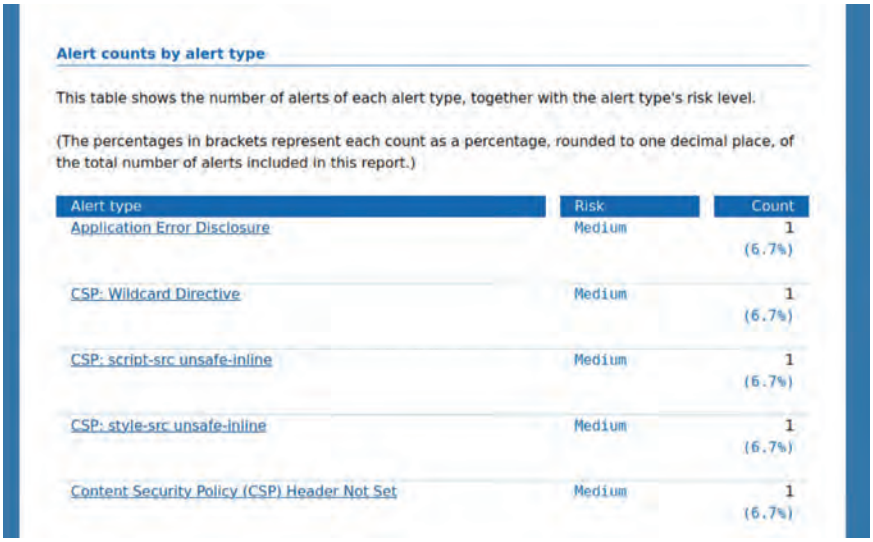

Рис.14. Отчет сканирования ZAP после применения методов защиты

при этом они могут быть связаны с внутренней архитектурой СУБД Neo4j, что необходимо исправлять разработчикам данного ПО.

В случае сканирования с помощью Acunetix необходимо было указать в инструменте в качестве цели тот же локальный хост (127.0.0.1), только другой порт 7473, так как СУБД в данном случае работает на порту протокола https [15]. После запуска сканера были обнаружены следующие результаты с указанием на одну выявленную уязвимость. (рис. 15)

Данная уязвимость заключается в отсутствии заголовка X-Frame-Options, отсутствие которого предоставляет возможность проведения атаки с исправлением поль зовательского интерфейса. При этом данная уязвимости имеет низкую степень тяжести последствий. Если сравнивать сканирования до и после применения методов защиты, то по сравнению с прошлым сканированием удалось избавиться от 4 уязвимостей из 5. Оставшаяся уязвимость, возможно, требует исправления на уровне разработки программного обеспечения.

Проведя сканирования цели в виде «127.0.0.1» с портом 7473 не удалось выявить уязвимостей у графовой СУБД Neo4j, что говорит о применимости предлагаемых методов защиты. При этом злоумышленник все равно может определить версию запущенной на АРМ СУБД Neo4j, что дает возможность определить актуальный перечень уязвимостей из открытых баз данных CVE.

Как говорилось ранее, для того от атаки типа Brute force, необходимо ограничить количество попыток входа для пользователя. Данная мера позволит снизить риск выявления учетных данных злоумышленником.

Запустив повторно программный код после применения предлагаемых методов можно увидеть (рис. 16), что в случае некорректного ввода пароля выводится сообщение «password incorrect», при этом после прохождения лимита попыток даже наличие правильного пароля не дает пользователю войти в СУБД. Посредством пере-

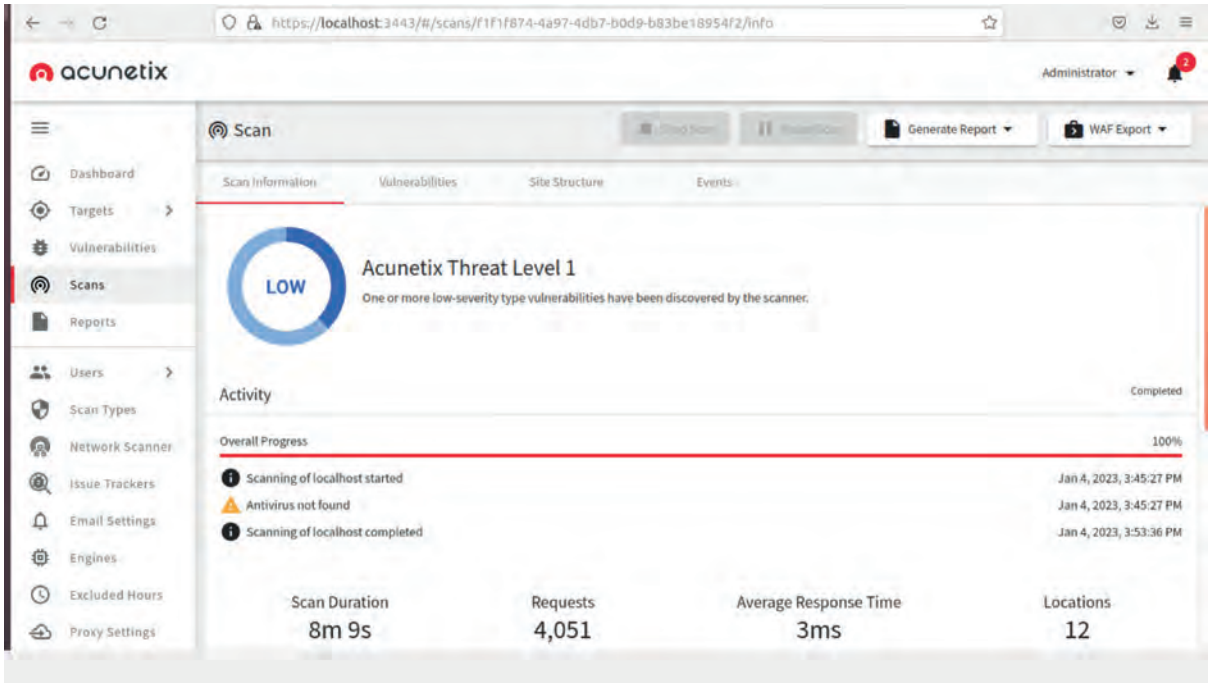

Рис.15. Результат сканирования Accunetix после применения методов защиты

```
ubuntu@ubuntu1804:~/Downloads$ python3 test2.py
Password:  1234
password incorrect
Finally
##################################################
Password:  neo4j
password incorrect
Finally
##################################################
Password:  qwerty
password incorrect
Finally
##################################################
Password:  admin
password incorrect
Finally
##################################################
Password:  amin
password incorrect
Finally
##################################################
Password:  admin
password incorrect
Finally
##################################################
Password:  dsfasdf
password incorrect
Finally
##################################################
Password:  fsadfvcxv
password incorrect
Finally
##################################################
ubuntu@ubuntu1804:~/Downloads$
```

Рис.16. Результат атаки типа Brute force после применения методов защиты

бора было рассмотрено восемь комбинаций, восемь из них вывели сообщение о неправильном пароле. В случае возникновения ошибки при входе, программа будет отображать некорректный пароль пользователя.

После применения предлагаемых процессов и мер защиты и проведения тестирования безопасности можно сделать вывод, что большая часть обнаруженных уязвимостей была успешно устранена.

Однако остальные уязвимости, которые не были представлены, могут быть связаны с архитектурой Neo4j и требуют вмешательства разработчика программного обеспечения для их решения.

Выводы

В ходе работы были рассмотрены угрозы, уязвимости и распространенные методы защиты данных для графовых СУБД. Определена применимость комбинации процессов и мер обеспечения информационной безопасности на примере Neo4j посредством проведения тестирования безопасности.

Полученные результаты позволят не только обеспечить ИБ графовых СУБД при внедрении в ИС, но и также помогут специалистам информационной безопасности составить общий перечень требований к безопасности СУБД данного типа, что обеспечит полное понимание при внедрении или разработке системы управления базы данных.

Благодаря использованию сочетания различных процессов и мер защиты большая часть выявленных уязвимостей была успешно исправлена, что подтверждает применимость выбранного набора методов защиты для графовой СУБД Neo4j. Это свидетельствует о том, что данные методы обеспечения безопасности могут быть эффективно применены в контексте работы с Neo4j и способны обеспечить необходимый уровень защиты информации, что доказало новизну работы. Однако следует продолжать обращать внимание на оставшиеся уязвимости и осуществлять необходимые меры для их устранения с участием разработчиков ПО.

Начальный перечень программного обеспечения, используемого для тестирования безопасности графовой СУБД, может быть расширен при интеграции в информационную систему, которая имеет свою собственную специфику деятельности. Каждая информационная система имееет свои уникальные требования и особенности, которые могут потребовать использования специализированного программного обеспечения для тестирования безопасности.

Литература

1. Sicari S., Rizzardi A., Coen-Porisini A. Security&privacy issues and challenges in NoSQL databases //Computer Networks. – 2022. – Т. 206. – С. 108828. DOI: 10.1016/j.comnet.2022.108828.
2. Плаксий К.В., Никифоров А.А., Милославская Н.Г. Исследование графовых СУБД, пригодных для работы с большими данными при обнаружении дел по отмыванию доходов, полученных преступным путем, и финансированию терроризма // Безопасность информационных технологий. – 2019. – Том 26, № 3. – С. 103-116. DOI: 10.26583/bit.2019.3.09.
3. Агафонов А. А. и др. Безопасность систем баз данных //Самара: Изд-во Самар. ун-та. – 2023. – Т. 1.
4. Плаксий К.В., Никифоров А.А., Милославская Н.Г., Кулагина Л.Л. Исследование вопросов обеспечения информационной безопасности графовых СУБД, пригодных для работы с большими данными, при обнаружении дел по отмыванию доходов, полученных преступным путем, и финансированию терроризма // Безопасность информационных технологий. – 2020. Том 27, № 4. – С. 53-64. DOI: 10.26583/bit.2020.4.05
5. Dissanayaka A. M. et al. Security assurance of MongoDB in singularity LXCs: an elastic and convenient testbed using Linux containers to explore vulnerabilities //Cluster Computing. – 2020. – Т. 23. – С. 1955-1971. DOI: 10.1007/s10586-020-03154-7
6. Макаренко С. И., Смирнов Г. Е. Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. – 2020. – №. 4. – С. 44-72. DOI: 10.24411/2410-9916-2020-10402
7. Kore A. et al. Burp Suite Extension for Script based Attacks for Web Applications //2022 6th International Conference on Electronics, Communication and Aerospace Technology. – IEEE, 2022. – С. 651-657. DOI: 10.1109/ICECA55336.2022.10009116
8. Abdullah H. S. Evaluation of open source web application vulnerability scanners //Academic Journal of Nawroz University. – 2020. – Т. 9. – №. 1. – С. 47-52. DOI: 10.25007/ajnu.v9n1a532
9. Devi R. S., Kumar M. M. Testing for security weakness of web applications using ethical hacking //2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184). – IEEE, 2020. – С. 354-361. DOI: 10.1109/ICOEI48184.2020.9143018
10. Saputra I. P., Utami E., Muhammad A. H. Comparison of anomaly based and signature based methods in detection of scanning vulnerability //2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). – IEEE, 2022. – С. 221-225. DOI: 10.23919/EECSI56542.2022.9946485
11. Putra S. A., Budiono A., Hediyanto U. Y. K. S. Vulnerability Assesment Web Proposal Tugas Akhir Mahasiswa Menggunakan Acunetix dan NMAP //eProceedings of Engineering. – 2023. – Т. 10. – №. 2.
12. Кучкин В. П. Методы защиты баз данных // Проблемы науки. – 2021. – №. 4 (63). – С. 33-35.
13. Fahd K., Venkatraman S., Hammeed F. K. A comparative study of NoSQL system vulnerabilities with big data //Int. J. Manag. Inf. Technol. – 2019. – Т. 11. – №. 4. – С. 1-19. DOI: 10.5121/ijmit.2019.11401
14. Ankomah E. et al. A Comparative Analysis of Security Features and Concerns in NoSQL Databases // International Conference on Frontiers in Cyber Security. – Singapore : Springer Nature Singapore, 2022. – С. 349-364. DOI: 10.1007/978-981-19-8445-7_22
15. Zirwan A. Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner // Jurnal Informasi dan Teknologi. – 2022. – С. 70-75. DOI: 10.37034/jidt.v4i1.190

INVESTIGATION OF PROCESSES AND MEASURES APPLICABLE FOR ENSURING INFORMATION SECURITY FOR SYSTEMS WITH A GRAPHIC DBMS

Karapetyants Mark[13], Plaksiy K.V.[14], Nikiforov A.A.[15]

Purpose of the paper: *research of popular information security processes and measures in information systems with graph DBMS and assessment of their applicability using vulnerability scanning tools and security testing methods.*

Methods: graph theory, system analysis, injection protection, input filtering, Brute force.

Results: *the main threats and vulnerabilities for graph DBMS have been identified. The analysis of information security processes and measures involved in SQL DBMS allowed the authors to determine a list of measures most suitable for use in graph DBMS. During the study the researchers tested Neo4j's security with help of software tools and utilities to identify vulnerabilities which were subsequently eliminated by information security processes and measures. Finally, the investigators checked and assessed security of graph DBMS's security tools combination. The results obtained have practical significance for various information systems that implement graph DBMS in business processes. They can also be used to develop basic criteria needed when creating or improving graph database management systems.*

Scientific novelty: *the novelty of the research lies in proof of processes' and measures' applicability that ensure information security of an information system with a graph DBMS.*

Keywords: *graph DBMS, processes and measures, information security, Acunetix, Nmap, OWASP ZAP proxy, Burp Suite, Neo4j, threats, vulnerabilities, vulnerability scanner*

References

1. Sicari S., Rizzardi A., Coen-Porisini A. Security&privacy issues and challenges in NoSQL databases //Computer Networks. – 2022. – Vol. 206. – pp. 108828. DOI: 10.1016/j.comnet.2022.108828.
2. K.V. Plaksij, A.A. Nikiforov, N.G. Miloslavskaya. Issledovanie grafovyh SUBD, prigodnyh dlya raboty s bol'shimi dannymi pri obnaruzhenii del po otmyvaniyu dohodov, poluchennyh prestupnym putem, i finansirovaniyu terrorizma // Bezopasnost informacionnyh tekhnologij. – 2019. – Vol. 26, № 3. – pp. 103-116. DOI: 10.26583/bit.2019.3.09.
3. Agafonov A. A. i dr. Bezopasnost sistem baz dannyh //Samara: Izd-vo Samar. un-ta. – 2023. – Vol. 1.
4. K.V. Plaksij, A.A. Nikiforov, N.G. Miloslavskaya, L. L. Kulagina. Issledovanie voprosov obespecheniya informacionnoj bezopasnosti grafovyh SUBD, prigodnyh dlya raboty s bol'shimi dannymi, pri obnaruzhenii del po otmyvaniyu dohodov, poluchennyh prestupnym putem, i finansirovaniyu terrorizma. // Bezopasnost informacionnyh tekhnologij. – 2020. Vol. 27, № 4. – pp. 53-64. DOI: 10.26583/bit.2020.4.05
5. Dissanayaka A. M. et al. Security assurance of MongoDB in singularity LXCs: an elastic and convenient testbed using Linux containers to explore vulnerabilities //Cluster Computing. – 2020. – T. 23. – C. 1955-1971. DOI: 10.1007/s10586-020-03154-7
6. Makarenko S. I., Smirnov G. E. Analiz standartov i metodik testirovaniya na proniknovenie //Sistemy upravleniya, svyazi i bezopasnosti. – 2020. – №. 4. – pp. 44-72. DOI: 10.24411/2410-9916-2020-10402
7. Kore A. et al. Burp Suite Extension for Script based Attacks for Web Applications //2022 6th International Conference on Electronics, Communication and Aerospace Technology. – IEEE, 2022. – C. 651-657. DOI: 10.1109/ICECA55336.2022.10009116
8. Abdullah H. S. Evaluation of open source web application vulnerability scanners //Academic Journal of Nawroz University. – 2020. – T. 9. – №. 1. – C. 47-52. DOI: 10.25007/ajnu.v9n1a532

13 Mark Karapetyants, Ph.D. student, National Research Nuclear University MEPhI, Moscow, Russia. E-mail: Mkarapetyants@mephi.ru, ORCID: 0009-0002-3262-1138.

14 Kirill V. Plaksiy, Senior Lecturer, National Research Nuclear University MEPhI, Moscow, Russia. E-mail: KVPlaksii@mephi.ru, ORCID: 0000-0002-8949-6772.

15 Andrey A. Nikiforov, Senior Lecturer, National Research Nuclear University MEPhI, Moscow,Россия. E-mail: andreinikiforov993@gmail.com,http://orcid.org/0000-0002-2726-0000

9. Devi R. S., Kumar M. M. Testing for security weakness of web applications using ethical hacking //2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184). – IEEE, 2020. – С. 354-361. DOI: 10.1109/ICOEI48184.2020.9143018
10. Saputra I. P., Utami E., Muhammad A. H. Comparison of anomaly based and signature based methods in detection of scanning vulnerability //2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). – IEEE, 2022. – С. 221-225. DOI: 10.23919/EECSI56542.2022.9946485
11. Putra S. A., Budiono A., Hediyanto U. Y. K. S. Vulnerability Assesment Web Proposal Tugas Akhir Mahasiswa Menggunakan Acunetix dan NMAP //eProceedings of Engineering. – 2023. – Т. 10. – №. 2.
12. Kuchkin V. P. Metody zashchity baz dannyh //Problemy nauki. – 2021. – №. 4 (63). – pp. 33-35.
13. Fahd K., Venkatraman S., Hammeed F. K. A comparative study of NoSQL system vulnerabilities with big data //Int. J. Manag. Inf. Technol. – 2019. – Т. 11. – №. 4. – С. 1-19. DOI: 10.5121/ijmit.2019.11401
14. Ankomah E. et al. A Comparative Analysis of Security Features and Concerns in NoSQL Databases //International Conference on Frontiers in Cyber Security. – Singapore : Springer Nature Singapore, 2022. – С. 349-364. DOI: 10.1007/978-981-19-8445-7_22
15. Zirwan A. Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner //Jurnal Informasi dan Teknologi. – 2022. – С. 70-75. DOI: 10.37034/jidt.v4i1.190

ВЕРИФИКАЦИЯ МЕТОДА БЕЗОПАСНОГО РАСПРЕДЕЛЕНИЯ СЕССИОННОГО КЛЮЧА В СИСТЕМЕ ОТСЛЕЖИВАНИЯ КАЧЕСТВА ПРОДУКЦИИ

Лэ В. Х.[1], Бегаев А.Н.[2], Комаров И.И.[3], Фунг В.К.[4]

Цель работы: *определение требований по обеспечению основных и дополнительных свойств информационной безопасности при взаимодействии контрагентов в информационных системах, связанных с обеспечением прослеживаемости качества продукции; разработка и формальная верификация метода генерации и безопасного распределения сессионного ключа, отвечающего этим требованиям.*

Результат: *Использование систем прослеживаемости качества товара является мощным инструментом для решения широкого спектра технологических и социальных задач, например: государственный контроль в регулируемых сферах, обеспечение безопасности потребителя, формирование конкурентного преимущества производителя и т. д. Однако, широкое внедрение таких децентрализованных систем сопряжено с рядом противоречий, одно из которых непосредственно связано с проблемой обеспечения конфиденциальности данных и необходимостью их контролируемого использования в динамическом составе контрагентов и потребителей.*

В работе предлагается направление по преодолению этого противоречия путём формирования сценариев получения контролируемого доступа к приватной информации взаимодействующей стороны с использованием криптографических процедур.

Для реализации таких сценариев разработан метод и базирующийся на нем протокол генерации и распределения секретного сессионного ключа с использованием доверенной третьей стороны. Приводится формальное доказательство безопасности предлагаемого решения с использованием специализированного инструментального средства верификации протоколов.

Полученные результаты в первую очередь ориентированы на применение в системах распределённого реестра, предполагающих разделение данных на приватные и публичные блоки. Однако они могут найти применение и в других системах, предъявляющих требования конфиденциальности, доступности и недоказуемости, особенно при наличии ограничений на вычислительные ресурсы.

Научная новизна: *заключается в проблемно-ориентированном анализе специфических требований по обеспечению информационной безопасности процесса внесения и извлечения данных в систему отслеживания качества товаров в заданных сценариях её использования. На основании выделенных требований формулируется и решается задача разработки адаптированного метода генерации и распределения секретного сессионного ключа между двумя абонентами с привлечением доверенной стороны. На базе разработанного метода синтезируется применимый на практике коммуникационный протокол и проводится формальное доказательство выполнения заданных требований по информационной безопасности, устойчивость к атакам типа «MITM» и повтора.*

Вклад авторов: *Бегаев А.Н. – анализ функциональных потребностей в процессе реализации прикладных распределённых защищённых систем, обоснование научно-методических проблем, определение требований и сценария применения технических решений, базирующихся на новом научном результате; Комаров И.И. – определение методологического противоречия и подхода к его разрешению, определение требований к научному результату, разработка плана исследования; Лэ В. Х. – разработка метода безопасного распределения сессионного ключа в системах отслеживания качества продукции, формализация разработанного метода в тер-*

1 Лэ Ван Хиеу, аспирант факультета безопасности информационных технологий, Университет ИТМО, Санкт-Петербург, Россия. E-mail: hieule250715@gmail.com

2 Бегаев Алексей Николаевич, кандидат технических наук, профессор Университета ИТМО, генеральный директор АО «Эшелон – Северо-Запад», Санкт-Петербург, Россия. E-mail: begaev@mail.ru

3 Комаров Игорь Иванович, кандидат физико-математических наук, доцент, доцент факультета безопасности информационных технологий, Университет ИТМО, Санкт-Петербург, Россия. E-mail: i_krov@mail.ru

4 Фунг Ван Кю, аспирант факультета программной инженерии и компьютерной техники, Университет ИТМО, Санкт-Петербург, Россия. E-mail: hieule250715@mail.com

минах высокоуровневого языка спецификации протоколов, определение ограничений и перспектив развития полученных результатов; Фунг В. К. – проведение эксперимента с помощью специализированного автоматизированного средства верификации безопасности протоколов, визуализация и интерпретация результатов.

Ключевые слова: *кибербезопасность, конфиденциальность, неотказуемость, сессионный криптографический ключ, распределённый реестр, формальная верификация протокола.*

DOI:10.21681/2311-3456-2023-6-112-121

Введение

Теоретическая модель систем распределённого реестра, ставшая основой широко применяющейся блокчейн-технологии, с точки зрения информационной безопасности обеспечивает несколько ключевых свойств хранимых данных. В первую очередь это целостность и неотказуемость. Вместе с тем использование технологии блокчейн сопряжено с высокой вычислительной сложностью и, следовательно, высокой стоимостью требуемых вычислительных средств для обеспечения доступности данных. Одновременно стоит вопрос об обеспечении заданного уровня конфиденциальности информации в реальных производственных цепочках, связанных со взаимодействием различных контрагентов.

Несмотря на пессимистические прогнозы, касающиеся защищённости прикладных систем на основе распределённого реестра в условиях квантовых вычислений [1, 2], считается целесообразным [3-5] продолжение работ в области автоматизации взаимодействия как производителей, так и потребителей в рамках расширенной производственной цепочки.

На примере системы отслеживания качества товара [6], а также ряда других перспективных информационных систем [7-9], предъявляющих специфические требования к процессу информационного взаимодействия, выделяется несколько групп противоречий, требующих разрешения, а именно: противоречие между различным уровнем конфиденциальности данных и единым алгоритмом доступа к ним, а также противоречие между потребностью оперативного получения целостных и аутентичных данных и высокой ресурсоёмкостью этого процесса. Одним из путей практического разрешения указанных противоречий является определение баланса в единой системе прослеживаемости качества товара за счёт использования различных моделей безопасности [10 - 12] для выполнения частных подзадач.

Предпосылки исследования

Работа базируется на достаточно широко известных исследованиях, последовательно развивающих концепцию распределённого реестра для применения в различных отраслях.

Так, Yingwen Chen и др. [13] предложена система, которая использует блокчейн консорциума Hyperledger Fabric для хранения зашифрованных медицинских данных и соответствующих политик контроля доступа. Для защиты конфиденциальности медицинских данных система использует комбинацию K-анонимности и методов шифрования с возможностью поиска. Она также обеспечивает управление доступом на основе атрибутов ABAC (Attribute-Based Access Control) для медицинских данных, что позволяет авторизованным пользователям получать доступ к данным на основе их атрибутов, таких как их роль, отделение и специальность. Однако используемая модель K-анонимности может быть уязвима для атак, если злоумышленник имеет доступ к дополнительной информации о пациентах, такой как их демографические данные или история болезни.

Zheng B.K. и др. [14] предлагают модели шифрования данных и управления ключами для повышения конфиденциальности в блокчейне. В их работе приводится пример применения к блокчейну криптосистемы Пайе, позволяющей защитить конфиденциальную информацию и решить проблему защиты конфиденциальности блока блокчейна. Потенциальная проблема схемы заключается в том, что она использует архитектуру с двумя блокчейнами. Это может увеличить сложность и стоимость системы. Кроме того, безопасность системы зависит от безопасности как общедоступных, так и частных блокчейнов. В работе остался без рассмотрения вопрос функционального (с учётом бизнес-логики процессов) разделения данных по уровням конфиденциальности.

Yang Y. и др. [15] рассматривают вопрос применения безопасных многосторонних вычислений SMPC (Secure Multi-Party Computation) с целью повышения конфиденциальности при совместном использовании данных между несколькими сторонами. При этом отмечается, что реализация безопасных многосторон-

них вычислений ограничена из-за неэффективного, сложного протокола вычислений и частого взаимодействия. Авторы базируются на особенности SMPC, позволяющей нескольким сторонам вычислять функцию на своих частных входных данных, не раскрывая эти входные данные друг другу или какой-либо третьей стороне. Позволяя сторонам совместно обрабатывать конфиденциальные данные, не раскрывая их другим, SMPC может помочь обеспечить безопасность и надёжность системы, в том числе в условиях реализации ряда потенциальных атак. Реализация схема Block-SMPC опирается на безопасность сети блокчейн. Естественным направлением совершенствования обсуждаемой системы является снижение вычислительной сложности протоколов для. большого числа участников.

Как показано в работе[5] коллектива авторов, одной из ключевых уязвимостей информационной безопасности распределённых систем является увеличение числа скомпрометированных элементов, участвующих в совместном обеспечении информационной безопасности, что ещё раз подтверждает требование обеспечения взаимного доверия как друг к другу, так и к совместно генерируемым ресурсам.

Сильные стороны каждого из упомянутых подходов можно использовать для повышения конфиденциальности приватных данных в системах отслеживания на основе блокчейна. В зависимости от конкретных потребностей и требований системы может подойти один или комбинация нескольких из них.

В работе [6] предложена модель повышения безопасности частной информации в системе отслеживания товаров за счёт классификации и разделения доказательно целостного массива на публичные и приватные блоки данных, обеспечивающие решение различных задач в системе прослеживаемости качества товара. Предполагается, что частная информация каждой транзакции будет зашифрована с помощью симметричного ключа, сгенерированного смарт-контрактом. В соответствии с классическими положениями криптографии информационная безопасность защищаемых блоков определяется безопасностью этого ключа. Авторы предлагают метод его защиты путём шифрования с помощью открытых ключей каждой из вовлечённых сторон и последующего сохранения в блокчейне.

5 Дранник А.Л., Егоров Д. А., Коваленко М. Е., Масленников О. С., Комаров И.И. Юрьева Р.А. Исследование деструктивного воздействия роботов-злоумышленников на эффективность работы мультиагентной системы // Процессы управления и устойчивость. – 2014. – Т. 1. – №. 1. – С. 336–340

В настоящей работе приводится метод и формальная верификация протокола использования инфраструктуры открытых ключей для обеспечения доступа к заданному информационному блоку, что обеспечивает соблюдение требований конфиденциальности и снижает ресурсоёмкость операции.

Постановка задачи и модель использования

Пусть в рамках системы прослеживаемости качества товаров двум сторонам (*A* и *B*) нужен общий секретный ключ *K*, сгенерированный доверенным сервером для шифрования их личных данных в каждой транзакции.

Требования:

- должна быть обеспечена взаимная аутентификация ранее «незнакомых» сторон *A* и *B*;
- ключ *K* должен быть секретным;
- протокол обмена ключами *K* должен быть безопасным;
- должна быть обеспечена защищённость от атак типа MITM (Man In The Middle) и повтора;
- используются открытые каналы взаимодействия.

Для решения поставленной задачи предлагается следующий *метод*, который лежит в основе протокола взаимной аутентификации и распределения ключей, основанный на асимметричных криптосхемах. Пусть имеется два заинтересованных контрагента *Alice* и *Bob*, а также третья сторона *Trent*, которой они оба доверяют.

Alice генерирует случайное число *Na* и, зашифровав свой идентификатор (*A*) и это число с открытым ключом *Bob*, и отправляет их *Bob*.

$$Alice \rightarrow \{E_{K_B}(A, Na)\} \rightarrow Bob \qquad (1)$$

Bob: расшифровывает полученное сообщение, извлекает отправленное число Na, генерирует случайное число *Nb* и, зашифровав свой идентификатор (*B*), это число и случайное число Na открытом ключом *Alice* и отправляет *Alice.*

$$Bob \rightarrow \{E_{K_A}(B, Na, Nb)\} \rightarrow Alice \qquad (2)$$

Alice отправляет *Bob* случайные числа, зашифровав сообщение открытом ключом *Bob.*

$$Alice \rightarrow \{E_{K_B}(Na, Nb)\} \rightarrow Bob \qquad (3)$$

Bob отправляет *Trent* оба идентификатора и случайные числа, шифруя его открытом ключом *Trent*.

$$Bob \rightarrow \{E_{K_T}(A, B, Na, Nb)\} \rightarrow Trent \qquad (4)$$

Trent расшифровывает сообщения от *Bob*, узнаёт идентификаторы и случайные числа участников, после чего генерирует сессионный ключ K и отправляет *Bob* два сообщения:

— в первом сообщении содержатся: идентификатор *Bob* (*B*), оба случайных числа (Na, Nb) и сессионный ключ (*K*), зашифрованные на открытом ключе *Alice*;

— во втором сообщении содержатся: идентификатор *Alice* (*A*), оба случайных числа (Na, Nb) и сессионный ключ (*K*), зашифрованные на открытом ключе *Bob*:

$$Trent \rightarrow \{E_{K_A}(B, Na, Nb, K), E_{K_B}(A, Na, Nb, K)\} \rightarrow Bob \quad (5)$$

Bob отправляет *Alice* два сообщения:

1) это сообщение (5), полученное от *Trent*;

2) оба случайных числа, зашифрованные на сессионном ключе:

$$Bob \rightarrow \{E_{K_A}(B, Na, Nb, K), \quad (6)$$

Alice расшифровывает первое сообщение, получает ключ K, расшифровывает второе сообщение и отправляет *Bob* его случайное число:

$$Alice \rightarrow \{E_K(Nb)\} \rightarrow Bob \quad E_K(Na, Nb)\} \rightarrow Alice \quad (7)$$

Таким образом задача генерации и безопасного распределения симметричного сессионного ключа решена при выполнении условия доверия к третьему лицу.

Моделирование протокола и анализ полученных результатов

Принятый авторами подход к верификации предлагаемого метода базируется на известных концепциях[6], получивших подтверждение и развитие в современных работах [16, 17,18, 19], и использует предположение о корректности преобразований следующих элементов: *метод → протокол → алгоритм → формальное описание→ автоматическая верификация в специализированной среде → результат*.

Для моделирования и верификации безопасности протокола взаимодействия трех сторон, базирующегося на предложенном *методе* (1–7), в работе использовано специализированное инструментальное средство AVISPA (Automated Validation of Internet Security Protocols and Applications)[7] с поддержкой языка HLPSL (High Level Protocol Specification Language).

AVISPA — это расширяемый модульный инструмент для автоматической проверки протоколов и приложений (рис. 1). Он использует язык HLPLS для формализованного описания безопасности тестируемых протоколов, набор инструментов для их формальной проверки и модели широко распространённых интерфейсов.

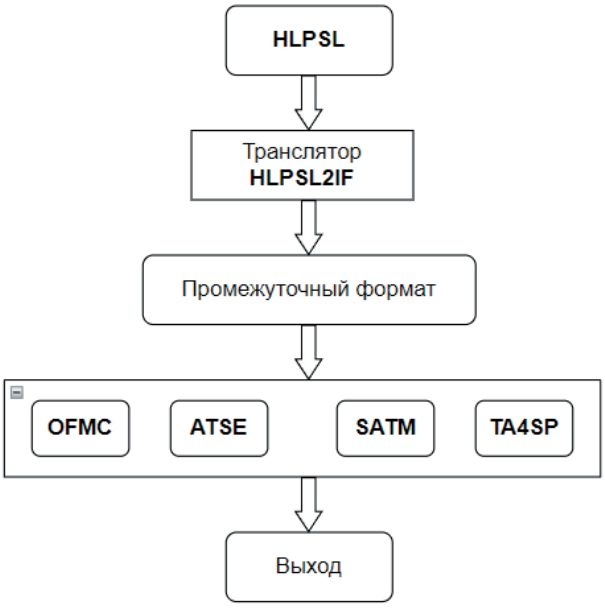

Рис. 1. Упрощённая архитектура инструментального средства AVISPA

OFMC и CL-AtSe — формализованные компоненты для анализа безопасности криптографических протоколов: OFMC ориентирован на проверку общих свойств безопасности, таких как аутентификация и секретность: модуль CL-AtSe целесообразно использовать для анализа конкретных атак.

Выбор инструментального средства определяется прежде всего: доверием профессионального сообщества, доказуемостью, удобством и наглядностью интерпретации результатов, гибкостью языка и доступностью самого инструментального средства.

В настоящей работе протокол взаимной аутентификации и распределения ключей проверен с использованием модулей OFMC и ATSE.

В исследуемом протоколе (1–7) взаимодействуют

6 И. В. Котенко, С. А. Резник, А. В. Шоров, Верификация протоколов безопасности на основе комбинированного использования существующих методов и средств, Тр. СПИИРАН, 2009, выпуск 8, 292–310

7 AVISPA. Deliverable 2.1: The High-Level Protocol Specification Language. Available. URL: https://www.avispa-project.org/(дата обращения 30.08.2023).

```
role role_A(A,B,T       :agent,
            PKa,PKb,PKt : public_key,
            SND,RCV     : channel(dy))
played_by A
def=
        local
                State:nat,
                Na, Nb,Nas:text,
                K: symmetric_key

        init    State := 0
        transition
        1. State  = 0   /\ RCV(start) =|>
           State':= 1   /\ Na' := new() /\ SND({A.Na'}_PKb)

        2. State  = 1   /\ RCV({B.Nb'.Na}_PKa)
                        /\ request(A,B,alice_bob_na,Na) =|>
           State':= 2   /\ SND({Na.Nb'}_PKb)
                        /\ witness(A,B,bob_alice_nb,Nb')
        3. State  = 2   /\ RCV({B.Na.Nb.K'}_PKa.{Na.Nb}_K') =|>
           State':= 3   /\ SND({Nb}_K')
                        /\ witness(A,B,bob_alice_k,K')
end role
```

```
role role_B(B,A,T       : agent,
            PKb,PKa,PKt : public_key,
            SND,RCV     : channel(dy))
played_by B
def=
        local
                State:nat,
                Na,Nb:text,
                K:symmetric_key

        init    State := 0
        transition
        1. State  = 0   /\ RCV({A.Na'}_PKb) =|>
           State':= 1   /\ Nb' := new() /\ SND({B.Nb'.Na'}_PKa)
                        /\ witness(B,A,alice_bob_na,Na')

        2. State  = 1   /\ RCV({Na.Nb}_PKb)
                        /\ request(B,A,bob_alice_nb,Nb) =|>
           State':= 2   /\ SND({A.B.Na.Nb}_PKt)

        3. State  = 2   /\ RCV({B.Na.Nb.K'}_PKa.{A.Na.Nb.K'}_PKb)
                        /\ request(B,T,bob_trusted_nb,Nb) =|>
           State':= 3   /\ SND({B.Na.Nb.K'}_PKa.{Na.Nb}_K')

        4. State  = 3   /\ RCV({Nb}_K) =|>
           State':= 4   /\ request(B,A,bob_alice_k,K)
end role
```

```
role role_T(T,A,B       :agent,
            PKt,PKa,PKb :public_key,
            SND,RCV     :channel(dy))
played_by T
def=
        local
                State:nat,
                Na,Nb:text,
                K:symmetric_key

        init    State := 0
        transition
        1. State  = 0   /\ RCV({A.B.Na'.Nb'}_PKt) =|>
           State':= 1   /\ K' := new()
                        /\ SND({B.Na'.Nb'.K'}_PKa.{A.Na'.Nb'.K'}_PKb)
                        /\ witness(T,B,bob_trusted_nb,Nb')
                        /\ secret(K',sec_1,{A,B,T})

end role
```

Рис. 2. Описание протокола взаимодействия агентов на языке HLPSL

3 агента *A* (*Alice*), *B (Bob*) и T (*Trent*). Формализованное описание действий агентов на языке HLPSL представлено на рис. 2.

Согласно условиям функционирования требованиями к протоколу являются: секретность данных, взаимная аутентификация агентов и защита от некоторых атак. Формализованное описание целей в терминах AVISPA представлено на рис. 3.

```
goal
        % Secrecy of the key
        secrecy_of sec_1
        % Agent A authenticates agent B
        authentication_on alice_bob_na
        % Agent B authenticates agent A
        authentication_on bob_alice_nb
        authentication_on bob_alice_k
        % Agent B authenticates agent T
        authentication_on bob_trusted_nb
end goal
```

Рис. 3. Цели протокола аутентификации

Параллельные процедуры взаимодействия показаны в «роли среды» (рис. 4), в которой злоумышленник может осуществить атаку.

В результате подготовительных процедур (рис. 2–4) завершено формирование исходных данных для проведения автоматического модельного эксперимента по оценке заданных требований информационной безопасности исследуемого протокола.

Результаты моделирования с использованием модулей OFMC и ATSE представлены на рис.5.а и 5.б соответственно: исследуемый протокол в рамках описанных формализмов и заданных типов атак безопасен (SUMMARY: SAFE). Защита от атак повтора обеспечивается уникальностью случайных чисел (Na, Nb), генерируемых (1, 2) в процессе взаимодействия.

На рис. 6 представлено графическое представление процесса моделирования последовательного взаимодействия между агентами *A*, *B* и *T*.

```
role environment()
def=
        const
                pka,pkb,pki,pkt:public_key,
                alice,bob,trusted:agent,
                sec_1,alice_bob_na,bob_alice_nb,bob_alice_k,bob_trusted_nb:protocol_id
        intruder_knowledge = {alice,bob,trusted,pka,pkb,pkt,pki,inv(pki)}
        composition
                %% We run the regular session
                session(alice,bob,trusted,pka,pkb,pkt)
                %% in parallel with another regular session
                /\ session(alice,bob,trusted,pka,pkb,pkt)
                %% and a session between the intruder  and bob
                /\ session(i,bob,trusted,pki,pkb,pkt)
                %% and a session between alice and the intruder)
                /\ session(alice,i,trusted,pka,pki,pkt)
end role
```

Рис. 4. Описание среды взаимодействия агентов.

```
% OFMC
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/keyExchange8.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 11.44s
  visitedNodes: 10608 nodes
  depth: 10 plies
```

А

а)

```
% ATSE
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/keyExchange8.if

GOAL
  As_specified

BACKEND
  CL-AtSe

STATISTICS
  Analysed : 24 states
  Reachable : 4 states
  Translation : 0.00 seconds
  Computation : 0.00 seconds
```

Б

б)

Рис. 5. Результаты проверки на модуль OFMC и ATSE

Диаграмма взаимодействия, с учётом возможностей атакующего (сторона *Intruder)* по реализации атаки типа MITM, представлена на рис. 7. Переход осуществляется из поля «входящие события» в «прошедшие события». Результаты моделирования в инструменте AVISPA иллюстрирует, что, хотя злоумышленник и перехватил сообщение, секретная информация осталась для него недоступной.

На основе анализа полученных данных формулируется вывод: исследуемый протокол взаимной аутентификации и распределения ключей является безопасным, обеспечивающим выполнение требований (целей) безопасности, установленных на этапе формализации требований к методу: безопасность данных, взаимная аутентификация стороны, защита от повторных атак, атаки MITM.

Применение протокола не требует вовлечения контрагентов в единую инфраструктуру открытых ключей, достаточным условием является попарное доверие к третьей промежуточной стороне. Это обеспечивает возможность взаимодействия контрагентов из различных нормативно-регуляторных, национальных и территориальных зон.

Заключение

В работе поставлена и решена задача разработки *метода* генерации и распределения симметричного сессионного ключа, устойчивого к атакам типа MITM и повтора, для двух контрагентов с использованием доверенной третьей стороны.

Проведено формализованное доказательства безопасности реализующего его *протокола* в задан-

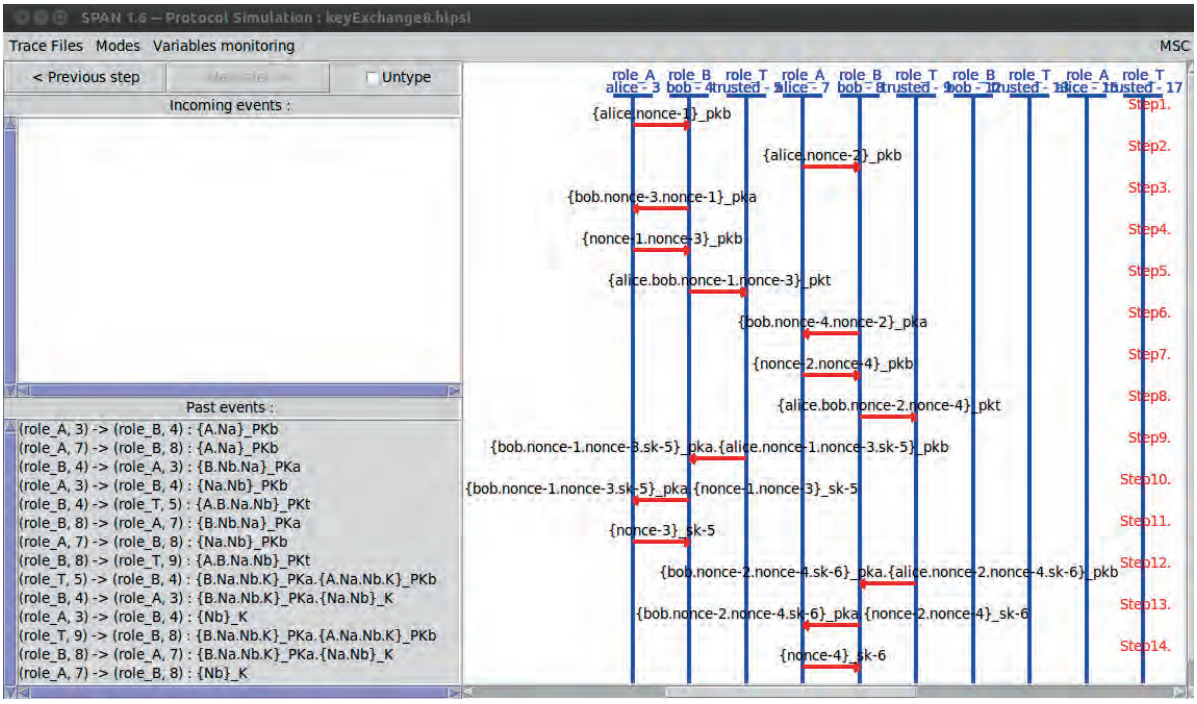

Рис. 6. Эмуляция протокола безопасности на AVISPA

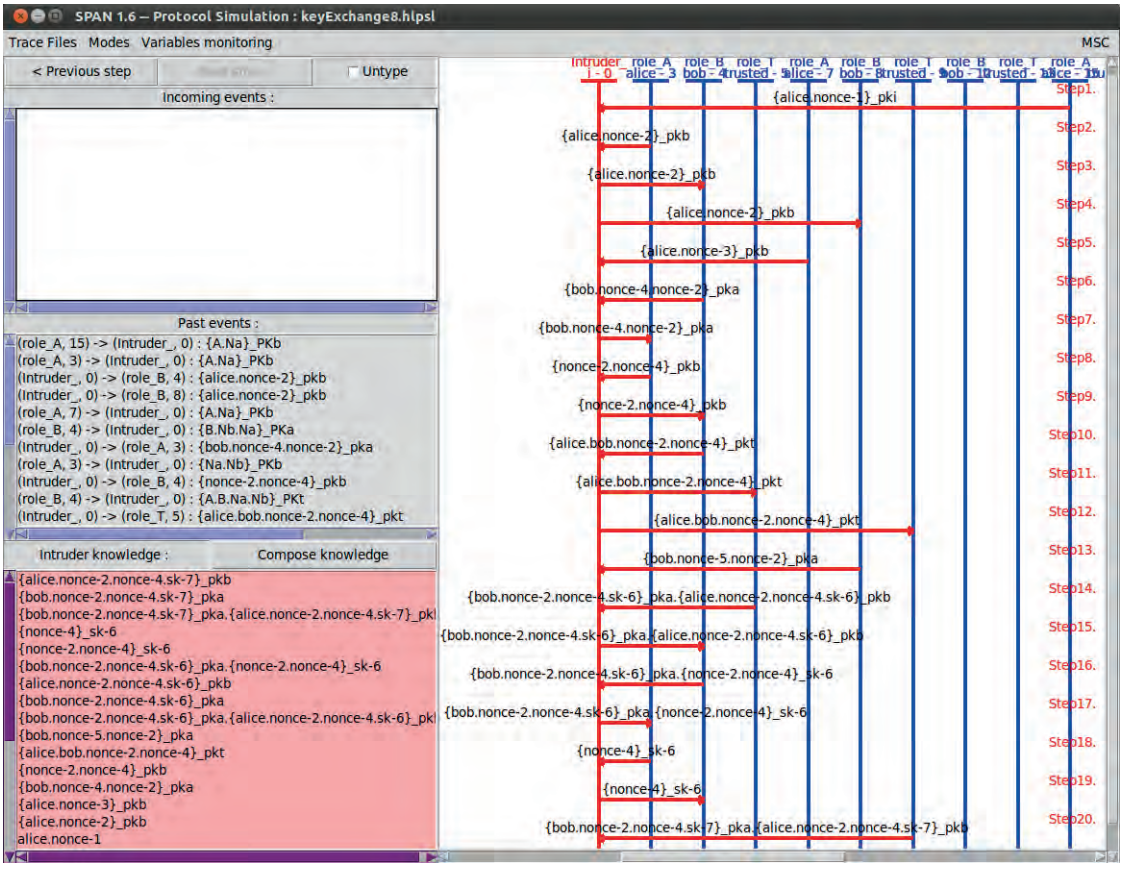

Рис. 7. Эмуляция протокола с учётом действий злоумышленника

ных условиях функционирования с использованием специализированного инструментального средства. Результаты моделирования подтверждают информационную безопасность предложенного протокола по обеспечению взаимной аутентификации, конфиденциальности данных, предотвращению атак MITM и повтора в рамках заданных ограничений.

Применение предлагаемых решений целесообразно для решения задач обеспечения конфиденциальности частной информации в системе отслеживания на основе блокчейна. В частности – для решения задач обеспечения аутентифицированного доступа к приватной части записи блока распределённого реестра, что является типовой задачей в системах прослеживаемости качества товара.

Литература

1. 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
2. Комарова А. В., Коробейников А. Г. Анализ основных существующих пост-квантовых подходов и схем электронной подписи //Вопросы кибербезопасности. – 2019. – №. 2 (30). – С. 58-68. DOI: 10.21681/2311-3456-2019-2-58-68
3. Макаров В. В., Волчик О. В. Цифровизация систем менеджмента качества в нефтегазовой отрасли // Экономика и качество систем связи. – 2023. – №. 1 (27). – С. 4–13.
4. Kolesnikova D. et al. Features of information support for decision-making in planning production processes //AIP Conference Proceedings. – AIP Publishing LLC, 2021. – Т. 2402. – №. 1. – С. 040036. DOI: 10.1063/5.0071707
5. Usova M., Chuprov S., Viksnin I. Informational space and messages interaction models for smart factory concept //2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT. – IEEE, 2020. – С. 617–621. DOI: 10.1109/MetroInd4.0IoT48571.2020.9138292
6. Лэ В., Ву Л., Комаров И. И. Обеспечение информационной безопасности в системе прослеживаемости морепродуктов на основе технологии блокчейна // Наука и бизнес: пути развития - 2022. - № 5(131). - С. 97–101
7. Котенко И.В., Саенко И.Б., Захарченко Р.И., Капустин А.С., Аль-Барри М.Х., Управление доступом к электронной информационно-образовательной среде вузов федеральных органов исполнительной власти// Вопросы кибербезопасности. 2023. № 2 (54). С. 73-84. DOI: 10.21681/2311-3456-2023-2-73-84
8. Куликов А. Л., Зинин В. М. Требования к информационной безопасности в электроэнергетике и их реализация в интеллектуальных устройствах цифровых подстанций //Интеллектуальная электротехника. – 2022. – №. 3 (19). – С. 49–78. DOI 10.46960/2658-6754_2022_3_49
9. Болдырев И. А. и др. Концепция распределённой ИИУС на основе технологий промышленного IoT для повышения отслеживаемости, экономичности и безопасности систем микрогрид //Современные проблемы теплофизики и энергетики. – 2020. – С. 489–490.
10. Язов Ю. К., Авсентьев А. О. Пути построения многоагентной системы защиты информации от утечки по техническим каналам // Вопросы кибербезопасности. – 2022. – №. 5. – С. 51. DOI: 10.21681/2311-3456-2022-5-2-13
11. Viksnin I. I., Marinenkov E. D., Chuprov S. S. A Game Theory approach for communication security and safety assurance in cyber-physical systems with Reputation and Trust-based mechanisms //Научно-технический вестник информационных технологий, механики и оптики. – 2022. – Т. 22. – №. 1. – С. 47-59. DOI: 10.17586/2226-1494-2022-22-1-47-59
12. Балюк А. А., Финько О. А. Многоагентная аутентификация цифровых двойников в киберфизических системах //Вопросы кибербезопасности. – 2022. – №. 5. – С. 51. DOI: 10.21681/2311-3456-2022-5-100-113
13. Yingwen Chen, Linghang Meng, Huan Zhou, Guangtao Xue, «A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection», Wireless Communications and Mobile Computing, vol. 2021, Article ID 6685762, 12 pages, 2021. https://doi.org/10.1155/2021/6685762
14. Zheng BK, Zhu LH, Shen M et al. Scalable and privacy-preserving data sharing based on blockchain. Journal of computer science and technology 33(3): 557–567 May 2018. DOI 10.1007/s11390-018-1840-5
15. Yuhan Yang, Lijun Wei, Jing Wu, and Chengnian Long. 2020. Block-SMPC: A Blockchain-based Secure Multi-party Computation for Privacy-Protected Data Sharing. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology (ICBCT'20). Association for Computing Machinery, New York, NY, USA, March 2020 Pages 46–51. https://doi.org/10.1145/3390566.3391664
16. Миронов А. М. Математическая модель и методы верификации криптографических протоколов //Интеллектуальные системы. – 2022. – Т. 26. – №. 2. – С. 85–144.
17. Нестеренко А. Ю., Семенов А. М. Методика оценки свойств безопасности криптографических протоколов //Межвузовская научно-техническая конференция студентов, аспирантов и молодых специалистов имени Е.В. Арменского. – 2021. – С. 249–251.
18. Перевышина Е. А., Бабенко Л. К. Моделирование свойств безопасности аутентификации криптографических протоколов с использованием средств формальной верификации SPIN //Информатизация и связь. – 2020. – №. 3. – С. 21-25. DOI: 10.34219/2078-8320-2020-11-3-21-25
19. Михайлова А. А., Уманский С. А., Шустрова А. Н. Критерии и методы оценки безопасности протоколов аутентификации //Цифровая наука. – 2021. – №. 6–1. – С. 4–10.

VERIFICATION OF SESSION KEY SAFE DISTRIBUTION METHOD IN THE PRODUCT QUALITY TRACEABILITY SYSTEM

Le W.H.[8], Begaev A.N.[9], Komarov I.I.[10], Fung W.K.[11]

The purpose of the work is *to determine the requirements for ensuring the basic and additional properties of information security in the interaction of counterparties in information systems related to ensuring the traceability of product quality; to develop and formally verify the method of generation and secure distribution of a session key that meets these requirements.*

Result: *The use of product quality traceability systems is a powerful tool for solving a wide range of technological and social problems, for example: state control in regulated areas, ensuring consumer safety, forming a competitive advantage of the manufacturer, etc. However, the widespread introduction of such decentralized systems is associated with a number of contradictions, one of which is directly related to the problem of ensuring data confidentiality and the need for their controlled use in the dynamic composition of counterparties and consumers. The paper proposes a direction for overcoming this contradiction by forming scenarios for obtaining controlled access to the private information of the interacting party using cryptographic procedures. To implement such scenarios, a method and a protocol based on it have been developed for generating and distributing a secret session key using a trusted third party. A formal proof of the security of the proposed solution is provided using a specialized tool for protocol verification. The results obtained are primarily focused on application in distributed ledger systems, which involve the division of data into private and public blocks. However, they can also be used in other systems that require confidentiality, accessibility, and unprovability, especially when there are limitations on computing resources.*

Scientific novelty: *consists in the problem-oriented analysis of the specific requirements for ensuring the information security of the process of entering and extracting data into the system for tracking the quality of goods in the given scenarios of its use. Based on the selected requirements, the problem of developing an adapted method for generating and distributing a secret session key between two subscribers with the involvement of a trusted party is formulated and solved. Based on the developed A practical communication protocol is synthesized and a formal proof of compliance with the specified information security requirements, resistance to MITM and repetition attacks is carried out.*

Keywords: *cybersecurity, confidentiality, non-repudiation, session cryptographic key, distributed register, formal protocol verification.*

References

1. Petrenko A. S., Petrenko S. A. Metod ocenivanija kvantovoj ustojchivosti blokchejn-platform //Voprosy kiberbezopasnosti. – 2022. – №. 3 (49). – S. 2–22. DOI: 10.21681/2311-3456-2022-3-2-22
2. Komarova A. V., Korobejnikov A. G. Analiz osnovnyh sushhestvujushhih post-kvantovyh podhodov i shem jelektronnoj podpisi //Voprosy kiberbezopasnosti. – 2019. – №. 2 (30). – S. 58-68. DOI: 10.21681/2311-3456-2019-2-58-68
3. Makarov V. V., Volchik O. V. Cifrovizacija sistem menedzhmenta kachestva v neftegazovoj otrasli // Jekonomika i kachestvo sistem svjazi. – 2023. – №. 1 (27). – S. 4–13.
4. Kolesnikova D. et al. Features of information support for decision-making in planning production processes //AIP Conference Proceedings. – AIP Publishing LLC, 2021. – T. 2402. – №. 1. – S. 040036. DOI: 10.1063/5.0071707
5. Usova M., Chuprov S., Viksnin I. Informational space and messages interaction models for smart factory concept //2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT. – IEEE, 2020. – S. 617–621. DOI: 10.1109/MetroInd4.0IoT48571.2020.9138292

8 Le W.H., Ph.D. student, Faculty of Information Technology Security, ITMO University, St. Petersburg, Russia. E-mail: hieule250715@gmail.com

9 Alexey N. Begaev, Ph.D. (Technology), Professor at ITMO University, CEO of Echelon North-West, St. Petersburg, Russia. E-mail: begaev@mail.ru

10 Igor I. Komarov, Ph.D. (Physics & Mathematics), Associate Professor, Faculty of Information Technology Security, ITMO University, St. Petersburg, Russia. E-mail: i_krov@mail.ru

11 Fung W.K., Ph.D. student, Faculty of Software Engineering and Computer Engineering, ITMO University, St. Petersburg, Russia. E-mail: hieule250715@gmail.com

6. Lje V., Vu L., Komarov I. I. Obespechenie informacionnoj bezopasnosti v sisteme proslezhivaemosti moreproduktov na osnove tehnologii blokchejna // Nauka i biznes: puti razvitija - 2022. - № 5(131). - S. 97–101
7. Kotenko I.V., Saenko I.B., Zaharchenko R.I., Kapustin A.S., Al'-Barri M.H., Upravlenie dostupom k jelektronnoj informacionno-obrazovatel'noj srede vuzov federal'nyh organov ispolnitel'noj vlasti//Voprosy kiberbezopasnosti. 2023. № 2 (54). S. 73-84. DOI: 10.21681/2311-3456-2023-2-73-84
8. Kulikov A. L., Zinin V. M. Trebovanija k informacionnoj bezopasnosti v jelektrojenergetike i ih realizacija v intellektual'nyh ustrojstvah cifrovyh podstancij //Intellektual'naja jelektrotehnika. – 2022. – №. 3 (19). – S. 49–78. DOI 10.46960/2658-6754_2022_3_49
9. Boldyrev I. A. i dr. Koncepcija raspredeljonnoj IIUS na osnove tehnologij promyshlennogo IoT dlja povyshenija otslezhivaemosti, jekonomichnosti i bezopasnosti sistem mikrogrid //Sovremennye problemy teplofiziki i jenergetiki. – 2020. – S. 489–490.
10. Jazov Ju. K., Avsent'ev A. O. Puti postroenija mnogoagentnoj sistemy zashhity informacii ot utechki po tehnicheskim kanalam //Voprosy kiberbezopasnosti. – 2022. – №. 5. – S. 51. DOI: 10.21681/2311-3456-2022-5-2-13
11. Viksnin I. I., Marinenkov E. D., Chuprov S. S. A Game Theory approach for communication security and safety assurance in cyber-physical systems with Reputation and Trust-based mechanisms //Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. – 2022. – T. 22. – №. 1. – S. 47-59. DOI: 10.17586/2226-1494-2022-22-1-47-59
12. Baljuk A. A., Fin'ko O. A. Mnogoagentnaja autentifikacija cifrovyh dvojnikov v kiberfizicheskih sistemah //Voprosy kiberbezopasnosti. – 2022. – №. 5. – S. 51. DOI: 10.21681/2311-3456-2022-5-100-113
13. Yingwen Chen, Linghang Meng, Huan Zhou, Guangtao Xue, "A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection", Wireless Communications and Mobile Computing, vol. 2021, Article ID 6685762, 12 pages, 2021. https://doi.org/10.1155/2021/6685762
14. Zheng BK, Zhu LH, Shen M et al. Scalable and privacy-preserving data sharing based on blockchain. Journal of computer science and technology 33(3): 557–567 May 2018. DOI 10.1007/s11390-018-1840-5
15. Yuhan Yang, Lijun Wei, Jing Wu, and Chengnian Long. 2020. Block-SMPC: A Blockchain-based Secure Multi-party Computation for Privacy-Protected Data Sharing. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology (ICBCT'20). Association for Computing Machinery, New York, NY, USA, March 2020 Pages 46–51. https://doi.org/10.1145/3390566.3391664
16. Mironov A. M. Matematicheskaja model' i metody verifikacii kriptograficheskih protokolov //Intellektual'nye sistemy. – 2022. – T. 26. – №. 2. – S. 85–144.
17. Nesterenko A. Ju., Semenov A. M. Metodika ocenki svojstv bezopasnosti kriptograficheskih protokolov //Mezhvuzovskaja nauchno-tehnicheskaja konferencija studentov, aspirantov i molodyh specialistov imeni E.V. Armenskogo. – 2021. – S. 249–251.
18. Perevyshina E. A., Babenko L. K. Modelirovanie svojstv bezopasnosti autentifikacii kriptograficheskih protokolov s ispol'zovaniem sredstv formal'noj verifikacii SPIN //Informatizacija i svjaz'. – 2020. – №. 3. – S. 21-25. DOI: 10.34219/2078-8320-2020-11-3-21-25
19. Mihajlova A. A., Umanskij S. A., Shustrova A. N. Kriterii i metody ocenki bezopasnosti protokolov autentifikacii //Cifrovaja nauka. – 2021. – №. 6–1. – S. 4–10.

АНАЛИЗ РЕАЛИЗАЦИИ ТЕХНОЛОГИЙ КОНФИДЕНЦИАЛЬНЫХ ВЫЧИСЛЕНИЙ

Загартдинов Б.Н.[1], Поляков М.В.[2]

Цель исследования: *анализ современного состояния технологий конфиденциальных вычислений.*

Метод исследования: *систематизация и анализ существующих решений реализующих аппаратную среду конфиденциальных вычислений.*

Результат исследования: *в статье проведены оценка моделей угроз аппаратных технологий конфиденциальных вычислений, таких как Intel TDX, AMD SEV или ARM CCA, и анализ их реализации. Выявлены общие признаки и рассмотрены особенности каждой из реализаций. Обнаружены основные проблемы, с которыми сталкиваются разработчики подобных систем: сложности с повторным использованием существующих технологий безопасности и необходимость проектирования технологий с учетом жизненного цикла защищаемого программного обеспечения. В каждой реализации применяются различные методы решения данных проблем. Главным преимуществом использования аппаратных технологий конфиденциальных вычислений является обработка данных в защищенных контейнерах, за счет чего обеспечивается конфиденциальность и целостность чувствительной информации. Поэтому решения данного типа могут быть рассмотрены к внедрению в распределенные системы в перспективе позволяя повысить их производительность за счет эффективного использования вычислительных ресурсов без ущерба для конфиденциальности.*

Научная новизна: *состоит в том, что представленная статья является одной из первых отечественных работ, представляющих анализ и систематизацию решений реализующих аппаратную среду конфиденциальных вычислений. Выявлены основные черты характеризующие современные системы конфиденциальных вычислений, а также проблемы, возникающие в процессе разработке таких систем.*

Ключевые слова: *безопасность облачных вычислений, аппаратные доверенные среды выполнения, удаленная аттестация, безопасность данных, информационная безопасность.*

DOI:10.21681/2311-3456-2023-6-122-127

Введение

В современных вычислительных системах и комплексах данные существуют в трех состояниях: в состоянии покоя (например, во время хранения на постоянных носителях информации), в использовании (во временной памяти) и во время передачи по каналам коммуникации. Для защиты данных при передаче по коммуникационным каналам используются хорошо изученные криптографические протоколы для конфиденциального обмена данными. Защита данных в состоянии покоя может рассматриваться как распределенный во времени криптографический протокол с предварительно согласованным общим секретом. В свою очередь вопрос защиты данных в процессе использования остается открытым.

Впервые о защите данных в процессе использования посредством применения криптографической защиты задумались в 1978 Ривест, Адлеман и Дертузос в своей работе[3], а в 1982 году в статье Эндрю Яо[4] впервые была упомянута проблема организации многосторонних безопасных вычислений. Потребовалось несколько десятков лет, чтобы идеи, предложенные Ривестом, Адлеманом, Дертузосом и Яо были восприняты научным сообществом. В настоящий момент, несмотря на большое количество академических работ, описывающих алгоритмы полностью гомоморфного шифрования и протоколы многосторонних безопасных вычислений, идеи не получили широкого

3 Rivest R. L. et al. On data banks and privacy homomorphisms //Foundations of secure computation. – 1978. – Т. 4. – №. 11. – С. 169-180.

4 Yao A. C. Protocols for secure computations //23rd annual symposium on foundations of computer science (sfcs 1982). – IEEE, 1982. – С. 160-164

1 Загартдинов Булат Назимович, магистр НИЯУ МИФИ, специалист НТЦ Вулкан, Москва, Россия. E-mail: me@vaire.lt

2 Поляков Михаил Вадимович, старший преподаватель МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: m.polyakov@bmstu.ru

практического применения и остаются нереализованными в прикладных приложениях по различным причинам. В работах [1] и [2] подробно разобраны существующие проблемы, препятствующие практической реализации гомоморфного шифрования и многосторонних безопасных вычислений.

На практике внедрение механизмов защиты данных во время использования позволяет предотвратить сразу несколько известных классов атак: RowHammer [3], Hyperjacking [4], DMA-атаки [5, 6], ColdBoot [7, 8].

В процессе развития методов построения вычислительных систем было предложено несколько различных решений, частично покрывающих вопросы защиты данных в процессе использования: скремблирование оперативной памяти для защиты от прямого чтения шины данных, Input/Output Memory Management Unit (IOMMU) для защиты от DMA-атак, аппаратные и программные доверенные среды выполнения для защиты от компрометации некоторых приложений, обрабатывающих критичные данные, со стороны непривилегированного ПО, выполняемого на той же системе.

Конфиденциальные вычисления – следующий этап развития прикладных технологий защиты данных во время использования. В то время как каждое решение покрывает лишь часть атак, они обобщают опыт предыдущих технологий и предоставляют приемлемое с практической точки зрения решение проблемы защиты данных во время использования.

Вопросы внедрения концепции конфиденциальных вычислений в индустриальные решения рассматриваются консорциумом конфиденциальных вычислений[5], однако пока термин конфиденциальные вычисления не имеет четкого определения, поскольку предложенные консорциумом формулировки являются достаточно расплывчатыми и нуждаются в доработке [9]. Несмотря на отсутствие строгой формулировки, возможно формализовать ряд требований, которым соответствуют решения, реализующие концепцию конфиденциальных вычислений, в научном сообществе термин используется для обобщения существующих решений, реализующих в первую очередь защиту от атак со стороны гипервизора, а также предоставляющих механизмы аттестации доверенной вычислительной базы.

Далее в работе виртуальная машина будет именоваться гостем, а гипервизор или ОС выполняющая роль гипервизора хостом.

1. Существующие решения

Реализация концепции конфиденциальных вычислений возможна как в рамках центрального процессора, так и за его пределами. Например, в работе [10] представлено решение, реализующее эту концепцию для решения задачи конфиденциального обучения моделей искусственного интеллекта в формате платы расширения с интерфейсом PCIe. Однако поскольку подобные расширения создаются для решения частных задач их применение имеет ограниченный характер. Далее в работе анализируются реализации, расширяющие функционал центрального процессора, поскольку их применение позволяет решать более широкий круг задач.

К индустриальным решениям, реализующим концепцию конфиденциальных вычислений, относятся следующие архитектурные решения:

- Intel Trust Domain Executions (TDX)
- AMD Secure Encrypted Virtualization – Secure Nested Paging (SEV-SNP)
- ARM Confidential Compute Architecture (CCA)
- IBM Protected Execution Facility (PEF)
- IBM Z Secure Execution
- RISC-V Application Processor Trusted Execution Environment (AP-TEE)

Данные решения сформировались вследствие развития отрасли в целом и моделей угроз каждого производителя или исследовательской группы, в частности. Каждое решение имеет уникальные особенности, но можно выделить ряд черт, характерных для каждого из них:

1.1. Аппаратная поддержка изоляции от привилегированного злоумышленника

Каждое решение вводит свой архитектурный примитив изоляции: Trusted Domains, Realm, Confidential/Trusted/Protected Virtual Machine и другие. В зависимости от технологии обеспечивается гарантия сохранения конфиденциальности и целостности против целого класса злоумышленников.

1.2. Малый размер доверенной вычислительной базы

Минимизация доверенной вычислительной базы снижает поверхность атаки позволяя гарантировать другие свойства безопасности вычислительной систем, например конфиденциальность и целостность памяти виртуальной машины.

5 Confidential Computing Consortium Scope [https://confidentialcomputing.io/scope/]

1.3. Аппаратный корень доверия и удаленная аттестация

Большинство технологий предоставляют аппаратный корень доверия (первоначальный этап загрузки в совокупности с платформо-зависимыми секретными параметрами) и протокол удаленной аттестации (верификация программно-аппаратной среды исполнения), с помощью которых удаленный клиент может получить надежные криптографические доказательства, что программное обеспечение было запущено в корректно инициализированной изолированной программно-аппаратной среде на удаленной (или локальной) машине.

2. AMD SEV-SNP

Модель угроз AMD SEV-SNP[6] включает в себя: атаки перехвата гипервизора, DMA атаки, атаки повторного использования на зашифрованных страницах памяти, манипуляции страницами памяти в таблице трансляции виртуальной машины, ColdBoot атаки, откат версии доверенной вычислительной базы.

Не включены в модель угроз атаки по побочным каналам с манипуляцией кэшем и таблицами трансляции, отказ в обслуживании гостевой виртуальной машины.

Основой защиты данных в AMD SEV-SNP является сопроцессор безопасности AMD PSP, встроенный в корпус основного процессора. Сопроцессор безопасности отвечает за шифрование памяти защищаемых виртуальных машин. Шифрование страниц памяти защищаемых виртуальных машин осуществляется с помощью AES на своем ключе, генерируемом при инициализации виртуальной машины, изменяющемся при каждой перезагрузке вычислительной системы. Зашифрованные страницы помечаются специальным битом в таблице трансляции. Технология SEV-SNP предоставляет механизм удаленной аттестации платформы с использованием аппаратного корня аттестации, предоставляемого сопроцессором безопасности. Для защиты целостности страниц защищенных виртуальных машин используется контролируемая сопроцессором безопасности таблица Reverse Mapping Table (RMP). Таблица индексируется физическим адресом страницы хоста, а каждая ее запись содержит физический адрес гостевой страницы, на который отображается соответствующая физическая страница хоста. RMP предотвращает неавторизованную запись в зашифрованные страницы, однако чтение зашифрованного содержимого страниц по-прежнему возможно.

AMD SEV-SNP также вводит разделение привилегий внутри защищенной виртуальной машины на 4 уровня от 0 до 3, где Virtual Machine Privilege Level 0 (VMPL0) наиболее привилегированный, а VMPL3 наименее.

3. Intel TDX

Модель угроз Intel TDX включает в себя атаки с физическим или удаленным доступом к вычислительной машине и контролем над загрузочным ПО, ПО в режиме System Management Mode (SMM), хостовой ОС, гипервизором и периферийными устройствами. Доступность защищаемой виртуальной машины при этом не гарантируется.

В реализации Intel TDX [11] применяются в том числе уже существующие технологии:

- Virtualization Technology (VT) как основа для виртуализации.
- Multi-key Total Memory Encryption (MKTME) в качестве аппаратного компонента используемого для шифрования страниц памяти.
- Guard Extensions (SGX) в качестве источника изученных на практике механизмов аттестации.
- Data Center Attestation Primitives (DCAP) в совокупности с алгоритмами SGX как автономный сервис аттестации.

Расширение Intel TDX вводит новый режим исполнения кода – Secure-Arbitration Mode (SEAM). Модуль TDX – программный компонент, выполняемый в режиме SEAM VMX-root, который предназначен для выполнения функций по управлению защищенными виртуальными машинами. К таким функциям относится запуск и управление защищенными виртуальными машинами – Trust Domains (TDs) в терминологии TDX, а также организация канала коммуникации между гипервизором и защищенными виртуальными машинами. Для управления защищенными страницами памяти используется отдельная таблица Secure-EPT, управление которой также возложено на Модуль TDX.

Каждой защищенной виртуальной машине назначается свой уникальный ключ шифрования памяти. TDX использует MKTME для шифрования страниц памяти защищенных виртуальных машин. Помимо шифрования, защищаемые страницы помещаются в специальную зону, недоступную за пределами Trusted Domain, выделяемую при помощи бита TD Owner. В TDX используются те же механизмы и инфраструктура удаленной и локальной аттестации что и в SGX.

6 AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More [https://www.amd.com/system/files/TechDocs/SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more.pdf]

4. ARM CCA

Модель угроз ARM CCA [12] включает в себя атаки без физического доступа, направленные на нарушение конфиденциальности или целостности данных защищаемой виртуальной машины, а именно: компрометация гипервизора, DMA атаки, переназначение памяти, программные атаки по побочным каналам.

В архитектуре ARM CCA добавляется новое расширение Realm Management Extension (RME)[7]. RME поддерживает новый тип проверяемой изолированной среды, называемый Realm. Виртуальная машина Realm отличается от доверенной операционной системы или доверенного приложения тем, что она управляется с хоста. В таких областях, как создание и распределение памяти, виртуальная машина Realm действует как любая другая виртуальная машина, управляемая с хоста. Кроме того, в режиме Realm отключены физические прерывания, все прерывания виртуализируются гипервизором, а затем передаются в гостевую операционную систему с помощью команд, обрабатываемых менеджером Realm режима (RMM). Это означает, что скомпрометированный гипервизор может помешать выполнению виртуальной машины Realm, поэтому в данном режиме нет никакой гарантии выполнения гостевой операционной системы, однако обеспечивается целостность и конфиденциальность.

CCA использует расширение Granule Protection Table (GPT) для отслеживания прав доступа к страницам памяти в различных режимах исполнения. Secure Monitor (Root World) управляет GPT, предоставляя интерфейс для изменения состояния таблицы со стороны менее привилегированного ПО (Non-Secure World, Secure World, Realm World).

5. IBM PEF/Z Secure Execution

Технология IBM Z Secure Execution [13] предоставляет поддержку для защищенных виртуальных машин, запускаемых в изолированной среде выполнения начиная с IBM Z15 и LinuxONE III. IBM Z Secure Execution вводит режим ультравизор в архитектуру IBM Z, используемый для подготовки и запуска защищенных виртуальных машин. Пользователь может использовать несколько симметричных ключей шифрования для различных данных, ключи помещаются в специальный заголовок и защищаются ключом шифрования платформы как часть разворачиваемого образа виртуальной машины. Начиная с IBM Z16 и LinuxONE Emperor 4 доступна удаленная аттестация.

Технология IBM PEF реализуемая с POWER9 также добавляет новый режим исполнения кода – ультравизор [14]. Задача ультравизора выступать связующим звеном между защищенным режимом исполнения и нормальным. Гипервизор запускает виртуальную машину, которая, используя инструкцию ESM (Enter Secure Mode) переходит в защищенный режим исполнения. Ультравизор конвертирует виртуальную машину в защищенную путем перемещения ее памяти в защищенную зону, недоступную не доверенному коду. Он использует Доверенный Платформенный Модуль (Trusted Platform Module – TPM) для формирования HMAC ключа, применяемого для проверки целостности, и симметричного ключа, используемого для расшифрования основной ОС. Доступ к TPM предоставляется ультравизору только в корректно загруженной системе, что обеспечивается посредством фиксации значений PCR регистров TPM.

6. RISC-V CoVE

Архитектурным расширением RISC-V CoVE [15] предусматривается защита от широкого класса злоумышленников: от непривилегированного программного обеспечения до системного ПО, аппаратных атак и атак по побочным каналам. Модель угроз RISC-V CoVE включает в себя:

- использование инструкций чтения/записи для доступа к защищаемым регионам памяти;
- программные атаки по стороннему каналу (атаки по кэшам, предсказателю переходов, отказам страниц, статистике выполнения);
- программные изменения памяти по побочному каналу (rowhammer);
- DMA-атаки;
- широкий класс атак внедрения аппаратного сбоя;
- атаки на используемые криптографические алгоритмы и примитивы;
- атаки понижения версии доверенной вычислительной базы.
- защита хоста от атак типа отказа в обслуживании со стороны защищаемой виртуальной машины также включена в модель угроз, в то время как обратная защита, как и в предыдущих решениях, не предусмотрена.

В качестве основы для RISC-V CoVE используется поддержка режима гипервизора, дополняемого конфиденциальным (Confidential) режимом исполнения.

7 Unlocking the power of data with Arm CCA [https://community.arm.com/arm-community-blogs/b/architectures-and-processors-blog/posts/unlocking-the-power-of-data-with-arm-cca]

Отслеживание дополнительного режима исполнения для каждого потока осуществляется посредством бита Confidential Qualifier. Для защиты страниц памяти конфиденциальных виртуальных машин вводится специальная битовая таблица Memory Tracking Table (MTT), содержащая информацию о защищаемых страницах.

Для обеспечения изоляции защищенных виртуальных машин вводится новый программный компонент – Trusted Execution Environment Security Manager (TSM). TSM выполняется в конфиденциальном режиме гипервизора и выступает в роли связующего звена между защищенными виртуальными машинами и гипервизором, выполняющим роль менеджера виртуальных машин. TSM-driver, работающий в режиме Machine, обеспечивает инициализацию системы, переключение между конфиденциальным и стандартным режимами, а также предоставляет интерфейс корня аттестации доверенной вычислительной базы.

Заключение

На текущем этапе развития основными проблемами, препятствующими широкому внедрению концепции конфиденциальных вычислений, являются сложности с повторным использованием существующих технологий безопасности и необходимость проектирования технологий с учетом жизненного цикла защищаемого программного обеспечения. Хотя все решения повторно используют криптографические алгоритмы для реализации механизмов аттестации, текущие реализации основаны на внедрении многих новых аппаратных компонентов безопасности. Новые компоненты требуют большого уровня доверия и изменений в системном программном обеспечении для управления жизненным циклом защищаемых объектов. Еще предстоит сформулировать терминологию для более точного описания набора уже существующих технологий конфиденциальных вычислений, а также связать эти технологии с развивающимися многосторонними вычислениями и гомоморфным шифрованием.

Несмотря на описанные проблемы технологии конфиденциальных вычислений активно развиваются и уже сейчас переходят от нишевого решения к массовому. Об этом свидетельствует повышенный интерес со стороны производителей процессоров, а также рост числа предложений размещения защищенных виртуальных машин у поставщиков облачных услуг, что позволяет повысить эффективность вычислений посредством интеграции технологий в распределенные вычислительные системы уже сейчас.

Литература

1. Аракелов Г. Г. Вопросы применения прикладной гомоморфной криптографии //Вопросы кибербезопасности. – 2019. – №. 5 (33). – С. 70-74.
2. Хлюпин А. А., Саакян А. О., Ниссенбаум О. В. Анализ эффективности алгоритмов шифрования для безопасных многосторонних вычислений //Математическое и информационное моделирование. – 2023. – С. 315-324.
3. Mutlu O., Kim J. S. Rowhammer: A retrospective //IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2019. – Т. 39. – №. 8. – С. 1555-1571.
4. Acosta G. The Role of Vmtheft and Hyperjacking in Virtualization: dissertation – Utica College, 2018.
5. Gross M. et al. Breaking trustzone memory isolation through malicious hardware on a modern fpga-soc //Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop. – 2019. – С. 3-12.
6. Markettos A. T. et al. Thunderclap: Exploring vulnerabilities in operating system IOMMU protection via DMA from untrustworthy peripherals. – 2019.
7. Won Y. S. et al. Practical cold boot attack on iot device-case study on raspberry pi //2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA). – IEEE, 2020. – С. 1-4.
8. Zimerman I., Nachmani E., Wolf L. Recovering AES Keys with a Deep Cold Boot Attack //International Conference on Machine Learning. – PMLR, 2021. – С. 12955-12966.
9. Sardar M. U., Fetzer C. Confidential computing and related technologies: a critical review //Cybersecurity. – 2023. – Т. 6. – №. 1. – С. 1-7.
10. Vaswani K. et al. Confidential machine learning within graphcore ipus //arXiv preprint arXiv:2205.09005. – 2022.
11. Cheng P. C. et al. Intel TDX Demystified: A Top-Down Approach //arXiv preprint arXiv:2303.15540. – 2023.
12. Li X. et al. Design and verification of the arm confidential compute architecture //16th USENIX Symposium on Operating Systems Design and Implementation (OSDI 22). – 2022. – С. 465-484.
13. Bornträger C. et al. Secure your cloud workloads with IBM Secure Execution for Linux on IBM z15 and LinuxONE III //IBM Journal of Research and Development. – 2020. – Т. 64. – №. 5/6. – С. 2: 1-2: 11.
14. Hunt G. D. H. et al. Confidential computing for OpenPOWER //Proceedings of the Sixteenth European Conference on Computer Systems. – 2021. – С. 294-310.
15. Sahita R. et al. CoVE: Towards Confidential Computing on RISC-V Platforms //Proceedings of the 20th ACM International Conference on Computing Frontiers. – 2023. – С. 315-321.

IMPLEMENTATION ANALYSIS OF CONFIDENTIAL COMPUTING TECHNOLOGIES

Zagartdinov B.N.[8], Polyakov M.V.[9]

Purpose: *analysis of the current state of confidential computing technologies.*

Methods: *systematization and analysis of existing and developing solutions implementing confidential computing.*

Result: *The article evaluates threat models of confidential computing hardware technologies, such as Intel TDX, AMD SEV or ARM CCA, and analyzes their implementation. Their common features are revealed and the features of each of the implementations are considered. The main problems faced by developers of such systems are revealed: difficulties with the reuse of existing security technologies and the need to design technologies taking into account the life cycle of the protected software. Each implementation uses different methods to solve these problems. The main advantage of using confidential computing technologies is the processing of data in protected containers, thereby ensuring the confidentiality and integrity of sensitive information. Therefore, solutions of this type can be considered for implementation at the design stage of the architecture of computing systems in the future, allowing them to increase their performance by increasing the efficiency of using computing resources without compromising confidentiality.*

Novelty: *lies in analysis and systematization of solutions implementing the hardware environment of confidential computing. The main features characterizing modern systems of confidential computing, as well as problems arising in the process of developing such systems, are revealed. Significant advances in this area will increase the efficiency of computing by sharing computing resources without compromising privacy.*

Keywords: *cloud computing security, hardware trusted execution environment, remote attestation, security of data, information security.*

References

1. Arakelov G.G. Voprosy primeneniya prikladnoj gomomorfnoj kriptografii // Voprosy kiberbezopasnosti [Cybersecurity issues]. – 2019. – № 5(33). – pp. 70-74.
2. Khlyupin A. A., Saakyan A. O., Nissenbaum O. V. Analiz effektivnosti algoritmov shifrovaniya dlya bezopasnyh mnogostoronnih vychislenij // Matematicheskoe i informacionnoe modelirovanie [Mathematical and information modeling]. – 2023. – pp. 315-324.
3. Mutlu O., Kim J. S. Rowhammer: A retrospective // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2019. – T. 39. – №. 8. – C. 1555-1571.
4. Acosta G. The Role of Vmtheft and Hyperjacking in Virtualization: dissertation – Utica College, 2018.
5. Gross M. et al. Breaking trustzone memory isolation through malicious hardware on a modern fpga-soc //Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop. – 2019. – C. 3-12.
6. Markettos A. T. et al. Thunderclap: Exploring vulnerabilities in operating system IOMMU protection via DMA from untrustworthy peripherals. – 2019.
7. Won Y. S. et al. Practical cold boot attack on iot device-case study on raspberry pi //2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA). – IEEE, 2020. – C. 1-4.
8. Zimerman I., Nachmani E., Wolf L. Recovering AES Keys with a Deep Cold Boot Attack //International Conference on Machine Learning. – PMLR, 2021. – C. 12955-12966.
9. Sardar M. U., Fetzer C. Confidential computing and related technologies: a critical review //Cybersecurity. – 2023. – T. 6. – №. 1. – C. 1-7.
10. Vaswani K. et al. Confidential machine learning within graphcore ipus //arXiv preprint arXiv:2205.09005. – 2022.
11. Cheng P. C. et al. Intel TDX Demystified: A Top-Down Approach //arXiv preprint arXiv:2303.15540. – 2023.
12. Li X. et al. Design and verification of the arm confidential compute architecture //16th USENIX Symposium on Operating Systems Design and Implementation (OSDI 22). – 2022. – C. 465-484.
13. Bornträger C. et al. Secure your cloud workloads with IBM Secure Execution for Linux on IBM z15 and LinuxONE III //IBM Journal of Research and Development. – 2020. – T. 64. – №. 5/6. – C. 2: 1-2: 11.
14. Hunt G. D. H. et al. Confidential computing for OpenPOWER //Proceedings of the Sixteenth European Conference on Computer Systems. – 2021. – C. 294-310.
15. Sahita R. et al. CoVE: Towards Confidential Computing on RISC-V Platforms //Proceedings of the 20th ACM International Conference on Computing Frontiers. – 2023. – C. 315-321.

8 Bulat N. Zagartdinov, master's student at NRNU MEPhI, specialist of STC Vulkan, Moscow, Russia. E-mail: me@vaire.lt

9 Mikhail V. Polyakov, Senior Lecturer at BMSTU, Moscow, Russia. E-mail: m.polyakov@bmstu.ru

СПУТНИКОВЫЕ СИСТЕМЫ УПРАВЛЕНИЯ С ПРИМЕНЕНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА[1]

Ромашкина Н.П.[2]

Цель статьи: *выявить актуальные на текущем этапе возможности применения искусственного интеллекта в космической индустрии для выработки предложений по расширению потенциала использования искусственного интеллекта в освоении ближнего космоса, околоземной орбиты для обеспечения экономического, научно-технологического развития и безопасности России.*

Метод исследования: *анализ данных о применении искусственного интеллекта в космической индустрии, синтез и научное прогнозирование, экспертная оценка, фактологический анализ в рамках системного подхода, междисциплинарный подход.*

Полученный результат: *представлен анализ текущей космической обстановки и применения технологий искусственного интеллекта в космической сфере, в том числе, в системах управления искусственных спутников Земли и многоспутниковых группировок. Приведены ключевые факторы, определяющие целесообразность применения искусственного интеллекта, а также основные направления его использования в космической индустрии. Выявлены перспективные технологии искусственного интеллекта в космических робототехнических средствах, исследовании дальнего космоса, контроле, диагностике и управлении техническим состоянием спутников, управлении многоспутниковой группировкой, обработке спутниковых изображений. Сформулированы проблемы влияния состояния спутниковой группировки на уровень стратегической стабильности, национальной и международной безопасности; значения искусственного интеллекта для развития космических технологий; подготовки кадров для космической отрасли на основе междисциплинарного научного подхода. Доказывается, что количественные и качественные характеристики спутниковой группировки являются сегодня одним из важнейших показателей влияния и потенциала государства в мире.*

Практическая ценность: *выработаны предложения по расширению потенциала использования искусственного интеллекта в освоении ближнего космоса, околоземной орбиты для обеспечения экономического, научно-технологического развития и безопасности России.*

Ключевые слова: *космическая индустрия, космическая обстановка, искусственный спутник Земли (ИСЗ), искусственный интеллект, орбитальная группировка, спутниковая система управления, многоспутниковая группировка, космический потенциал России, междисциплинарный научный подход.*

DOI: 10.21681/2311-3456-2023-6-128-137

Введение

По данным Управления ООН по вопросам космического пространства (*United Nations Office for Outer Space Affairs (UNOOSA)*)[3], 1 ноября 2023 г. в космосе насчитывалось 16864 объекта искусственного происхождения

3 United Nations Office for Outer Space Affairs (UNOOSA) // https://www.unoosa.org/ (дата обращения 29.10.2023).

1 Статья опубликована в рамках проекта «Посткризисное мироустройство: вызовы и технологии, конкуренция и сотрудничество» по гранту Министерства науки и высшего образования РФ на проведение крупных научных проектов по приоритетным направлениям научно-технологического развития (Соглашение № 075-15-2020-783).

2 Ромашкина Наталия Петровна, кандидат политических наук, руководитель подразделения проблем информационной безопасности Национального исследовательского института мировой экономики и международных отношений им. Е.М. Примакова РАН, Москва, Россия. E-mail: Romachkinan@yandex.ru

(космических аппаратов, а также ступеней ракетоносителей, их частей и другого космического мусора)[4].

В период с 1 января по 1 ноября 2023 г. было запущено 2253 космических аппарата (КА)[5] (табл. 1). Только за октябрь 2023 г. на орбиты отправлены 115 искусственных спутников Земли (ИСЗ)[6], 112 из которых принадлежат США и 3 – Китаю.[7] Следовательно, риск столкновений между объектами в космосе будет возрастать [1, 2].

В спутниковой индустрии в топ-10 ведущих стран входят США, Китай, Россия, Великобритания, Япония, Индия, Франция, Канада, Германия и Люксембург[8] По данным ООН в настоящее время в космосе находится более 8000 ИСЗ, но многие из них неактивны. Среди активных на различных орбитах около 67% принадлежит США, около 9% принадлежит КНР, России – около 3%, 21% – всем другим странам (рис. 1), в число которых входит большое количество государств – союзников и партнеров США[9]. Таким образом, важнейшей характеристикой текущего этапа является существенная диспропорция в обладании странами искусственными спутниками Земли [3-6].

На рис. 1 также представлено функциональное распределение ИСЗ по классификации США. Именно в число коммерческих ИСЗ, которые составляют более 88%, входит масштабная группировка *Starlink* американской компании *SpaceX,* которая сегодня активно используется вооруженными силами Украины (ВСУ). Эти факты добавляют риски национальной и международной безопасности, а также снижают уровень стратегической стабильности [7-9].

Одним из инструментов снижения рисков сегодня является искусственный интеллект (ИИ) – область исследований, в рамках которой разрабатываются модели, системы и устройства, имитирующие интеллектуальную деятельность человека (восприятие различной информации и логическое мышление), а также практическое применение их результатов.

Таблица 1

Количество запущенных КА по странам (период с 01.01.2023 по 01.11.2023)[10]

№	Государство	Количество КА
1	Бразилия	2
2	Бельгия	1
3	Великобритания	138
4	Дания	2
5	Израиль	1
6	Индия	6
7	Индонезия	1
8	Иран	1
9	КНР	107
10	Люксембург	10
11	Малайзия	1
12	Объединенные Арабские Эмираты	2
13	Республика Корея	8
14	Россия	58
15	США	1823
16	Турция	4
17	Уругвай	6
18	Финляндия	3
19	ЮАР	1
20	Япония	6
21	Другие*	72

* Принадлежность государству не определена, получена Управлением ООН по вопросам космического пространства из других источников и не была официально передана Организации Объединенных Наций // https://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id=, (дата обращения 29.10.2023).

4 Космический объект – тело, которое находится в космическом пространстве. Различают естественные (звезды, планеты, астероиды, кометы и др.) и искусственные (КА, последние ступени РН и их части) космические объекты. В международном праве термин «космический объект» используется только для обозначения объектов искусственного происхождения, а естественные носят название небесных тел // https://dictionary.mil.ru/folder/123087/item/130225/, (дата обращения 15.08.2023).

5 Космический аппарат (КА) – общее название различных технических устройств, предназначенных для выполнения целевых задач в космосе. КА разделяют на две основные группы: околоземные орбитальные КА, движущиеся по геоцентрическим орбитам, не выходя за пределы сферы действия гравитационного поля Земли – искусственные спутники Земли и межпланетные КА // https://dictionary.mil.ru/folder/123087/item/130225/, (дата обращения 15.09.2023).

6 Искусственный спутник Земли (ИСЗ) – космический летательный аппарат (КА), совершающий свободный полёт по геоцентрическим орбитам вокруг Земли (не менее одного оборота) и выводятся на орбиту ракетами-носителями. В соответствии с международной договоренностью космический аппарат называется спутником, если он совершает не менее одного оборота вокруг Земли. При несоблюдении этого условия он считается ракетным зондом, проводящим измерения вдоль баллистической траектории, и не регистрируется как спутник // https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5270@morfDictionary, (дата обращения 23.09.2023).

7 Online Index of Objects Launched into Outer Space. United Nations Office for Outer Space Affairs (UNOOSA) // https://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id=, (дата обращения 29.10.2023).

8 How Many Satellites are Orbiting Around Earth in 2022 // https://www.geospatialworld.net/prime/business-and-industry-trends/how-many-satellites-orbiting-earth/, (дата обращения 23.07.2023).

9 UCS Satellite Database. Union of Concerned Scientists (UCS) // https://www.ucsusa.org/resources/satellite-database, (дата обращения 27.09.2023).

10 Таблица построена автором на основе: Online Index of Objects Launched into Outer Space. United Nations Office for Outer Space Affairs (UNOOSA) // https://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id= (дата обращения 29.10.2023).

Искусственный интеллект для космоса и в космосе

Технологии искусственного интеллекта в космической области к настоящему времени приобретают статус стратегических, поскольку потенциально способны оказывать огромное влияние на различные сферы деятельности человека. Логично прогнозировать рост такого влияния в дальнейшем.

Основные факторы, определяющие целесообразность применения технологий ИИ в космической сфере:

- потенциальное обеспечение решения прикладных задач с более высоким выходным качеством и оперативностью (по сравнению с традиционными технологиями) при необходимых вычислительных и других ресурсах;
- обеспечение более высокого уровня автономности КА и (или) орбитальной группировки, в том числе, в условиях существенной априорной неопределенности относительно условий их функционирования, без ущерба эффективности их целевого применения.

Основные направления применения ИИ в космической технике:

- робототехнические средства;
- исследование дальнего космоса и реализация дальних космических миссий;
- контроль, диагностика и управление техническим состоянием КА;
- бортовая обработка целевой информации;
- тематическая обработка спутниковых изображений;
- управление многоспутниковыми орбитальными группировками;
- интеллектуальные системы поддержки проектных решений;
- обработка больших массивов разнородной спутниковой информации;

Рассмотрим более подробно некоторые из них [10].

Робототехнические средства (РБС) уже являются традиционной областью применения ИИ. Применительно к космической технике можно выделить следующие основные направления применения РБС:

- орбитальное обслуживание КА (ремонт, заправка, сборка, увод с орбиты);
- космические зонды (по существу, они сами представляют собой автономные или полуавтономные РБС, способные в условиях априорной неопределенности относительно условий их функционирования самостоятельно принимать необходимые решения по осуществлению возложенных на них миссий);
- робототехнические линии сборки, обеспечивающие массовое серийное производство КА нового поколения в интересах создания многоспутниковых систем;
- автономное выполнение опасных работ, например, заправка ракеты-носителя.

Системы с поддержкой ИИ в робототехнике используются, чтобы упростить и ускорить процесс производства и улучшить его продуктивность, а также проводят регулярное оценивание эффективности операций, результаты которого помогают их оптимизировать. Используемые на сборочных конвейерах коллаборативные роботы – коботы[11] принимают на себя наиболее трудоёмкие и подверженные ошибкам операции. В настоящее время космические агентства и промышленность работают над технологией *human-robot collaboration (HCR)* – новый вид робототехники, основанный на взаимодействии человеческого интеллекта и робота уже внедряется в космической сфере. Крупные космические агентства проводят исследования и эксперименты и прогнозируют значительно более активное внедрение коботов уже в ближайшие годы [11].

ИИ используются в космических зондах, исследующих дальний космос. Так, специализированные алгоритмы обрабатывают огромные массивы данных, изучая характеристики других планет, сравнивая их с запрограммированными показателями потенциально пригодного для жизни космического объекта, чтобы определить вероятность обитаемости планеты. Кроме того, возрастает роль ИИ для принятия автономных решений, например, для изменения траектории движения или поиска образцов пород местности, а также для сортировки данных с целью выбора только полезной информации для передачи в центры мониторинга. ИИ также используют для навигации КА и марсоходов.[12]

Искусственный интеллект для спутников и спутниковых систем

Большое внимание в последние годы уделяется применению технологий ИИ в бортовых системах

11 Коллаборативные роботы или коботы – роботы нового поколения, которые разработаны специально для работы рядом и вместе с людьми. Это автоматические устройства, которые могут работать совместно с человеком для создания или производства различных продуктов. Как и промышленные роботы, коботы состоят из манипулятора и перепрограммируемого устройства управления, которое формирует управляющие воздействия, задающие требуемые движения исполнительных органов манипулятора. Применяются в решении задач, которые нельзя полностью автоматизировать.

12 AI Today Podcast #109: Live at Amazon Re: MARS – Interview with Tom Soderstrom, Jet Propulsion Laboratory (JPL) // https://www.aidatatoday.com/ai-today-podcast-107-live-at-amazon-remars-interview-with-tom-soderstrom-jet-propulsion-laboratory-jpl/, (дата обращения 23.07.2023).

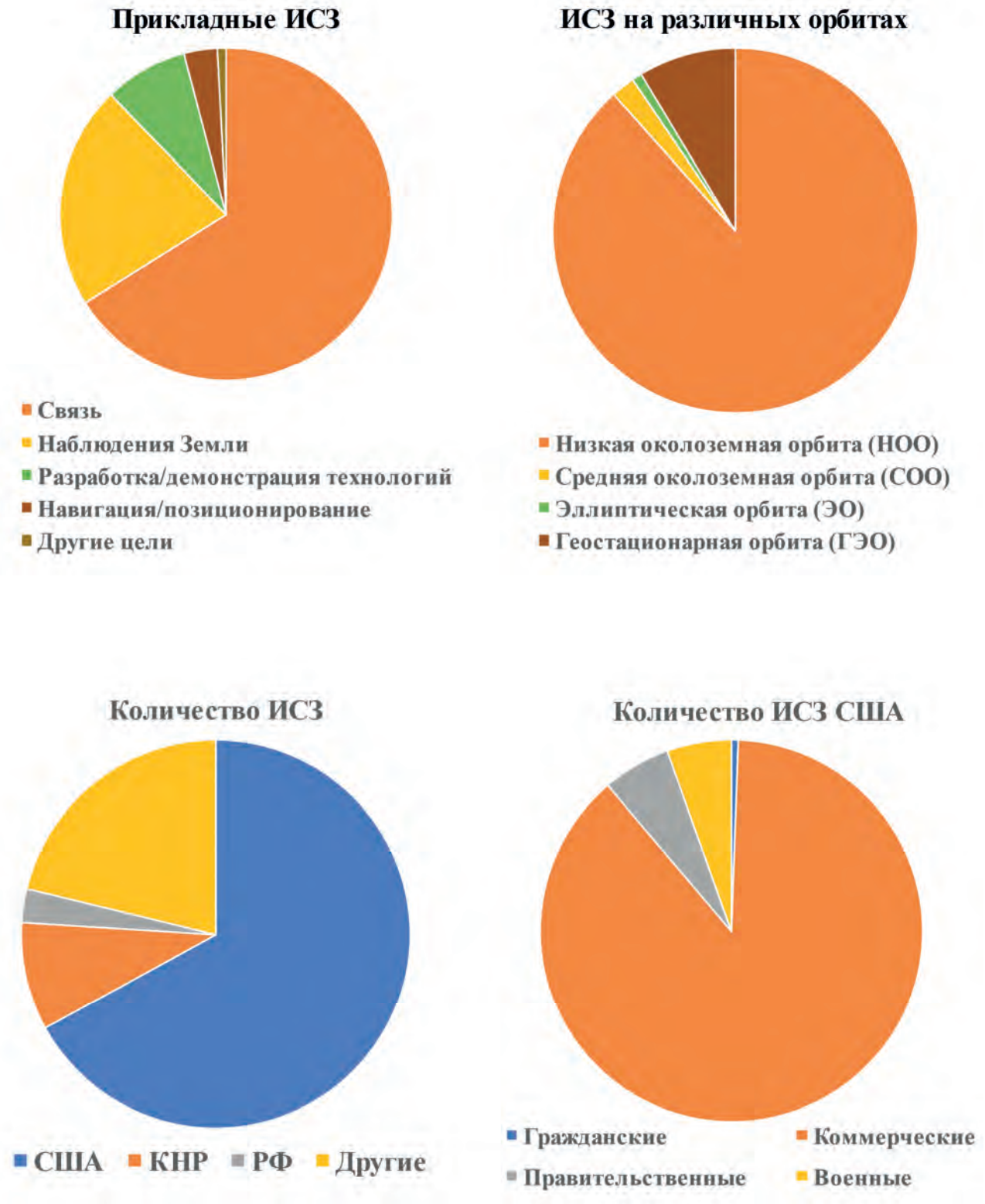

*Рис. 1. Данные об ИСЗ на орбитах в 2023 г.**

* Рисунок построен автором на основе данных: https://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id=; https://www.geospatialworld.net/prime/business-and-industry-trends/how-many-satellites-orbiting-earth/ (дата обращения 23.07.2023).

контроля, диагностики и управления техническим состоянием (СКДУ) ИСЗ. Это обосновано, так как решаемые ими задачи по уровню сложности (прежде всего в силу сложности формального описания самого объекта контроля и управления) могут быть отнесены к классу трудноформализуемых задач. Кроме того, интерес обусловлен потенциальной возможностью существенного повышения уровня автономности КА. В настоящее время на борту спутников осуществляется в основном контроль технического состояния, а диагностирование и управление техническим состоянием проводится наземными комплексами управления.

В ряде российских ИСЗ связи уже более двадцати лет применяются бортовые программные комплексы автономного контроля, диагностики и управления, построенные по принципу динамических экспертных систем. В КА *NASA* в качестве аналога российских СКДУ выступают системы управления живучестью *ISHM (Integrated Systems Health Management*), которые используют нейросетевые методы для решения задачи прогнозирования технического состояния аппарата.

Программы ИИ для контроля состояния ИСЗ постоянно совершенствуются, исходя из постоянного расширения списка как потенциально предсказуемых, так и маловероятных рисков: это огромное количество вариантов от рядовых неисправностей до столкновения с другими космическими объектами. Используются ИИ, непрерывно отслеживающие показатели большого количества сенсоров, которые могут не только оповещать людей о проблемах, но и самостоятельно их решать. Так, компания *SpaceX* уже установила на свои ИСЗ системы сенсоров и механизмов, которые могут отслеживать положение аппарата и корректировать его для исключения столкновения с другими объектами[13].

Поскольку контроль, диагностика и управление техническим состоянием бортовых систем ИСЗ должны осуществляться непрерывно, то, по мнению специалистов, среди всех технологий ИИ для решения этих задач наиболее целесообразно использовать так называемые динамические экспертные системы, которые способны в реальном масштабе времени по результатам измерения различных параметров бортовых систем ИСЗ и их обработки с использованием базы знаний (в общем случае динамически развивающейся) осуществлять управление их техническим состоянием.

Помимо контроля и управления спутниками, алгоритмы ИИ также необходимы для поддержания стабильной связи и преодоления практически любых проблем [12, 13]. На качество соединения может влиять близость других аппаратов, солнечный ветер, возмущения в атмосфере Земли и т.д. ИИ на борту постоянно определяет мощность и частоты, необходимые для передачи данных на Землю или на другие ИСЗ.

Тематическая обработка спутниковых изображений сегодня является одной из ставших уже традиционными областей применения технологий ИИ, позволяющим улучшить качество съемки поверхности Земли и других объектов. Спутники и космические телескопы каждую минуту генерируют миллионы снимков, ежедневно обрабатываются сотни терабайтов данных для передачи на Землю информации о наземных объектах, погодных условиях, состоянии лесов и морей, формирования актуальных онлайн-карт и т. д. Спутниковые изображения используются сегодня практически во всех отраслях деятельности – геологии и гидрологии, лесоводстве, охране окружающей среды, сельском хозяйстве, планировке территорий, в образовательных, разведывательных и военных целях.

Наибольшее распространенными в этой области стали нейросетевые технологии, которые получили интенсивное развитие после появления впечатляющих результатов их применения в области обработки изображений с применением так называемых методов глубокого обучения, например, сверхточные нейронные сети [14-16]. В настоящее время нейросетевые методы обработки спутниковых изображений реализованы в ряде различных программных инструментов, например, *ENVI, ScanEx Image Processor, ArcSDM* (модуль в составе *ArcView*) и др., которые достаточно активно используются на практике.

Искусственный интеллект в наземных центрах управления спутниками

В настоящее время управление спутниками осуществляется удаленно с наземных центров, где оператор может одновременно контролировать и вмешиваться в работу каждого отдельного спутника или группы ИСЗ, установленной в многоспутниковых системах, когда оператор вручную выбирает данные из настроек подсистем каждого спутника в группировке и переключается между различными связанными интерфейсами. Приоритеты вмешательства должны оце-

13 Passant Rabie. SpaceX Starlink Satellites Have to Dodge Objects in Orbit Nearly 140 Times Every Day, July 10, 2023, // https://gizmodo.com/spacex-starlink-satellites-dodge-137-objects-daily-1850616506, (дата обращения 27.07.2023).

ниваться оператором с учетом потенциальных последствий в случае непринятия корректирующих действий. Поэтому, независимо от уровня автономности отдельных спутников в многоспутниковых системах мониторинг деятельности требует управления все большим объемом информации в сложных сценариях эксплуатации. ИИ «предлагает» спутник, в работу которого должен вмешаться оператор, а также тип вмешательства, которое должно быть реализовано в соответствии с анализом данных в реальном времени и конкретными условиями и потребностями. Таким образом, это может снизить неопределенность и сложность информации, которой нужно управлять, а также определить приоритетность данных, подлежащих обработке, что, в итоге, сделает процесс принятия решений более эффективным.

Так, входящий в госкорпорацию «Роскосмос» холдинг «Российские космические системы» (РКС) разрабатывает саморегулируемую технологию управления многоспутниковыми орбитальными группировками с элементами ИИ и минимальным участием человека, которая позволит в будущем автоматизировать управление спутниковыми группировками из тысяч КА. Особенностью новой технологии является переход от применяемого сегодня точечного управления отдельными КА к управлению системным эффектом всей орбитальной группировки. Специалисты РКС используют методы согласованной самоорганизации (гомеостаза), который позволит эффективно управлять орбитальной структурой, ее численностью, ресурсами системы, сетью передачи данных и орбитальной вычислительной сетью. При существующей сегодня в России космической группировке, состоящей из более чем 150 спутников, наземный автоматизированный комплекс ежесуточно проводит до 2 тысяч сеансов управления.[14] Применяемая до этого традиционная технология, предполагающая обслуживание каждого КА в отдельности, отслеживая его работоспособность и орбитальную позицию, парируя отклонения или угрозы, имеет свои лимиты: дальнейший рост группировки с учетом ограничений по наращиванию ресурсов управления создают вероятность коллапса. Новая же саморегулируемая технология с ИИ позволит реализовать отечественные проекты многоспутниковых мультисервисных орбитальных группировок численностью от нескольких сотен до тысяч КА для обеспечения навигации, связи, дистанционного зондирования Земли и других функций.

Для новой системы управления разработчики предлагают иерархическую структуру. На верхних ее уровнях будут вводиться новые задачи управления в соответствии с системным и целевым эффектами. Система управления самостоятельно определит КА для формирования орбитальных структур для реализации различных целевых эффектов — проведения космической съемки поверхности, передачи информации или навигационного сигнала и др. Для этого она будет оценивать орбитальные позиции каждого спутника, их техническое состояние, наличие энергоресурса и запасы рабочего тела. Для дальнейшего увеличения возможностей саморегулируемой системы для многоспутниковых орбитальных группировок предполагается использовать технологию GRID-систем путем создания глобального «виртуального суперкомпьютера» — объединения в единую сеть вычислительных мощностей автоматизированных систем управления и самих космических аппаратов.

Человек для космического искусственного интеллекта

Помимо алгоритмов анализа данных ИСЗ и определения приоритетов, для интеграции ИИ в процессы управления спутниками необходимы интуитивно понятные и «легкие для чтения» интерфейсы. Это задача, которая требует активного включения человеческого фактора. Основная цель интеллектуальных интерфейсов – улучшить взаимодействие пользователя с машиной и, следовательно, повысить производительность оператора. В этой области исследования сосредоточены на так называемых адаптивных интерфейсах, которые предназначены для адаптации к когнитивной структуре пользователя (т.е. его образу мышления), его психическому и эмоциональному состоянию. Для приложений с небольшим количеством данных и сценариев управления разработка адаптивных интерфейсов относительно проста. Но если сложность возрастает, как в случае управления несколькими спутниками, объем информации также увеличивается. Таким образом, интерфейсы должны быть способны представлять все эти данные пользователям в понятной форме, чтобы избежать стрессовой нагрузки и снижения внимания человека. При этом создание адаптивных интерфейсов связаны с целой группой возникающих при взаимодействии человека с элементами системы проблем, решение которых необходимо для удобства человека и производительности самой системы. В

14 Перспективная технология управления многоспутниковой орбитальной группировкой // https://www.roscosmos.ru/29579/, (дата обращения 23.07.2023).

частности, это проблема рисков лишения оператора возможности прогнозировать поведение системы в определенных условиях при воздействии ИИ, в том числе, в случае необходимости управления несколькими операторами, каждый из которых обладает естественными когнитивными отличиями. Следовательно, разработка и реализация адаптивной автоматизации представляют собой сложную задачу для исследований, но эти инновационные интерфейсы имеют много преимуществ, а их значение в космической индустрии будет ускоренно возрастать уже в ближайшей перспективе.

Таким образом, мы выходим на ключевую проблему в области космонавтики, а именно на вопросы подготовки кадров – учёных, конструкторов, инженеров, специалистов среднего звена для космической отрасли. Максимально актуальны сегодня конкурентные решения, направленные на совершенствование всех уровней образования, в том числе, с учётом появления принципиально новых профессий и технологических направлений. Необходима активизация деятельности научного и экспертного сообщества, направленной на решение проблемы междисциплинарной подготовки специалистов космической индустрии с привлечением результатов из различных наук и научных направлений (кроме обязательных точных наук, в частности, это максимально широкое развитие знаний и навыков в различных областях программирования (в том числе, ИИ), политологии, психологии, международных отношений и др.).

Заключение

Представленный в статье анализ космической обстановки, российских и иностранных разработок в сфере применения ИИ в космической сфере позволяет сделать вывод о важной роли ИИ в развитии современных космических технологий, влиянии состояния спутниковой группировки на уровень стратегической стабильности, национальной и международной безопасности, что доказывает значимость количественных и качественных характеристик спутниковой группировки в качестве одного из важнейших показателей авторитета и потенциала государства в мире.

Для обеспечения экономического, научно-технологического развития и безопасности России целесообразно:

- расширить потенциал использования ближнего космоса, околоземной орбиты на основе российских и совместных международных разработок;
- совершенствовать механизмы обеспечения безопасности КА;
- увеличить количественный и качественный потенциал спутниковой группировки РФ, обеспечить создание и эксплуатацию российских многоспутниковых группировок;
- использовать новейшие технологии, в том числе, ИИ для обеспечения безопасной космической обстановки как совокупности космических объектов, факторов и условий космического пространства, влияющих на подготовку, ход и исход операций и процессов в космическом пространстве;
- использовать и развивать возможности ИИ для расширения доступности ключевых космических сервисов и транспортно-логистических коридоров, в том числе Северного морского пути;
- расширить применение космических услуг, в том числе, с использованием ИИ для развития потенциала перспективных секторов экономики;
- расширить применение ИИ для обеспечения безопасности критической военной технологии, направленной на решение принципиально новых военно-технических задач;
- совершенствовать процессы обеспечения благоприятных условий для недопущения завоевания противником превосходства в стратегической космической зоне, для чего необходим комплекс мероприятий, проводимых в космическом пространстве и на территории России, в том числе, новых проектов в сфере ИИ;
- обеспечить условия для разработки инновационного национального российского проекта в области спутниковых технологий с привлечением внебюджетных средств в космическую сферу[15];
- разработать механизмы использования ИИ для решения задач, поставленных Президентом РФ В.В. Путиным на Совещании по вопросам развития космической отрасли от 26 октября 2023 г.:
- налаживание серийного производства космических аппаратов, переход к конвейерной сборке;
- радикальное снижение стоимости доставки КА на околоземную орбиту, создание необходимой инфраструктуры для массовых запусков спутни-

15 Совещание по вопросам развития космической отрасли // http://www.kremlin.ru/events/president/news/72606, (дата обращения 26.10.2023).

ков, включая малые КА, и обеспечить доступ к ней для частных технологических компаний;
— развитие экспорта российских космических продуктов и услуг;
— при подготовке и развитии кадрового потенциала в сфере космической индустрии применять междисциплинарный научный подход, включающий возможность взаимодействия двух или более научных дисциплин и выявление новых областей знания, которые не исследуются существующими дисциплинами;
— для обеспечения безопасности и устойчивости глобальной информационной инфраструктуры расширить международное сотрудничество в сфере ИИ, в первую очередь, в рамках СНГ, Евразэс, ШОС, БРИКС и ОДКБ.

Литература

1. Datta A. How many satellites orbit Earth and why space traffic management is crucial, 08.23.2020. // https://www.geospatialworld.net/blogs/how-many-satellites-orbit-earth-and-why-space-traffic-management-is-crucial/, (дата обращения 23.08.2023).
2. Artificial Intelligence for satellite management: the HMI challenge / Redazione, 28.03.2023. // https://dblue.it/en/artificial-intelligence-for-satellite-management-the-hmi-challenge/, (дата обращения 15.09.2023).
3. Ромашкина Н.П. Космос как часть глобального информационного пространства в период военных действий // Вопросы кибербезопасности. 2022. № 6 (52). С. 100-111, DOI 10.21681/2311-3456-2022-6-100-111.
4. Ромашкина Н.П. Космос как сфера конфронтации: спутники США в новых реалиях // Информационные войны. 2023. № 2 (66). С. 16-24.
5. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Information Technologies and International Security : [electronic resource]. – Moscow : IMEMO, 2023. – 111 p. – ISBN 978-5-9535-0613-7. – DOI 10.20542/978-5-9535-0613-7. // https://www.imemo.ru/publications/info/information-technologies-and-international-security.
6. Ромашкина Н.П. Международно-правовой режим контроля над кибероружием в будущем миропорядке: угрозы и перспективы // Дипломатическая служба. 2023. № 2. С. 150-161. DOI 10.33920/vne-01-2302-07. // https://www.imemo.ru/files/File/ru/publ/2023/DipSluzhba-022023-Romashkina.pdf, (дата обращения 23.09.2023).
7. Марков А.С., Шеремет И.А. Безопасность программного обеспечения в контексте стратегической стабильности // Вестник академии военных наук. 2019. № 2 (67). С. 82–90.
8. Ромашкина Н. П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. №. 1 (29). С. 2–9, DOI: 10.21681/2311–3456-2019-1-2-9.
9. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. – 98 с. DOI: 10.20542/978-5-9535-0581-9. // https://www.imemo.ru/publications/info/romashkina-np-markov-as-stefanovich-dv-mezhdunarodnaya-bezopasnosty-strategicheskaya-stabilynosty-i-informatsionnie-tehnologii-otv-red-av-zagorskiy-np-romashkina-m-imemo-ran-2020-98-s, (дата обращения 23.07.2023).
10. Искусственный интеллект в космической технике: состояние, перспективы развития // Ракетно-космическое приборостроение и информационные системы, 2019, том 6, выпуск 1, с. 65–75. DOI 10.30894/issn2409-0239.2019.6.1.65.75.
11. Frąckiewicz M., The Role of Collaborative Robots (Cobots) in Space Exploration, May 15, 2023, // https://ts2.space/ru/%D1%80%D0%BE%D0%BB%D1%8C-%D0%BA%D0%BE%D0%BB%D0%BB%D0%B0%D0%B1%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D1%8B%D1%85-%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%BE%D0%B2-%D0%BA%D0%BE%D0%B1%D0%BE%D1%82%D0%BE-4/, (дата обращения 23.09.2023).
12. Marrero L. M., Merlano-Duncan J. C., Querol J., Kumar S., Krivochiza J., Sharma S. K., Chatzinotas S., Camps A., and Ottersten B. Architectures and Synchronization Techniques for DistributedSatellite Systems: A Survey, IEEE Access, vol. 10, pp. 45 375–45 409,2022.
13. Homssi B. A., Dakic K., Wang K., Alpcan T., Allen B., Kan-deepan S., Al-Hourani A., and Saad W. Artificial Intelligence Tech-niques for Next-Generation Mega Satellite Networks. arXiv preprintarXiv:2207.00414, 2022.
14. Николенко С.И., Кадурин А. А., Архангельская Е. О. Глубокое обучение. СПб: Питер, 2018. 480 с.
15. Городецкий В. И. Самоорганизующиеся сети агентов — базовая модель группового и кооперативного поведения автономных объектов // Сборник трудов научно-технической конференции Минобороны РФ «Искусственный интеллект: проблемы и пути решения», 14–15 марта 2018. С. 9–15.
16. Лихтенштейн В. Е., Конявский В. А., Росс Г. В., Лось В. П. Мультиагентные системы. Самоорганизация и развитие. М.: Финансы и статистика, 2018. 264 с.

SATELLITE CONTROL SYSTEMS USING ARTIFICIAL INTELLIGENCE[16]

Romashkina N.P.[17]

Purpose: *To identify the current opportunities for the use of artificial intelligence in the space industry based and to develop proposals that can expand the potential of using artificial intelligence in the exploration of near space, near-Earth orbit to ensure economic, scientific and technological development and security of Russia.*

Research method: *analysis of open data sources on the use of artificial intelligence in the space industry, synthesis and scientific forecasting, expert assessment, factological analysis within the framework of a systems approach, interdisciplinary approach.*

Result: *the article presents an analysis of the current space situation and the use of artificial intelligence technologies in the space sector, including in control systems of artificial Earth satellites and multi-satellite constellations. The article presents the key factors that determine the feasibility of using artificial intelligence, as well as the main directions of its use in the space industry. The article identifies promising artificial intelligence technologies in space robotics, deep space exploration, monitoring, diagnostics and management of the technical condition of satellites, management of a multi-satellite constellation, and processing of satellite images. The author poses the problems of the influence of the state of the satellite constellation on the level of strategic stability, national and international security; the importance of artificial intelligence for the development of space technologies; training personnel for the space industry based on an interdisciplinary scientific approach. The article proves that the quantitative and qualitative characteristics of a satellite constellation are today one of the most important indicators of the influence and potential of a state in the world.*

Practical value: *Proposals have been developed to expand the potential of using artificial intelligence in the exploration of near space, near-Earth orbit to ensure the economic, scientific and technological development and security of Russia.*

Keywords: *space industry, space situation, artificial Earth satellite (AES), artificial intelligence (AI), orbital constellation, satellite control system, multi-satellite constellation, Russian space potential, interdisciplinary scientific approach.*

References

1. Datta A. How many satellites orbit Earth and why space traffic management is crucial, 08.23.2020. // https://www.geospatialworld.net/blogs/how-many-satellites-orbit-earth-and-why-space-traffic-management-is-crucial/, (accessed 23.08.2023).
2. Artificial Intelligence for satellite management: the HMI challenge / Redazione, 28.03.2023. // https://dblue.it/en/artificial-intelligence-for-satellite-management-the-hmi-challenge/, (accessed 15.09.2023).
3. Romashkina N.P. Kosmos kak chast' global'nogo informacionnogo prostranstva v period voennyh dejstvij // Voprosy kiberbezopasnosti. 2022. № 6 (52). S. 100-111, DOI 10.21681/2311-3456-2022-6-100-111.
4. Romashkina N.P. Kosmos kak sfera konfrontacii: sputniki SSHA v novyh realiyah // Informacionnye vojny. 2023. № 2 (66). S. 16-24.
5. Romashkina N.P., Markov A.S., Stefanovich D.V. Information Technologies and International Security : [electronic resource]. – Moscow: IMEMO, 2023. – 111 p. – ISBN 978-5-9535-0613-7. – DOI 10.20542/978-5-9535-0613-7. // https://www.imemo.ru/publications/info/information-technologies-and-international-security.
6. Romashkina N.P. Mezhdunarodno-pravovoj rezhim kontrolya nad kiberoruzhiem v budushchem miroporyadke: ugrozy i perspektivy // Diplomaticheskaya sluzhba. 2023. № 2. S. 150-161. DOI 10.33920/vne-01-2302-07. // https://www.imemo.ru/files/File/ru/publ/2023/DipSluzhba-022023-Romashkina.pdf, (accessed 23.09.2023).
7. Markov A.S., SHeremet I.A. Bezopasnost' programmnogo obespecheniya v kontekste strategicheskoj stabil'nosti // Vestnik akademii voennyh nauk. 2019. № 2 (67). P. 82–90.
8. Romashkina N. P. Global'nye voenno-politicheskie problemy mezhdunarodnoj informacionnoj bezopasnosti: tendencii, ugrozy, perspektivy // Voprosy kiberbezopasnosti. 2019. №. 1 (29). S. 2–9, DOI: 10.21681/2311–3456-2019-1-2-9.

16 The article was prepared within the project «Post-crisis world order: challenges and technologies, competition and cooperation» supported by the grant from Ministry of Science and Higher Education of the Russian Federation program for research projects in priority areas of scientific and technological development (Agreement № 075-15-2020-783).

17 Nataliya P. Romashkina, Ph.D. (Political Science), Head of the Informational Security Problems Group of the Primakov National Research Institute of World Economy and International Relations (IMEMO) of the Russian Academy of Sciences, Moscow, Russia. E-mail: Romachkinan@yandex.ru.

9. Romashkina N.P., Markov A.S., Stefanovich D.V. Mezhdunarodnaya bezopasnost', strategicheskaya stabil'nost' i informacionnye tekhnologii / otv. red. A.V. Zagorskij, N.P. Romashkina. – M.: IMEMO RAN, 2020. – 98 s. DOI: 10.20542/978-5-9535-0581-9. // https://www.imemo.ru/publications/info/romashkina-np-markov-as-stefanovich-dv-mezhdunarodnaya-bezopasnosty-strategicheskaya-stabilynosty-i-informatsionnie-tehnologii-otv-red-av-zagorskiy-np-romashkina-m-imemo-ran-2020-98-s, (accessed 23.07.2023).
10. Iskusstvennyj intellekt v kosmicheskoj tekhnike: sostoyanie, perspektivy razvitiya // Raketno-kosmicheskoe priborostroenie i informacionnye sistemy, 2019, tom 6, vypusk 1, c. 65–75. DOI 10.30894/issn2409-0239.2019.6.1.65.75.
11. Frąckiewicz M., The Role of Collaborative Robots (Cobots) in Space Exploration, May 15, 2023, https://ts2.space/ru/роль-коллаборативных-роботов-кобото-4 (accessed 23.09.2023).
12. Marrero L. M., Merlano-Duncan J. C., Querol J., Kumar S., Krivochiza J., Sharma S. K., Chatzinotas S., Camps A., and Ottersten B. Architectures and Synchronization Techniques for DistributedSatellite Systems: A Survey, IEEE Access, vol. 10, pp. 45 375–45 409,2022.
13. Homssi B. A., Dakic K., Wang K., Alpcan T., Allen B., Kan-deepan S., Al-Hourani A., and Saad W. Artificial Intelligence Tech-niques for Next-Generation Mega Satellite Networks. arXiv preprintarXiv:2207.00414, 2022.
14. Nikolenko S.I., Kadurin A. A., Arhangel'skaya E. O. Glubokoe obuchenie. SPb: Piter, 2018. 480 s.
15. Gorodeckij V. I. Samoorganizuyushchiesya seti agentov — bazovaya model' gruppovogo i kooperativnogo povedeniya avtonomnyh ob"ektov // Sbornik trudov nauchno-tekhnicheskoj konferencii Minoborony RF «Iskusstvennyj intellekt: problemy i puti resheniya», 14–15 marta 2018. S. 9–15.
16. Lihtenshtejn V. E., Konyavskij V. A., Ross G. V., Los' V. P. Mul'tiagentnye sistemy. Samoorganizaciya i razvitie. M.: Finansy i statistika, 2018. 264 s.

CYBERSECURITY ISSUES

SCIENTIFIC PEER-REVIEWED JOURNAL

2023, № 6 (58)

Cybersecurity Issues is a research periodical scientific and practical publication specializing in information security. Published six times a year

WWW.CYBERRUS.COM

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

7-8 ФЕВРАЛЯ 2024 | ЦИФРОВОЕ ДЕЛОВОЕ ПРОСТРАНСТВО

БОЛЬШОЙ НАЦИОНАЛЬНЫЙ ФОРУМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИНФОФОРУМ-2024

www.infoforum.ru/infoforum-2024

7 декабря 2023

«ЦИФРОВЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ В СФЕРЕ ТРАНСПОРТА И ОБРАЗОВАНИЯ»

II НАЦИОНАЛЬНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Основными задачами конференции являются:

- Представление научных достижений и исследований в сфере цифровизации транспорта и образования;
- Определение приоритетов научно-технического развития образовательного потенциала в области цифровых технологий и информационной безопасности;
- Оценка стратегии развития научно-технического и образовательного потенциала в условиях импортозамещения;
- Формирование рекомендаций по развитию образовательных программ подготовки специалистов в области информационных технологий и информационной безопасности транспортной отрасли.

www.imiit.ru/events/cifr-texn-2023

8 ноября 2023

МТУСИ

III Всероссийская научно-практическая конференция

ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направления:

- Криптографические алгоритмы и анализ сетевого трафика;
- Организационно-правовые и инженерно-технические методы защиты инфокоммуникационных систем;
- Проблемы цифрового суверенитета и программно-аппаратные средства защиты инфокоммуникационных систем;
- Кибербезопасность.

г. Москва, ул. Авиамоторная, д. 8, стр. 39. Конгресс-центр МТУСИ

30 ноября 2023

Конференция по информационной безопасности, посвящённая памяти Заслуженного деятеля науки и техники РФ Ю.Г. Ростовцева

Целями конференции являются:

– обмен информацией о новых научных разработках в области обеспечения информационной безопасности;
– совершенствование учебно-воспитательного процесса кадров в области информационной безопасности.

Организатор ВКА им. А.Ф.Можайского.
г. Санк-Петербург, РАНХиГС.

CYBERSECURITY ISSUES
VOPROSY KIBERBEZOPASNOSTI

№6 2023

DOI: 10.21681/2311-3456

- Risk-oriented Approach
- Intrusion Detection
- International Security

www.cyberrus.com
editor@cyberrus.com