ПОДСИСТЕМА ПРЕДУПРЕЖДЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ: АНАЛИЗ ФУНКЦИОНИРОВАНИЯ И РЕАЛИЗАЦИИ

Котенко И.В.[1], Саенко И.Б.[2], Захарченко Р.И.[3], Величко Д.В.[4]

Цель статьи: *проведение системного анализа требований к подсистеме предупреждения компьютерных атак на объекты критической информационной инфраструктуры с целью обоснования направлений дальнейшего совершенствования научно-методического аппарата для полноценного функционирования подсистемы предупреждения компьютерных атак.*

Метод исследования: *теоретический и системный анализ требований нормативно-правовых актов, научных публикаций, технологий защиты и средств их реализации в ведомственных системах обнаружения, предупреждения и ликвидации последствий компьютерных атак.*

Полученный результат: *проведено обоснование необходимости построения механизмов предупреждения компьютерных атак на объекты критической информационной инфраструктуры и требований к подсистеме предупреждения компьютерных атак, предложен подход к предупреждению компьютерных атак на этапах разведки злоумышленником объектов критической информационной инфраструктуры, основанный на внедрении механизма корреляции событий безопасности с автоматической адаптацией к анализируемой информационной инфраструктуре и выполняемым ею функциям в текущий момент времени и детальной спецификацией правил корреляции.*

Область применения предложенного подхода: *подсистема предупреждения компьютерных атак ведомственных систем обнаружения, предупреждения и ликвидации последствий компьютерных атак, которая должна заблаговременно выявлять и предупреждать попытки проведения компьютерных атак на объекты критической информационной инфраструктуры.*

Научная новизна *заключается в проведенном всестороннем анализе необходимости построения механизмов предупреждения компьютерных атак на объекты критической информационной инфраструктуры, анализе требований к подсистеме предупреждения компьютерных атак, ее функций и средств реализации. Показано, что функции предупреждения компьютерных атак в отечественных технических решениях реализованы не в полном объеме, и что существует подмена понятия «подсистема предупреждения компьютерных атак» понятием «контрольно-технические мероприятия». Обосновано, что для реализации функций предупреждения компьютерных атак имеется технологический задел в виде готовой технологии на базе технологии построения SIEM-систем. Показано, что существует необходимость доработки научно-методического аппарата реализации функций предупреждения компьютерных атак на базе методов искусственного интеллекта и технологий больших данных.*

Вклад: *Котенко И.В. – анализ функциональных возможностей подсистемы предупреждения компьютерных атак, постановка задачи и предложения по развитию функциональности подсистемы предупреждения компьютерных атак на объекты критической информационной инфраструктуры; Саенко И.Б. – анализ подсистемы предупреждения компьютерных атак в общем контексте теории информационной безопасности, обосно-*

1 Котенко Игорь Витальевич, доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: ivkote@comsec.spb.ru

2 Саенко Игорь Борисович, доктор технических наук, ведущий научный сотрудник, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: ibsaen@comsec.spb.ru

3 Захарченко Роман Иванович, доктор технических наук, начальник кафедры, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: romanzakharchenko@yandex.ru

4 Величко Дмитрий Владимирович, адъюнкт, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: redbull1666@mail.com

DOI:10.21681/2311-3456-2023-1-13-27

вание реализации функций предупреждения компьютерных на базе технологии построения SIEM-систем и больших данных; Захарченко Р.И. – анализ технических решений, обеспечивающих реализацию подсистемы предупреждения компьютерных атак, Величко Д.В. – подход к выявлению компьютерных атак на этапах разведки злоумышленником объектов критической информационной инфраструктуры. Все авторы участвовали в написании статьи.

Ключевые слова: *кибербезопасность, компьютерная атака, информационно-телекоммуникационные системы и сети, информационно-техническое воздействие, системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.*

DOI:10.21681/2311-3456-2023-1-13-27

1. Введение

Современный этап развития информационных и телекоммуникационных технологий, обеспечивающий высокий уровень автоматизации в ведомственных системах управления в целом и в системах передачи данных в частности, а также объединение разнотипных автоматизированных систем специального назначения между собой в единое информационное пространство посредством информационно-телекоммуникационной сети общего пользования, приводят к их доступности из киберпространства для проведения информационно-технических воздействий.

Особенно актуальным является создание единого информационного пространства для министерств и ведомств, осуществляющих свою деятельность в области обороны государства, здравоохранения, образования и т.д., а также для государственных корпораций страны. Под единым информационным пространством понимается объединение баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей [1].

Под киберпространством будем понимать масштабируемую неоднородную искусственную систему с сетецентрическим управлением, обеспечивающую процессы генерации, передачи, хранения, обработки и потребления информации в интересах разнородных, в том числе антагонистических систем управления, в которой свойства (характеристики) элементов зависят от собственных характеристик, объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей [2].

Под информационно-техническим воздействием понимается целенаправленное программно-аппаратное и/или программное воздействие, приводящее к нарушению устойчивости функционирования информационно-управляющей системы [3]. Наиболее распространенными средствами информационно-технических воздействий в настоящее время являются [4]: удаленные сетевые атаки; вирусы; программные закладки; аппаратные закладки; нейтрализаторы тестовых программ; ложные объекты информационного пространства; средства компьютерной разведки; средства моделирования боевых и военных действий; средства технической разведки; средства разведки по открытым каналам.

В соответствии с ГОСТ Р 51275-2006 под сетевой атакой будем понимать компьютерную атаку с использованием протоколов межсетевого взаимодействия. Возможными результатами воздействия сетевых атак на компьютерные сети и системы являются несанкционированный доступ, блокирование управляющей информации, внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации в автоматизированных системах контроля и управления, отказы и сбои в работе компьютерной сети, а также компрометация передаваемой или получаемой информации [5].

В соответствии с Указом Президента РФ от 15.01.2013 № 31с (ред. от 22.12.2017) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» защита от компьютерных атак и/или информационно-технических воздействий объектов информатизации различных автоматизированных систем специального назначения, информационно-телекоммуникационных сетей, ведомственных информационных систем является основополагающей в обеспечении национальной и информационной безопасности страны.

Процесс защиты этих систем обеспечивают ведомственные системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА) соответствующих федеральных органов исполнительной власти страны. Эти системы представляют собой технологии, технические, программные, лингвистические, организационные, правовые средства, включая сети и средства связи, средства сбора и анализа информации, поддержки принятия управленческих решений, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы соответствующих органов власти. Совокупность всех ведомственных систем обнаружения, предупреждения и ликвидации последствий компьютерных атак является одной их важнейших составляющих Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) страны. Порядок функционирования и реализации ГосСОПКА регламентируется руководящими документами, которые обязательны для исполнения всеми органами власти. Следовательно, общие принципы построения ведомственных систем обнаружения, предупреждения и ликвидации последствий компьютерных атак являются одинаковыми во всех ведомственных системах. В рамках данной статьи ограничимся рассмотрением этих систем для федеральных органов исполнительной власти (ФОИВ), а реализацию информационно-технических воздействий ограничим компьютерными атаками (КА).

Разработан ряд методических рекомендаций по созданию ведомственных и корпоративных центров ГосСОПКА, по обнаружению компьютерных атак на информационные ресурсы страны, по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации, по проведению мероприятий по оценке степени защищенности от компьютерных атак. Анализ требований, содержащихся в этих нормативно-правовых актах, научных публикаций по данной проблематике [6–14], а также применяемых в настоящее время концепций построения СОПКА [11, 15] показал, что в настоящее время основное внимание при развертывании таких систем уделяется подсистемам обнаружения и ликвидации последствий компьютерных атак. При этом вопросы построения, реализации и функционирования подсистемы предупреждения компьютерных атак остаются недостаточно раскрытыми. Рассмотрение результатов анализа подсистемы предупреждения компьютерных атак является целью настоящей работы.

2. Анализ функциональных возможностей подсистемы предупреждения компьютерных атак

Под предупреждением компьютерных атак понимается комплекс превентивных мероприятий, направленных на снижение количества компьютерных инцидентов и повышение уровня защищенности информационных ресурсов [11]. Данные мероприятия должны проводиться в рамках подсистемы предупреждения компьютерных атак (ППКА), которая реализуется на основе технологий, а также технических, программных, лингвистических, правовых и организационных средств, включая сети и средства связи, средства сбора и анализа информации, поддержки принятия управленческих решений (ситуационные центры), предназначенные для предупреждения компьютерных атак на критическую информационную инфраструктуру (КИИ) и мониторинга уровня ее реальной защищенности [16].

Для определения места ППКА в СОПКА рассмотрим пример реализации так называемой «убийственной» цепочки – Cyber Kill Chain [17]. Cyber Kill Chain – это схематическое описание последовательных действий (этапов) нарушителя в виде взаимосвязанных звеньев цепи [18]. Иными словами, Cyber Kill Chain определяет пошаговый порядок действий злоумышленника, направленный на достижение поставленной им цели.

Процесс реализации компьютерных атак с декомпозицией этапов их проведения с выделением действий по преодолению уровней защиты СОПКА представлен на рис. 1. На рисунке отображены 3 этапа (цепочки) реализации атаки.

Как видно из рис. 1, ППКА должна выполнять свои функции на всех трех этапах осуществления компьютерных атак при проведении противником разведки объектов КИИ.

На рис. 2 показана роль ППКА в контексте функций сегмента СОПКА [19].

Раскроем каждую из возлагаемых на ППКА функций.

Инвентаризация информационных ресурсов заключается в сборе следующих сведений:

- ФИО, должности и контактные данные лиц, ответственных за функционирование информационного ресурса;
- доменные имена и сетевые адреса компонентов информационного ресурса (средств вычислительной техники, телекоммуникационного оборудования, виртуальных машин и т. п.) в соответствии с системой имен и сетевой адресацией информационного ресурса;
- доменные имена и сетевые адреса компонентов информационного ресурса, доступные из

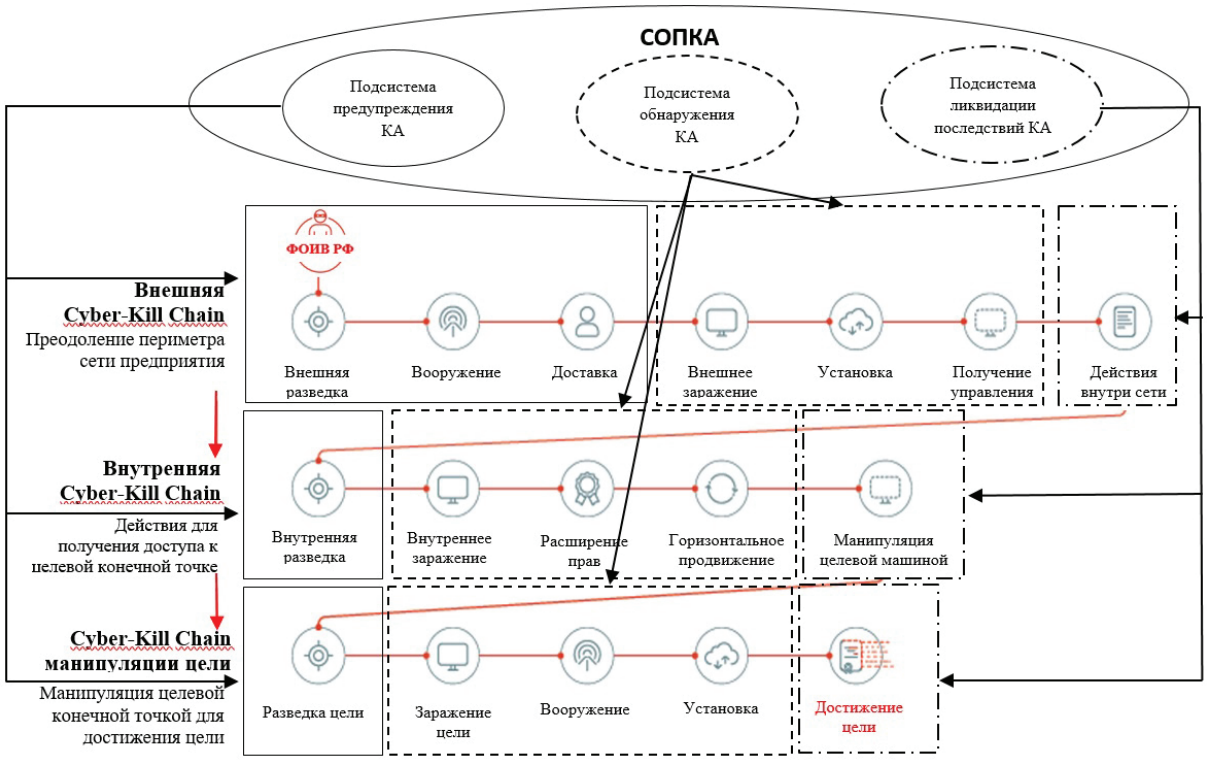

Рис. 1. Обобщенная схема реализации ППКА применительно к Cyber Kill Chain

Рис. 2. Роль ППКА в общем контексте функций сегмента СОПКА

сети Интернет, в соответствии с системой имен и сетевой адресацией сети Интернет, а также сведения о протоколах (включая параметры транспортного уровня взаимодействия), по которым разрешен доступ к этим компонентам;

— сведения о сегментации и топологии локальных вычислительных сетей, правилах маршрутизации и коммутации, настройках средств межсетевого экранирования;

— перечень программного обеспечения (прикладного и системного), установленного на каждом средстве вычислительной техники;

— параметры настройки программного и аппаратного обеспечения информационного ресур-

са, существенные с точки зрения обеспечения безопасности информации;
— параметры настройки средств обеспечения информационной безопасности.

Выявление уязвимостей информационных ресурсов включает в себя следующие способы:
— выявление известных уязвимостей сетевых служб, доступных для сетевого взаимодействия, с применением автоматизированных средств анализа защищенности (сетевого сканирования);
— выявление известных уязвимостей программного обеспечения информационных ресурсов путем анализа состава установленного программного обеспечения и обновлений безопасности с применением автоматизированных средств анализа защищенности (системного сканирования, исследования с использованием привилегированных учетных записей и/или программных агентов), а также других средств защиты информации;
— тестирование на проникновение в условиях, соответствующих условиям нарушителя, действующего со стороны сети Интернет и/или со стороны информационных ресурсов, внешних по отношению к зоне ответственности сегмента ГосСОПКА;
— тестирование на проникновение в условиях, соответствующих условиям нарушителя, действующего со стороны информационных ресурсов, входящих в зону ответственности сегмента ГосСОПКА;
— тестирование устойчивости к атакам типа «отказ в обслуживании»;
— контроль устранения ранее выявленных уязвимостей и недостатков;
— контроль выполнения требований безопасности информации, предъявляемых к контролируемой ИС;
— анализ настроек программного и аппаратного обеспечения ИС, а также средств защиты информации;
— анализ проектной, конструкторской и эксплуатационной документации ИС;
— оценка соответствия применяемых мер защиты требованиям безопасности информации, предъявляемым нормативными документами Российской Федерации и владельцев информационных ресурсов.

Анализ угроз информационной безопасности по результатам инвентаризации и выявления уязвимостей информационных ресурсов имплицирует уточнение следующих методических документов организации:
— описание компьютерных атак, актуальных для информационных ресурсов, находящихся в зоне ответственности сегмента ГосСОПКА;
— методические рекомендации по предупреждению, обнаружению и ликвидации последствий компьютерных атак;
— решающие правила средств обнаружения компьютерных атак;
— настройки средств обеспечения информационной безопасности;
— политики обеспечения информационной безопасности;
— нормативные правовые акты организации;
— дополнительные требования по обеспечению информационной безопасности для их включения в технические задания на создание новых, доработку и обслуживание существующих информационных ресурсов;
— правила корреляции событий, направленные на определение попыток реализации угроз, связанных с проведением компьютерных атак;
— инструкции для персонала по выявлению признаков проведения типовых компьютерных атак, порядку их обнаружения, действиям по ликвидации их последствий;
— инструкции по действиям пользователей информационных ресурсов в случае возникновения инцидентов, связанных с компьютерными атаками;
— требования к квалификации персонала и пользователей, необходимой для выполнения указанных выше инструкций.

Средства предупреждения компьютерных атак должны выполнять следующие функции:

1) сбор и обработка (добавление, просмотр и изменение) сведений об инфраструктуре контролируемых информационных ресурсов, а также справочной информации:
— об архитектуре и объектах контролируемых информационных ресурсов (сетевые адреса и имена, наименования и версии используемого ПО);
— о выполняющихся на объектах контролируемых ресурсов сетевых службах;
— об источниках событий информационной безопасности;
— о показателе доверия (репутации) сетевых адресов, доменных имен, серверов электронной почты, серверов доменных имен;
— о владельцах сетевых адресов, доменных имен,

серверов электронной почты, серверов доменных имен;
— о местоположении и географической принадлежности сетевых адресов;
— об известных уязвимостях используемого ПО;
— о компьютерных сетях, состоящих из управляемых с использованием вредоносного ПО средств вычислительной техники, включая сведения об их управляющих серверах;

2) сбор и обработка сведений об уязвимостях и недостатках в настройке ПО, используемого в контролируемых информационных ресурсах:

— сбор данных о дате и времени проведения исследования контролируемых информационных ресурсов;
— формирование перечня выявленных уязвимостей и недостатков в настройке используемого ПО (для каждого объекта контролируемого информационного ресурса);
— статистическая и аналитическая обработка полученной информации;

3) формирование рекомендаций по минимизации угроз безопасности информации, которые должны содержать перечень мер, направленных на устранение

Таблица 1

Пример типового паспорта угроз вредоносной программы

Элемент описания	Описание вредоносной программы
Наименование	Careto
Тип	Бэкдор, модульный
Дата обнаружения	2014
Краткое описание	ВП скрытно внедряется и предоставляет нарушителю удаленный доступ, выполняет различные команды, поступающие из сервера удаленного управления
Объект ВП	Государственные учреждения и коммерческие организации
Степень опасности	Высокая
Структура ВП	модуль установки; основной модуль; модуль сетевого взаимодействия с центром удаленного управления; функциональный модуль; модуль контроля исполнения функционального и сетевого модуля; модуль удаления; модуль сбора системной информации и аутентификационных данных (возможна загрузка дополнительных модулей из центра удаленного управления).
Основные функциональные возможности	— файл конфигурации и файл полезной нагрузки зашифрованы модифицированным алгоритмом RC4 (потоковый шифр, применяющийся, например, в протоколах SSL и TLS, алгоритмах обеспечения безопасности беспроводных сетей WEP и WPA); — закрепление в автозагрузке в качестве COM-объекта; — внедрение вредоносного кода в процессы explorer.exe, iexplore.exe, firefox.exe. chrome.exe; — перезапись кодовой секции системных библиотек; — безопасное закрытие обработчиков процесса работы модулей; — прием и передача данных шифруется алгоритмами AES и RSA; — запуск исполняемых файлов с определенными аргументами; — получение CAB-файла, извлечение из него файла и последующий запуск с определенными аргументами; — извлечение исполняемого модуля из CAB-файла и последующий запуск в памяти; — изменение конфигурационного файла, смена сервера удаленного управления; — сбор информации об информационно-телекоммуникационной сети и передача на сервер удаленного у правления; — полное удаление ВП из информационно-телекоммуникационной сети.

Элемент описания	Описание вредоносной программы
Индикаторы компрометации информационно-телекоммуникационной сети	**(Файлы, фрагмент)** %AppData%\Microsoft\objframe.dll|shmgr.dll|Shlink(32|64).dll **(Реестр, фрагмент)** [HKLM\Software\Classes\CLSID\{E6BB64BE-0618-4353-9193-0AFE606D6F0C}\InprocServer32] = «%System% browseui.dll» **(Сети, фрагмент)** http://202.75.58.153/cgi-bin/commcgi.cgi Поле User-Agent: Mozilla/4.0 (compatible: MSIE 4.01: Windows NT)
Способ обнаружения	**Средства антивирусной зашиты (фрагмент)** Kaspersky: Trojan.Win32|Win64.Careto.*
Возможные меры по устранению	— переустановка ОС и форматирование носителей информации; — проведение ручной проверки индикаторов компрометации информационно-телекоммуникационной сети (элементы автозагрузки, сетевое взаимодействие, активность файловой системы, анализ лог-файлов ОС); — обновление средств антивирусной защиты и проведение полной проверки информационно-телекоммуникационной сети.
Сведения о ВП	https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20133638/unveilingthemask_v1.0.pdf

уязвимостей и недостатков в настройке ПО, используемого в контролируемых информационных ресурсах;

4) учет угроз безопасности информации, при осуществлении которого средства предупреждения должны обеспечивать:

— создание и изменение записи, содержащей уведомление об угрозе безопасности информации в форматах, обрабатываемых Национальным координационным центром по компьютерным инцидентам, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами КИИ, а также с иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными;

— создание и изменение инструкций по реагированию на компьютерные инциденты, связанные с угрозами безопасности информации, включающих порядок принятия решений, очередность выполняемых действий и способы организации совместных действий участвующих в мероприятиях по реагированию на компьютерные инциденты и ликвидации последствий компьютерных атак работников субъекта КИИ и/или работников привлекаемой в соответствии с действующим законодательством субъектом КИИ организации, осуществляющей лицензируемую деятельность в области защиты информации;

— создание и изменение инструкций по обработке запросов и уведомлений, поступающих из Национального координационного центра по компьютерным инцидентами.

Таким образом, функции ППКА и средств ее реализации в соответствии с нормативно-правовыми актами в целом совпадают.

3. Средства подсистемы предупреждения компьютерных атак в общем контексте теории информационной безопасности

Проведем дальнейшее рассмотрение функций, выполняемых средствами ППКА, в общем контексте теории информационной безопасности (рис. 3) [20, 21].

Из рисунка 3 видно, что результатом выполнения первой функции при рассмотрении активов (ресурсов) информационной системы организации (предприятия) является база (таблица) данных, в которой отражены все серверы, конечные хосты, коммутационное оборудование и телекоммуникационная система, посредством которой осуществляется взаимодействие между данными устройствами и информационно-телекоммуникационной сетью, а также вся необходимая служебная информация об этих устройствах.

Результатом выполнения второй функции при рассмотрении возможных уязвимостей ИС организации (предприятия), реализующихся за счет угроз со стороны нарушителя, является база (таблица) данных уязвимостей и недостатков в настройке ПО, установленного в автоматизированной системе специального

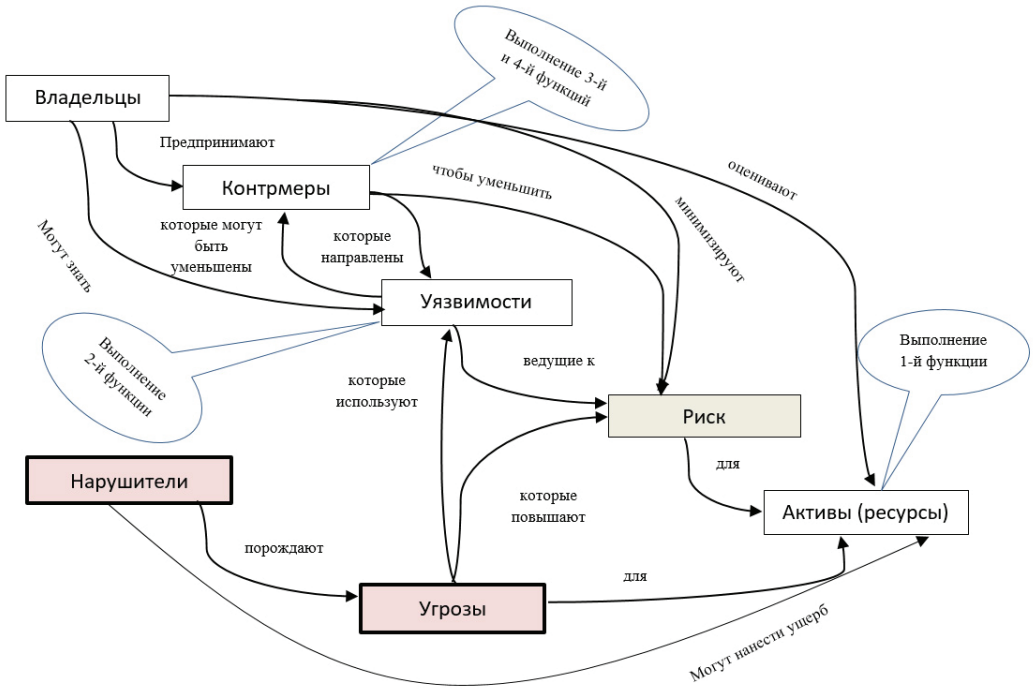

Рис. 3. Функции средств предупреждения компьютерных атак в общем контексте теории информационной безопасности

назначения, для каждого объекта контролируемого информационного ресурса.

Результатами выполнения третьей и четвертой функций являются:

- возможные угрозы, связанные с компьютерными атаками на информационный ресурс;
- идентифицированные уязвимости;
- способы проведения атак, их признаки, способы их обнаружения и меры реагирования на них;
- возможные пути и организационно-технические меры противодействия атакам.
- По окончании выполнения третьей и четвертой функций формируется набор методических документов (правил, политик, инструкций для персонала и т.д.), в том числе «Типовой паспорт реализации угроз вредоносной программы (ВП)» (таблица 1), в котором определяются меры по устранению возможных уязвимостей.

4. Анализ средств подсистемы предупреждения компьютерных атак в рамках концепции построения ведомственных систем обнаружения, предупреждения и ликвидации последствий компьютерных атак

Концепция построения СОПКА ФОИВ, в целом, реализуется в соответствии с требованиями нормативно-правовых документов. Проведем анализ технологий защиты и средств их реализации, позволяющих осуществить в ведомственных системах СОПКА рассмотренные выше функции защиты, и определим место этих средств и технологий в соответствии с эталонной моделью взаимодействия открытых систем (модели OSI) (таблица 2).

В соответствии с представленной в таблице 2 классификацией технологий защиты и средств их реализации, используемых в ведомственных системах СОПКА, подсистема ППКА в явном виде не представлена ни в одной из рассмотренных технологий. Частично ППКА реализуется на прикладном уровне модели OSI, используя контентный анализ прикладного программного обеспечения (ППО) и программно-аппаратных комплексов (ПАК).

Таким образом, проведенный анализ требований нормативно-правовых актов и используемых технологий защиты и средств их реализации в ведомственных СОПКА показал, что требования к ППКА предъявлены, но выполнение ее функций возлагается на технологии и средства защиты, относящиеся к подсистеме обнаружения компьютерных атак (см. таблицу 2), а на уровне методических рекомендаций реализация данных функций осуществляется в рамках контрольно-технических мероприятий по оценке защищенности объектов КИИ. Под контрольно-техническими мероприятиями при этом понимаются организационно-технические мероприятия по получению сведений и оценке реального состояния защищенности информационно-телекоммуникационной сети и информационной системы от деструктивных информационных воздействий, в том числе угроз реализации компью-

Таблица 2

Базовые технологии защиты и средства их реализации в соответствии с моделью OSI

Уровень эталонной модели OSI	Технологии защиты	Место и способ реализации	Протоколы	Тип средства защиты информации
Прикладной	Сигнатурный анализ	ППО, ПАК	SSH, Open VPN	AV, IDS, IPS, NGFW, WAF
	Шифрование	ППО, ПАК		VPN
	Эвристический анализ	ППО, ПАК		AV, IDS, IPS
	Контентный анализ	ППО, ПАК		DLP, SIEM, Proxy, WAF
Представительский	Шифрование	Операционная система (ОС), ППО	SSL, TLS	VPN
Сеансовый	Межсетевой экран (МЭ) с контролем состояния соединения (stateful)	ППО, ПАК, сетевое оборудование	SOCKS	МЭ
	Socks-proxy	ППО		
Транспортный	МЭ (пакетный фильтр)	ОС, ППО, ПАК, сетевое оборудование	Специализированные протоколы ПАК (определяются производителем)	МЭ
Сетевой	ACL (базовые, расширенные)	Маршрутизатор	IPSec (AH, ESP, IKE)	Маршрутизаторы с функцией защиты
	NAT	МЭ, маршрутизатор		
	Шифрование (VPN)	ОС, сетевое оборудование (МЭ, маршрутизатор)		
Канальный	Порт-MAC (Port Security)	Коммутаторы (L2+)	WEP, WPA, WPA2	Коммутаторы с функцией защиты
	Source Guard			
	VLAN			
	Шифрование на канальном уровне	Wi-Fi оборудование		
	Storm Control	Коммутаторы (L2+)		
	DHCP Snooping			
	Dynamic ARP Inspection			
	VPN	ОС, ППО	PPTP, L2F, L2TP	
Физический	Помехоустойчивое кодирование	Технологии, протоколы и средства защиты определяются провайдером, оказывающим услуги на данном уровне		

Примечания: ACL (Access Control List) – список контроля доступа, NAT (Network Address Translation) – трансляция сетевых адресов, ARP (Address Resolution Protocol) – протокол определения адреса, DHCP (Dynamic Host Configuration Protocol) – протокол динамической настройки узла, VLAN (Virtual Local Area Network) – виртуальная локальная компьютерная сеть, VPN (Virtual Private Network) – виртуальная частная сеть, AV (AntiVirus) – антивирус, IDS (Intrusion Detection System) – система обнаружения вторжений, IPS (Intrusion Prevention System) – система предотвращения вторжений, WAF (Web Application Firewall) – брандмауэр веб-приложений, SIEM (Security Information and Event Management) – управление информацией и событиями безопасности, NGFW (Next Generation Firewall) – брандмауэр следующего поколения, DLP (Data Leakage Protection) – защита от утечки данных.

DOI:10.21681/2311-3456-2023-1-13-27

терных атак и внедрения вредоносного ПО, а также по выявлению действующих каналов их проникновения. Другими словами, контрольно-технические мероприятия – это фактическая проверка настройки средств информационной инфраструктуры и защиты информации, установленных на объектах КИИ.

Таким образом, прослеживается подмена понятий при реализации требований нормативно-правовых актов в СОПКА ФОИВ, связанных с ППКА и реализацией ее функций согласно руководящих документов. На основании вышеизложенного видно, что фактически в настоящее время подсистема ППКА в СОПКА ФОИВ реализована не в полном объеме.

5. Анализ технических решений, обеспечивающих реализацию подсистемы предупреждения компьютерных атак

Для полной реализации функций ППКА, а также решения задач, связанных с обеспечением необходимого уровня защищенности автоматизированных систем специального назначения, интегрированных посредством информационно-телекоммуникационной сети в единое информационное пространство, целесообразно построение и внедрение многоуровневой интеллектуальной системы, обеспечивающей безопасность защищаемых ресурсов. Данная система должна реализовывать принципы не только априорной защиты, которые обеспечиваются межсетевыми экранами и системами обнаружения атак (вторжений), антивирусными средствам и т.д., но и принципы апостериорной защиты, связанной со сбором информации о событиях безопасности и выработкой контрмер на основе ее анализа при учете непрерывного воздействия компьютерных атак. Примером такого класса систем являются системы управления информацией и событиями безопасности (анг. – Security Information and Event Management, SIEM) [22].

Основной целью построения и функционирования SIEM-систем является значительное повышение уровня информационной безопасности в информационной инфраструктуре за счет обеспечения возможности в режиме, близком к реальному времени, манипулировать информацией о безопасности и осуществлять проактивное управление инцидентами и событиями безопасности [23]. При этом термин «проактивный» означает «действующий до того, как ситуация станет критической». Как предполагается, проактивное управление инцидентами и событиями безопасности должно основывается на автоматических механизмах, которые используют историческую информацию об анализируемых сетевых событиях и прогнозе будущих событий, а также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы [24].

SIEM-система обеспечивает анализ в реальном времени событий (предупреждений) безопасности, исходящих от сетевых устройств и приложений, и дальнейшее выявление отклонений от норм по заданным критериям [25]. Как правило, она является результатом интеграции и конвергенции следующих двух систем:

- системы управления событиями безопасности (Security Event Management, SEM), которая действует в реальном или близком к реальному масштабе времени и осуществляет автоматический мониторинг событий безопасности, их сбор, корреляцию и генерацию предупреждающих сообщений;
- системы управления информацией о безопасности (Security Information Management, SIM), которая, в свою очередь, анализирует накопленную информацию с помощью статистических и других методов с целью выявления различных отклонений (аномалий) и т.д.

Базовые функции SIEM-систем включают: сбор записей о событиях из различных источников; нормализацию собранных данных с целью представления записей о событиях из различных источников в едином формате для связи и анализа событий; корреляцию данных с целью выявления связей между события, поступившими от различных источников, для ускорения обнаружения и реагирования на угрозы безопасности; агрегацию данных с целью снижения их объема данных путем удаления идентичных записей; формирование отчетов с целью представления результатов заинтересованным лицам в реальном времени или в форме долгосрочных отчетов; решение задач форензики [26].

В настоящее время существует достаточно большое множество SIEM-систем, созданных различными разработчиками [27]. Среди отечественных систем такого типа следует выделить SIEM-системы KOMRAD Enterprise SIEM [28], разработчиком которой является АО «Эшелон Технологии», и MaxPatrol SIEM от Positive Technologies [29]. Проведенный анализ данных систем показывает, что практически все они имеют типовую архитектуру, представленную на рис. 4.

Основная задача SIEM-системы – сбор и корреляция событий информационной безопасности с точки зрения выявлений отклонений поведения защищаемой инфраструктуры от нормального профиля поведения, на основе которых принимается решение о ком-

пьютерном инциденте. В качестве источников данных о событиях безопасности, как показано на рис. 4, могут выступать записи регистрационных журналов операционных систем (ОС), систем управления базами данных (СУБД), МЭ, антивирусных средств, систем обнаружения атак (вторжений), маршрутизаторов и других сетевых средств. Собираемые данные попадают в хранилище SIEM-системы, а затем поступают на обработку в различные аналитические модули, которые, в частности, осуществляют формирование и применение правил корреляции, визуализацию данных о событиях безопасности, моделирование распространения компьютерных атак и поведения защищаемой инфраструктуры, поддержку принятия решения и выбор контрмер по противодействию атакам.

В связи с тем, что правила корреляции, как правило, поставляются поставщиком SIEM-системы или составляются администратором безопасности системы вручную, а также актуальность данных правил, зачастую, утрачивается, можно сделать вывод, что существующие SIEM-системы в качестве самостоятельного решения не способны предупреждать инциденты нарушения информационной безопасности в режиме реального времени.

Для того, чтобы ППКА выявляла атаки на этапе разведки всех уровней реализации, как показано на рис. 1, целесообразно внедрение механизма корреляции событий безопасности с автоматической адаптацией к анализируемой информационной инфраструктуре и выполняемым ею функций в текущий момент времени и детальным написанием правил корреляции, что позволит реагировать на девиантное поведение защищаемой инфраструктуры при подготовке нарушителем компьютерной атаки. Сущность данного предложения заключается в применении гибкого и независимого от спецификаций и платформ защищаемой инфраструктуры решения, обеспечивающего управление информационной безопасностью в автоматическом режиме.

Исследования, проведенные авторами в этой области, позволяют выделить в качестве направлений дальнейшего совершенствования SIEM-систем, определяющих облик SIEM-систем нового поколения [30], и, соответственно, решений по построению и функционированию ППКА, следующие научно-технические предложения:

— применение онтологического подхода к построению хранилища данных в SIEM-системе [31, 32];
— применение онтологий и логического вывода выработки решений по предупреждению компьютерных атак и ликвидации их последствий [33];
— реализация механизмов профилирования пользователей и процессов, а также адаптивной корреляции данных о событиях безопасности на основе технологии больших данных и машинного обучения [34];
— применение методов машинного обучения и обработки больших данных для обнаружения

Рис. 4. Типовая архитектура SIEM-системы

атак, аномальной активности и нарушений критериев и политик безопасности [35, 36].

Сущность этих предложений заключается во внедрении в архитектуру SIEM новых модулей (компонентов), реализующих такие методы искусственного интеллекта, как онтологическое представление знаний, логический вывод и машинное обучение. Их особенностью является ориентация на реализацию в среде распределенных, параллельных и/или суперкомпьютерных вычислений.

6. Заключение

В статье с позиций системного анализа рассмотрена проблема функционирования и реализации подсистемы предупреждения компьютерных атак в следующей последовательности:

(1) рассмотрен алгоритм реализации компьютерной атаки с выделением на каждом его этапе мест реализации функций ППКА;

(2) проведен обзор нормативно-правовых актов по СОПКА в части, касающейся данной подсистемы;

(3) рассмотрены функции ППКА и средств ее реализации, ожидаемые результаты их выполнения;

(4) представлены известные технологии защиты информации и реализующие их средства в соответствии с эталонной моделью OSI;

(5) рассмотрены применяемые и доступные на отечественном рынке технические решения, пригодные для реализации ППКА;

(6) показано, что функции ППКА в отечественных технических решениях реализованы не в полном объеме и что существует подмена понятия «подсистема предупреждения компьютерных атак» понятием «контрольно-технические мероприятия».

В то же время, имеется технологический задел в виде готовой технологии на базе технологии построения SIEM-систем. Однако существует необходимость доработки ее научно-методического аппарата, который в полном объеме позволить реализовать все функции ППКА, определяемые нормативно-правовыми документами.

Предлагаемые направления реализации этих функций связываются, в основном, с применением методов искусственного интеллекта (машинного обучения) и технологии обработки больших данных.

Данная проблемная ситуация определяет актуальность дальнейшего исследования предметной области ППКА, а также необходимость доработки и/или совершенствования вышеуказанного научно-методического аппарата.

Рецензент: Стародубцев Юрий Иванович, доктор военных наук, профессор, Заслуженный деятель науки РФ, профессор кафедры Военной академии связи им. Маршала Советского Союза С.М. Буденного.
E-mail: prof.starodubtsev@gmail.com.

Литература

1. Саенко И.Б., Николаев В.В. Подход к построению оптимальной схемы распределения информационных ресурсов в едином информационном пространстве // Труды ЦНИИС. Санкт-Петербургский филиал. – 2022. – Т. 1. – № 13. – с. 65-68.
2. Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А. Управление качеством информационных услуг. – СПб.: СПбПУ, 2017.
3. Антонов С. Г., Гвоздева Г.А., Климов С.М. Методика повышения устойчивости функционирования информационно-управляющих систем при информационно-технических воздействиях // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – 2019. – С. 6-11.
4. Макаренко С.И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. – 2016. – №3. – С. 292-376.
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.
6. Климов С.М. Методы и интеллектуальные средства предупреждения и обнаружения компьютерных атак на критически важные сегменты информационно-телекоммуникационных систем // Известия ТРТУ. – 2005. – № 4 (48). – С. 74-82.
7. Шабля В.О., Коноваленко С.А., Едунов Р.В. Анализ процесса функционирования SIEM-систем // E-Scio. – 2022. – № 5 (68). – С. 284-295.
8. Ширин К. О. Современные подходы к решению проблемы защиты от сетевых атак «отказ в обслуживании»: системы автоматического предотвращения вторжений // T-Comm: Телекоммуникации и транспорт. – 2011. – Т. 5, № 7. – С. 161-163.
9. Котенко И.В., Коновалов А.М., Шоров А.В. Агентно-ориентированное моделирование функционирования бот-сетей и механизмов защиты от них // Защита информации. Инсайд. – 2010. – № 4 (34). – С. 36-45.
10. Бутова Л.В. Разработка алгоритма обнаружения и предупреждения компьютерных атак / Л.В. Бутова, К.В. Фурсов // Актуальные направления научных исследований XXI века: теория и практика. – 2015. Т. 3, № 5-4 (16-4). – С. 45-50.
11. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении. – СПб.: Издательский Дом «Афина», 2017. – 440 с.
12. Лобач Д.В., Смирнова Е.А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2019. – Т. 11, № 4. – С. 23-32.
13. Королев И.Д., Литвинов Е.С., Пестов С.В. Анализ потоков данных о событиях и инцидентах информационной безопасности, по-

ступающих из разнородных источников // Результаты современных научных исследований и разработок. Сборник статей VIII Всероссийской научно-практической конференции. – 2020. – С. 26-34.
14. Мирошниченко Е.Л., Калач А.В., Зенин А.А. Разработка модели сбора информации о состоянии защищаемой системы для решения задач управления системой обнаружения, предупреждения и ликвидации последствий компьютерных атак // Вестник Воронежского института ФСИН России. – 2020. – № 1. – С. 102-107.
15. Петренко А.С., Петренко С.А. Проектирование корпоративного сегмента СОПКА // Защита информации. Инсайд. – 2016. – № 6 (72). – С. 28-30.
16. Бирюков Д.Н., Ломако А.Г., Петренко С.А. Порождение сценариев предупреждения компьютерных атак // Защита информации. Инсайд. – 2017. – № 4 (76). – С. 70-79.
17. Что такое Cyber-Kill Chain и почему ее надо учитывать в стратегии защиты. – URL: https://habr.com/ru/company/panda/blog/327488/ (дата обращения: 05.11.2022).
18. Котенко И.В., Хмыров С.С. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак // Вопросы кибербезопасности. – 2022. – № 4 (50). – С. 52-79.
19. С. Куц. Взаимодействие КИИ и ГосСОПКА. Positive Technologies. – URL: https://www.ussc.ru/upload/files/Взаимодействие%20КИИ%20и%20ГосСОПКА.pdf (дата обращения: 07.11.2022).
20. Милославская Н. Г., Толстой А. И. Управление рисками информационной безопасности. М.: Горячая линия – Телеком, 2019. 224 с.
21. Дойникова Е.В., Котенко И.В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью. СПб.: Изд-во «Наука», 2021. – 197 с. ISBN 978-5-907366-23-7.
22. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд. – 2012. – № 5 (47). – С. 54-65.
23. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. – 2012. – № 1 (20). – С. 27-56
24. Котенко И.В., Воронцов В.В., Чечулин А.А., Уланов А.В. Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов // Информационные технологии. – 2009. – № 1. – С.37-42.
25. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. – 2012. – № 2. – С. 57-68.
26. Дойникова Е.В., Котенко И.В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью. – Москва: Российская академия наук, 2021. – 184 с.
27. Обзор SIEM-систем на мировом и российском рынке [электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/ (дата обращения: 05.11.2022).
28. KOMRAD Enterprise SIEM. – URL: https://etecs.ru/komrad/ (дата обращения: 05.11.2022).
29. MaxPatrol SIEM. – URL: https://positivetech.softline.com/solution/maxpatrol-siem (дата обращения: 05.11.2022).
30. Котенко И.В., Саенко И.Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук. – 2014. – Т. 84, № 11. – С. 993-1001.
31. Kotenko I., Polubelova O., Saenko I. The Ontological Approach for SIEM Data Repository Implementation // 2012 IEEE International Conference on Green Computing and Communications. – 2012. – Pp. 761-766.
32. Котенко И.В., Саенко И.Б., Полубелова О.В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. – 2013. – № 2 (25). – С. 113-134.
33. Котенко И.В., Полубелова О.В., Саенко И.Б., Чечулин А.А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности. – 2012. – Т. 8, № 2. – С. 100-108.
34. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. – 2017. – № 5 (24). – С. 2-16.
35. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning // IEEE Access. – 2018. – Vol. 6. – P. 72714-72723.
36. 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.

SUBSYSTEM FOR PREVENTION OF COMPUTER ATTACKS AGAINST OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE: ANALYSIS OF FUNCTIONING AND IMPLEMENTATION

Igor Kotenko[1], Igor Saenko[2], Roman Zakharchenko[3], Dmitry Velichko[4]

1 Igor Kotenko, Dr.Sc., Professor, Chief Scientist and Head of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: ivkote@comsec.spb.ru

2 Igor Saenko, Doctor of Technical Sciences, Leading researcher at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: ibsaen@comsec.spb.ru

3 Roman Zakharchenko, Doctor of Technical Sciences, Head of the Department 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: romanzakharchenko@yandex.ru

4 Dmitry Velichko, Adjunct at 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: redbull1666@mail.com

The purpose of the article: *conducting a system analysis of the requirements for the subsystem for preventing computer attacks on critical information infrastructure in order to substantiate the directions for further improved scientific and methodological apparatus for the full functioning of the subsystem for preventing computer attacks.*

Research method: *theoretical and systematic analysis of the requirements of legal acts, scientific publications, protection technologies and means of their implementation in departmental systems for detecting and countering computer attacks.*

The result obtained: *the rationale for the need to build mechanisms for preventing computer attacks on critical information infrastructure objects and the requirements for the subsystem for preventing computer attacks was carried out, an approach was proposed to prevent computer attacks at the stages of reconnaissance by an attacker of critical information infrastructure objects, based on the introduction of a security event correlation mechanism with automatic adaptation to the analyzed information infrastructure and the functions it performs at the current time and a detailed specification of the correlation rules.*

Scope of the proposed approach: *a subsystem for preventing computer attacks of departmental systems for detecting and countering computer attacks, which should identify and prevent attempts to conduct computer attacks on critical information infrastructure objects in advance.*

The scientific novelty *consists in a comprehensive analysis of the need to build mechanisms for preventing computer attacks on critical information infrastructure objects, an analysis of the requirements for the computer attack prevention subsystem, its functions and means of implementation. It is shown that the functions of preventing computer attacks in domestic technical solutions are not fully implemented, and that there is a substitution of the concept of "subsystem for preventing computer attacks" by the concept of "control and technical measures". It is substantiated that for the implementation of the functions of preventing computer attacks, there is a technological backlog in the form of a ready-made technology based on the technology for building SIEM systems. It is shown that there is a need to refine the scientific and methodological apparatus for implementing computer warning functions based on artificial intelligence methods and big data technologies.*

Contribution: *Kotenko I.V. – analysis of the functionality of the subsystem for preventing computer attacks, setting the task and proposals for developing the functionality of the subsystem for preventing computer attacks on critical information infrastructure objects; Saenko I.B. – analysis of the subsystem for preventing computer attacks in the general context of the theory of information security, substantiation of the implementation of the functions of preventing computer attacks based on the technology of building SIEM systems and big data; Zakharchenko R.I. — analysis of technical solutions that ensure the implementation of the subsystem for preventing computer attacks, Velichko D.V. – an approach to detecting computer attacks at the stages of reconnaissance by an attacker of objects of critical information* infrastructure. All authors participated in the writing of the article.

Keywords: *cybersecurity, computer attack, information and telecommunication systems and networks, information and technical impact, systems for detecting, preventing and eliminating the consequences of computer attacks.*

References

1. Saenko I.B., Nikolaev V.V. Approach to the construction of an optimal scheme for the distribution of information resources in a single information space // Proceedings of LO ZNIIS. St. Petersburg branch. — 2022. — T. 1. — No. 13. — pp. 65-68.
2. Starodubtsev Yu.I., Begaev A.N., Davlyatova M.A. Quality management of information services. — St. Petersburg: SPbPU, 2017.
3. Antonov S.G., Gvozdeva G.A., Klimov S.M. Methods of improving the stability of the functioning of information and control systems under information and technical influences // Secure Information Technologies. Proceedings of the Tenth International Scientific and Technical Conference. — 2019. — pp. 6-11.
4. Makarenko S.I. Information weapon in the technical sphere: terminology, classification, examples // Control systems, communications and security. — 2016. — No. 3. – pp. 292-376.
5. Kotenko V.I., Saenko I.B., Kotsynyak M.A., Lauta O.S. Estimation of cyber stability of computer networks based on the simulation of cyber attacks by the method of transformation of stochastic networks // Proceedings of SPIIRAS. — 2017. — No. 6 (55). — S. 160-184.
6. Klimov S.M. Methods and intelligent means of preventing and detecting computer attacks on critically important segments of information and telecommunication systems // Izvestiya TRTU. — 2005. — No. 4 (48). — pp. 74-82.
7. Shablya V.O., Konovalenko S.A., Edunov R.V. Analysis of the process of functioning of SIEM systems // E-Scio. — 2022. — No. 5 (68). – pp. 284-295.
8. Shirin K. O. Modern approaches to solving the problem of protection against network attacks "denial of service": automatic intrusion prevention systems // T-Comm: Telecommunications and transport. — 2011. — V. 5, No. 7. — pp. 161-163.

9. Kotenko I.V., Konovalov A.M., Shorov A.V. Agent-based modeling of the functioning of botnets and mechanisms of protection against them // Protection of information. Inside. — 2010. — No. 4 (34). — pp. 36-45.
10. Butova L.V., Fursov K.V. Development of an algorithm for detecting and preventing computer attacks // Actual directions of scientific research of the XXI century: theory and practice. – 2015. V. 3, No. 5-4 (16-4). — pp. 45-50.
11. Petrenko S.A., Stupin D.D. National Computer Attack Early Warning System. — St. Petersburg: Publishing House "Athena", 2017. — 440 p.
12. Lobach D.V., Smirnova E.A. The state of cybersecurity in Russia at the present stage of the digital transformation of society and the formation of a national system for counteracting cyberthreats // Territory of new opportunities. Bulletin of the Vladivostok State University of Economics and Service. — 2019. — V. 11, No. 4. — pp. 23-32.
13. Korolev I.D., Litvinov E.S., Pestov S.V. Analysis of data flows on information security events and incidents coming from heterogeneous sources // Results of modern scientific research and development. Collection of articles of the VIII All-Russian Scientific and Practical Conference. — 2020. — pp. 26-34.
14. Miroshnichenko E.L., Kalach A.V., Zenin A.A. Development of a model for collecting information about the state of the protected system for solving problems of managing the system for detecting, preventing and eliminating the consequences of computer attacks // Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. — 2020. — No. 1. — pp. 102-107.
15. Petrenko A.S., Petrenko S.A. Design of the SOPKA corporate segment // Protection of information. Inside. — 2016. — No. 6 (72). – pp. 28-30.
16. Biryukov D.N., Lomako A.G., Petrenko S.A. Generation of scenarios for preventing computer attacks // Information Security. Inside. — 2017. — No. 4 (76). — pp. 70-79.
17. What is Cyber-Kill Chain and why should it be considered in a protection strategy. – URL: https://habr.com/ru/company/panda/blog/327488/ (date of access: 11/05/2022).
18. Kotenko I.V., Khmyrov S.S. Analysis of models and methods used for attribution of violators of cybersecurity in the implementation of targeted attacks // Issues of cybersecurity. — 2022. — No. 4 (50). — pp.52-79.
19. Kuts S. Interaction of KII and GosSOPKA. positive technologies. – URL: https://www.ussc.ru/upload/files/Interaction%20KII%20i%20GosSOPKA.pdf (date of access: 07.11.2022).
20. Miloslavskaya N.G., Tolstoy A.I. Information security risk management. M.: Hotline — Telecom, 2019. 224 p.
21. Doynikova E.V., Kotenko I.V. Security assessment and selection of countermeasures for cybersecurity management. St. Petersburg: Nauka Publishing House, 2021. — 197 p.
22. Kotenko I.V., Saenko I.B. SIEM systems for managing security information and events Information protection. Inside. — 2012. — No. 5 (47). — pp. 54-65.
23. Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A. Application of Information and Security Events Management Technology for Information Protection in Critical Infrastructures // Proceedings of SPIIRAS. — 2012. — No. 1 (20). – pp. 27-56
24. Kotenko I.V., Vorontsov V.V., Chechulin A.A., Ulanov A.V. Proactive protection mechanisms against network worms: approach, implementation and results of experiments // Information technologies. — 2009. — No. 1. — pp.37-42.
25. Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A. Technologies for managing information and security events for protecting computer networks // Problems of information security. Computer systems. — 2012. — No. 2. — pp. 57-68.
26. Doynikova E. V., Kotenko I. V. Security assessment and choice of countermeasures for cybersecurity management. — Moscow: Russian Academy of Sciences, 2021. — 184 p.
27. Overview of SIEM systems in the global and Russian market [electronic resource]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/ (date of access: 11/05/2022).
28. KOMRAD Enterprise SIEM. – URL: https://etecs.ru/komrad/ (date of access: 11/05/2022).
29. MaxPatrol SIEM. – URL: https://positivetech.softline.com/solution/maxpatrol-siem (date of access: 11/05/2022).
30. Kotenko I.V., Saenko I.B. Creation of new systems for monitoring and managing cybersecurity // Bulletin of the Russian Academy of Sciences. — 2014. — T. 84, No. 11. — pp. 993-1001.
31. Kotenko I., Polubelova O., Saenko I. The Ontological Approach for SIEM Data Repository Implementation // 2012 IEEE International Conference on Green Computing and Communications. – 2012. – pp. 761-766.
32. Kotenko I.V., Saenko I.B., Polubelova O.V. Perspective data storage systems for monitoring and managing information security // Proceedings of SPIIRAS. — 2013. — No. 2 (25). — pp. 113-134.
33. Kotenko I.V., Polubelova O.V., Saenko I.B., Chechulin A.A. Application of ontologies and logical inference for managing information and security events // High Availability Systems. — 2012. — V. 8, No. 2. — pp. 100-108.
34. Kotenko I.V., Fedorchenko A.V., Saenko I.B., Kushnerevich A.G. Big data technologies for correlation of security events based on connection types // Cybersecurity Issues. — 2017. — No. 5 (24). — pp. 2-16.
35. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning // IEEE Access. — 2008. — Vol. 6. — pp. 72714-72723.
36. 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.