УДК 004.056.53
doi:10.31799/1684-8853-2025-2-37-49
EDN: PVFXDP

Научные статьи
Articles

Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя

В. А. Липатников[a], *доктор техн. наук, профессор, orcid.org/0000-0002-3736-4743, lipatnikovanl@mail.ru*
А. А. Шевченко[a], *канд. техн. наук, старший научный сотрудник, orcid.org/0000-0001-9113-1089*
К. В. Мелехов[a], *адъюнкт, orcid.org/0009-0007-3474-412X*
В. А. Задбоев[a], *младший научный сотрудник, orcid.org/0009-0003-9362-1307*
[a]*Военная академия связи им. Маршала Советского Союза С. М. Буденного, Тихорецкий пр., 3, Санкт-Петербург, 194064, РФ*

Введение: *развитие IT-технологий и особенности динамического взаимодействия сторон конфликта объектов критической информационной инфраструктуры и нарушителей приводит к появлению новых кибератак.* ***Цель:*** *разработать новый подход к мониторингу, анализу и прерыванию цепочки атаки еще до достижения цели вторжения на ранних этапах атак с учетом результатов моделирования процессов противоборства.* ***Результаты:*** *структурирован процесс реализации кибератаки, включающий в себя основные фазы: анализ и внедрение, активное воздействие и завершение с выводом данных. Учтены особенности современных методов многоэтапных атак и используемых программ нарушителем. Разработаны временная модель многоэтапной атаки и граф состояний действий нарушителя, что позволило рассчитать вероятностно-временные характеристики успешного воздействия нарушителя на сеть. Предложен алгоритм прерывания кибератаки на этапе сканирования сети, предполагающий выявление попыток сканирования сети, сбор и обработку информации о нарушителе, а также формирование ответных мер для прерывания атаки и автоматизированный контроль эффективности системы с возможностью корректировки мер защиты. В результате смоделирован процесс реализации активной защиты информационно-вычислительной сети от кибератаки, продемонстрировавший эффективность предложенного метода защиты.* ***Практическая значимость:*** *применение метода прерывания цикла кибератаки на объекты критической информационной инфраструктуры позволит повысить оперативность пресечения воздействий на ранних стадиях проникновения.*

Ключевые слова *— информационно-вычислительная сеть, кибератака, моделирование угрозы, прерывание атаки.*

Для цитирования: Липатников В. А., Шевченко А. А., Мелехов К. В., Задбоев В. А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя. *Информационно-управляющие системы*, 2025, № 2, с. 37–49. doi:10.31799/1684-8853-2025-2-37-49, EDN: PVFXDP
For citation: Lipatnikov V. A., Shevchenko A. A., Melekhov K. V., Zadboev V. A. Active protection method against cyberattacks for the objects of critical information infrastructure based on the interruption of the process of an intruder's impact. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 2, pp. 37–49 (In Russian). doi:10.31799/1684-8853-2025-2-37-49, EDN: PVFXDP

Введение

В современных условиях геополитической нестабильности обеспечение безопасности объектов критической информационной инфраструктуры (КИИ), а именно информационных систем и в частности информационно-вычислительных сетей (ИВС), является актуальным направлением [1], которое включает в себя развитие методик повышения защищенности ИВС от кибератак (КА). Развитие IT-технологий и постоянный рост количества пользователей и аппаратных мощностей информационных систем приводят к неконтролируемому появлению новых уязвимостей в них, которые позволяют нарушителю получать доступ к ИВС КИИ, сканировать ресурсы сети, повышать права доступа в атакуемом сегменте сети, внедрять скрипты, удаленно подключаться к оборудованию ИВС и выключать его, искать конфиденциальную информацию, блокировать учетные записи пользователей [2, 3].

Воздействие КА приводит к повышению в ИВС нелегитимной активности [4], которая влечет за собой изменение пропускной способности телекоммуникационного оборудования, искажению сведений в хранилищах данных или перехвату конфиденциальной информации.

В настоящее время для обеспечения защищенности объектов КИИ, например ИВС государственного учреждения, используется государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Анализ применения ГосСОПКА [5] показал, что в ней развернуты и действуют подсистемы обнаружения, предупреждения и ликвидации последствий КА. Основное внимание по функционированию уделено подсистемам обнаружения и ликвидации

последствий КА, в то время как к подсистеме предупреждения КА, согласно нормативно-правовым документам [5], предъявляются только требования к ее созданию и реализации, но не рассматривается вопрос функционирования. Ввиду этого необходима разработка новых методов предупреждения КА.

В работах [6, 7] представлены способы, в которых делается акцент на управление информационной безопасностью (ИБ) инфраструктуры на основе выявления уязвимостей в процессе функционирования. В данных источниках управление ИБ является реактивным, так как не подразумевается прогнозирование развития атаки на сеть. Вновь разрабатываемые способы и методики управления ИБ должны быть направлены на анализ не только динамики действий нарушителя, но и содержания блоков данных протоколов по этапам атаки.

Наряду с этим одним из требований к управлению ИБ ИВС является реализация способов контроля защищенности в режиме времени, близком к реальному. Отсюда вытекает противоречие между интенсивно развивающимися способами и их реализующими возможностями воздействия на ИВС с одной стороны и применяемыми методами управления ИБ с другой стороны.

В отличие от традиционных методов, которые чаще всего основаны на обнаружении и реагировании на угрозы, активная защита предполагает меры по прерыванию цепочки атаки еще до достижения цели вторжения. Необходим анализ содержания цикла КА в ИВС, т. е. последовательности действий нарушителя.

В статье [8] исследуется цикл КА при наблюдении за параметрами трафика внутри ИВС. Представлено четкое позиционирование и места хранения результатов сканирования, с которыми придется работать администратору ИБ. Однако в предложенной системе отсутствует прогнозирование возможных нарушений ИБ или какие-нибудь противодействия уже проведенной атаке на ИВС.

Целью статьи является представление нового метода мониторинга, анализа и прерывания цепочки атаки еще до достижения цели вторжения с учетом результатов моделирования процесса реализации КА.

Моделирование этапов реализации кибератаки на информационно-вычислительную сеть

Прежде чем переходить к разработке способов противодействия нарушителю, необходимо подробно изучить процесс воздействия на ИВС. Такой подход позволяет не только фиксировать потенциальные угрозы, но и структурировать данные, которые будут необходимы администратору ИБ для оперативного реагирования и принятия мер.

Перед разработкой временной диаграммы (рис. 1) были проанализированы документ ФСТЭК [9] и зарубежная матрица MITRE ATT & CK, описывающие современные тактики и техники, которые применяют нарушители в ИВС. Так как целью исследования является пресечение внедрения нарушителя в ИВС на начальных этапах атаки, то при создании временной диаграммы был сделан акцент на начальные этапы реализации КА с дальнейшим обобщением последующих этапов.

Представлен обобщенный цикл КА при реализации угрозы, который состоит из трех фаз.

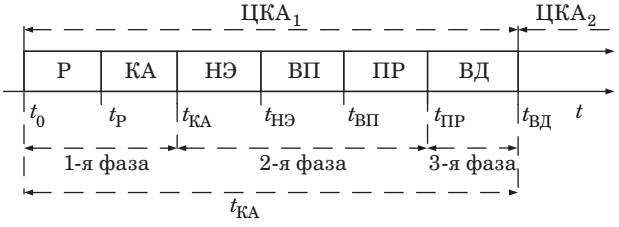
В первой фазе «Анализ и внедрение» нарушитель первоначально проводит разведку, собирая данные об объектах КИИ и изучая систему для выявления слабых мест в ее структуре. Наличие этого этапа зависит от типа атаки и не всегда является обязательным, как, например, для применения SQL-инъекции на публичный веб-ресурс.

После сбора данных осуществляется этап «КА», в котором нарушитель выбирает вид атаки и принимает решение по воздействию на ИВС на основе доступных ему методов в виде вирусов и эксплойтов с целью получить доступ к ИВС для дальнейших действий.

Во второй фазе «Активное воздействие» нарушитель загружает выбранные на предыдущем этапе программы или код в зараженную систему.

После внедрения программы или кода нарушитель начинает их выполнение на зараженной системе, включая сбор информации, установку дополнительного вредоносного ПО, запуск процессов и т. д.

С помощью реализованных ранее программ повышается доступ к более значимым данным



■ ***Рис. 1.*** Временная диаграмма цикла реализации КА: *ЦКА* – цикл кибератаки; *Р* – разведка; *НЭ* – начальная эксплуатация; *ВП* – выполнение программ; *ПР* – повышение ранга; *ВД* – вывод данных

■ ***Fig. 1.*** Time chart of the cyberattack implementation cycle: *ЦКА* – the cyberattack cycle; *Р* – intelligence; *НЭ* – initial exploitation; *ВП* – program execution; *ПР* – rank increase; *ВД* – data output

или выполняются более разрушительные действия в системе.

В третьей фазе «Вывод данных/вредоносные действия» нарушитель завершает свои действия путем кражи или уничтожения данных [10].

Рассмотрим подробнее этапы реализации представленной КА.

При необходимости разведки нарушитель проводит сбор данных с помощью сканирования ИВС (рис. 2).

Слева на рис. 2 показана стандартная передача пакетов при общении сервера с легитимным пользователем, перед началом работы происходит трехстороннее рукопожатие (TCP handshake), в котором пользователь и сервер синхронизируются путем подтверждения (SYN + ACK) пакетов, после чего начинается свободная передача файлов.

Нарушитель при данном методе синхронизации с сервером использует уязвимость, заключающуюся в том, что он отправляет большое количество рукопожатий, предварительно добавив в них точечные запросы о системе с принудительным прерыванием синхронизации, тем самым получая возможность продолжать посылать такие запросы.

Нарушитель при сканировании ИВС способен получить сведения о сервере, обнаружить активные устройства в сети и их IP- и MAC-адреса, определить статусы портов (открыт, закрыт, фильтруется и т. д.) и протоколов (какие используются и уровни их защиты), выявить неактивные или слабозащищенные ресурсы, сформировать карту сети, а при усложненных запросах или недостаточной защите ИВС — получить сведения об уязвимостях сервера, на котором обрабатываются данные, или обнаружить закрытые разделы сайта [11, 12].

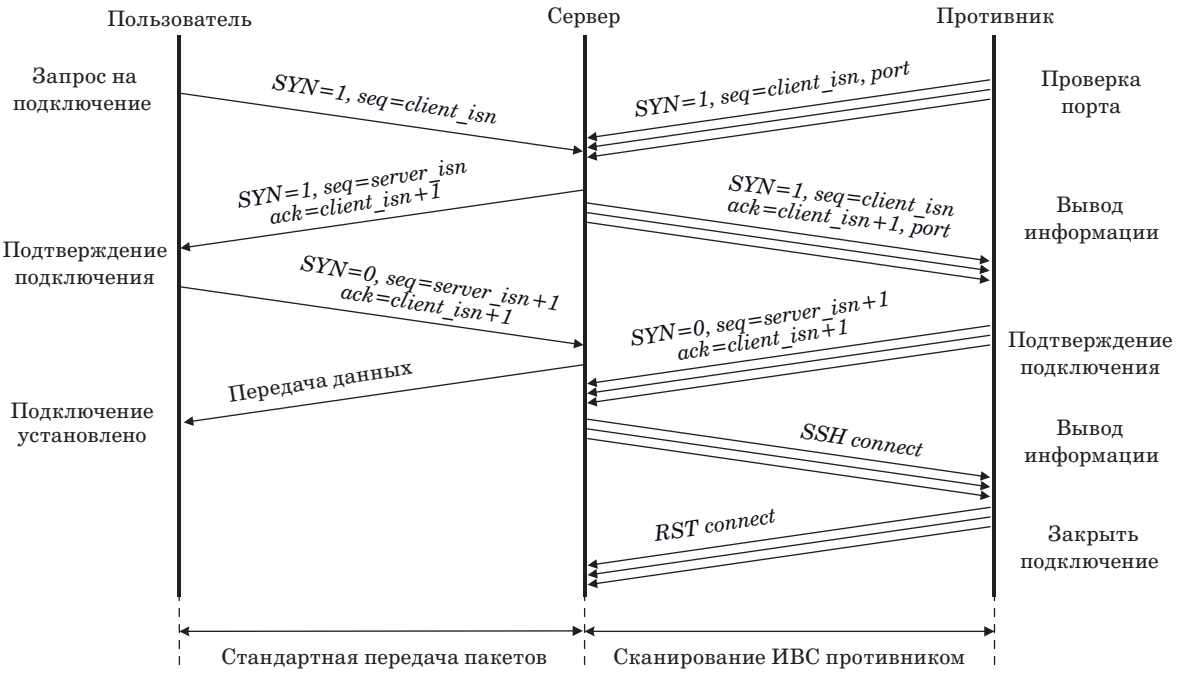
Таким образом нарушитель может получить ценный набор информации о цели атаки, после изучения которой проводит планирование атаки. Например, полезными сведениями могут послужить открытые уязвимости (vulners), сведения о структуре сервера (http-enum) и статусы портов (открыт, закрыт, фильтруется и т. д.) [13].

Ввиду вышесказанного готовое решение по воздействию на ИВС будет выглядеть следующим образом: «Загрузка вредоносного ПО на /admin/index.php через порт 22/tcp с использованием уязвимости CVE-2023-51385».

Загрузка вредоносного ПО представляет собой атаки типа Troyan, Ransomware, Keylogger, Spyware и т. д., которые заражают компьютеры или целые ИВС, в целях кражи данных или получения прав доступа к управлению системой. В случае успешной атаки нарушитель приступает к активным действиям для выполнения своей задачи.

Атаки на ИВС могут быть разнообразными. Возникает необходимость учитывать все сигнатуры, по которым возможно определить нарушителя. Перечень сигнатур представлен на сайте ФСТЭК [9], наиболее известными являются:

1. Угроза утечки информации, удаления информационных ресурсов, ненадлежащего (нецелевого) использования.



■ ***Рис. 2.*** Способ сканирования ИВС нарушителем

■ ***Fig. 2.*** Method of scanning the information and computer network by an intruder

При эксплуатации уязвимостей в ПО нарушитель внедряет в ИВС эксплойты, используя уязвимости в операционных системах, веб-приложениях или другом ПО для получения несанкционированного доступа к системе, выполнения кода или кражи данных. Для реализации своих эксплойтов нарушитель может воспользоваться различными инструментами:

— Metasploit Framework — мощный набор инструментов для разработки, тестирования и использования эксплойтов;

— ExploitDB — онлайн-база данных, содержащая большое количество готовых эксплойтов для различных уязвимостей;

— Immunity Canvas — коммерческое ПО для разработки и тестирования собственных эксплойтов;

— Burp Suite — набор инструментов, используемый для тестирования безопасности веб-приложений, включающий модуль для эксплуатации уязвимостей [14].

2. Угрозы несанкционированного доступа, модификации (искажения), подмены.

Атака типа MiTM (человек посередине) работает следующим образом: нарушитель устанавливает маршрутизатор между двумя устройствами, которые обмениваются данными. Для анализа трафика нарушитель использует программу, например WireShark. Нарушитель создает точку доступа с идентичным названием и паролем, что и у исходной сети, перенаправляет через нее трафик клиентов и запускает WireShark для его прослушивания. Такая атака позволяет ему перехватывать, изменять или внедрять данные в передаваемый трафик.

После достижения своих целей нарушитель забирает всю необходимую информацию, параллельно скрывая или удаляя следы своих действий. Это происходит путем:

— удаления и модификации системных логов в серверах и SIEM;

— удаления временных файлов в хосте, находящихся в папках /temp и оперативной памяти;

— удаления вредоносного ПО или его скрытия для дальнейшего использования;

— создания и маскировки бэкдоров для упрощенного доступа к сети;

— использования VPN и прокси для скрытия точек подключения;

— маскировки вредоносного сетевого трафика под обычные протоколы;

— шифрования и удаления файлов системы.

3. Угроза отказа в обслуживании, нарушения функционирования (работоспособности).

DDoS-атаки (Distributed Denial of Service — атаки, направленные на распределенный отказ в обслуживании) представляют собой один из видов, целью которых является нарушение работоспособности или затруднение доступа к системе для обычных пользователей. При реализации данной атаки нарушитель использует ботнеты (сети зараженных компьютеров) для одновременного направления огромного объема запросов на серверы или сети, что приводит к их перегрузке и временному отказу в обслуживании для пользователей данной сети.

APDoS-атака (Advanced Persistent Denial of Service — усовершенствованная постоянная атака отказа в обслуживании) представляет собой разновидность КА, связанной с высокой степенью угрозы, требующей особых методов защиты от DDoS-атак.

В подобных сценариях нарушитель может намеренно переключаться между разными целями, чтобы отвлечь внимание и обойти меры противодействия, сосредотачивая основную мощь атаки на одной выбранной жертве. Такой нарушитель, обладая постоянным доступом к мощным сетевым ресурсам, способен организовать длительную атаку, сопровождающуюся созданием огромного объема DDoS-трафика.

Особенности APDoS-атак:

— использование OSINT (Open Source Intelligence — разведка по открытым источникам) для тщательного анализа перед атакой, а также сканирование инфраструктуры, позволяющее скрываться в течение длительного времени;

— тактическое исполнение атак по нескольким целям для отвлечения внимания от основной цели атаки;

— большая вычислительная мощность (использование значительных сетевых и аппаратных ресурсов для организации атак);

— одновременные многопоточные атаки на нескольких уровнях OSI (от 3-го до 7-го);

— долговременная активность вышеперечисленных действий [15].

Для реализации атаки, как говорилось выше, первоначально нарушителю необходимо заразить большое количество компьютеров для создания своего ботнета, самым известным ПО является Mirai, способное, помимо компьютеров, заражать устройства интернета вещей (IoT), такие как IP-камеры, маршрутизаторы и умные устройства.

Далее после выбора цели атаки нарушитель удаленно активирует свой ботнет с использованием таких программ, как DDoS-as-a-Service (использование сторонних услуг для DDoS), NTP Reflection Attack Tools и Memcached DDoS Tools для реализации TCP/UDP Flood, HTTP Flood и DNS-amplification [16].

4. Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника.

Использование недостатков, связанных с некорректной настройкой сетевого доступа, — это тип атаки, при котором нарушитель эксплуатирует ошибки в конфигурации сетевых служб, маршрутизации или прав доступа для получения доступа к чувствительным данным или системам. Такие уязвимости могут возникать из-за неправильной настройки брандмауэров (Firewall Misconfiguration Attack), маршрутизаторов (Default Credential Exploitation), серверов (Network Sprawl Attack) и других сетевых компонентов.

5. Угроза распространения противоправной информации.

Целенаправленная рассылка через рассылку рекламных писем. Атака реализуется после получения доступа к ресурсам организации, например для рассылки электронных писем от лица доверенной организации, с целью распространить вредоносное ПО.

6. Угроза несанкционированного массового сбора информации.

SQL-инъекции — это атаки, направленные на взлом веб-приложений путем внедрения злонамеренного SQL-кода в поле ввода на вебстранице, что может привести к несанкционированному доступу к базе данных и краже или модификации данных. Ниже описан пример реализации SQL-инъекции с использованием программы Havij.

Нарушитель использует Havij для сканирования веб-сайтов на наличие уязвимых точек ввода, в которые вводится злонамеренный SQL-код, например ' *OR* 1=1 --, который заставляет вывести все записи таблицы, из которых с помощью «парсинга» нарушитель добывает ценные сведения [17].

Математическая модель процесса реализации кибератаки на информационно-вычислительную сеть

Проведем моделирование воздействия нарушителя на ИВС, так как это позволит детально изучить процесс реализации угроз, оценить вероятность их успешного выполнения и на основе полученных результатов выявить наиболее уязвимые этапы цепочки КА и разработать эффективные способы противодействия.

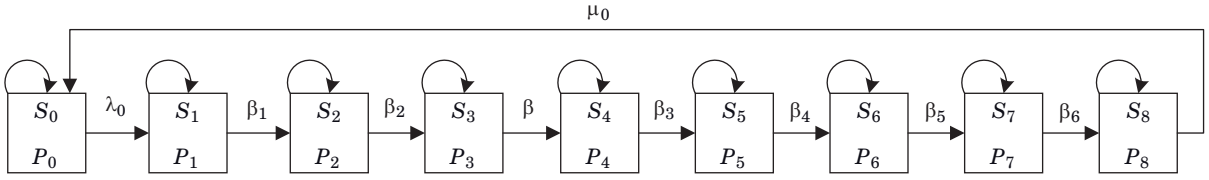
В качестве примера воздействия нарушителя разработана модель реализации угрозы типа DDoS-атаки с реализацией проникновения в ИВС с использованием эксплуатации уязвимостей.

Для исследования процесса реализации КА, а также оценки вероятностно-временных характеристик КА в рамках настоящего исследования на основе теории марковских процессов разработана математическая модель в виде графа состояний (рис. 3, где P_i — вероятность нахождения нарушителя в i-м состоянии), параметры процесса КА представлены в таблице. Данная модель позволит выполнить расчет вероятностных характеристик успешного проведения атаки.

Взяв за основу полученный выше граф состояний, составим систему дифференциальных уравнений

$$\begin{cases} \frac{dP_0(t)}{dt} = \mu_0 P_8(t) - \lambda_0 P_0(t); \\ \frac{dP_1(t)}{dt} = \lambda_0 P_0(t) - \beta_1 P_1(t); \\ \frac{dP_2(t)}{dt} = \beta_1 P_1(t) - \beta_2 P_2(t); \\ \frac{dP_3(t)}{dt} = \beta_2 P_2(t) - \beta P_3(t); \\ \frac{dP_4(t)}{dt} = \beta P_3(t) - \beta_3 P_4(t); \\ \frac{dP_5(t)}{dt} = \beta_3 P_4(t) - \beta_4 P_5(t); \\ \frac{dP_6(t)}{dt} = \beta_4 P_5(t) - \beta_5 P_6(t); \\ \frac{dP_7(t)}{dt} = \beta_5 P_6(t) - \beta_6 P_7(t); \\ \frac{dP_8(t)}{dt} = \beta_6 P_7(t) - \mu_0 P_8(t), \end{cases} \quad (1)$$

решение которой представлено выражением



■ ***Рис. 3.*** Граф состояний действий нарушителя при реализации угрозы

■ ***Fig. 3.*** Graph of the states of the attacker's actions during the implementation of the threat

$$
\begin{cases}
P_0 = \dfrac{1}{\left(1+\lambda_0\left(\dfrac{1}{\beta_1}+\dfrac{1}{\beta_2}+\dfrac{1}{\beta}+\dfrac{1}{\beta_3}+\dfrac{1}{\beta_4}+\dfrac{1}{\beta_5}+\dfrac{1}{\beta_6}+\dfrac{1}{\mu_0}\right)\right)}; \\
P_1 = \dfrac{\lambda_0}{\beta_1}\dfrac{1}{\left(1+\lambda_0\left(\dfrac{1}{\beta_1}+\dfrac{1}{\beta_2}+\dfrac{1}{\beta}+\dfrac{1}{\beta_3}+\dfrac{1}{\beta_4}+\dfrac{1}{\beta_5}+\dfrac{1}{\beta_6}+\dfrac{1}{\mu_0}\right)\right)}; \\
P_2 = \dfrac{\lambda_0}{\beta_2}\dfrac{1}{\left(1+\lambda_0\left(\dfrac{1}{\beta_1}+\dfrac{1}{\beta_2}+\dfrac{1}{\beta}+\dfrac{1}{\beta_3}+\dfrac{1}{\beta_4}+\dfrac{1}{\beta_5}+\dfrac{1}{\beta_6}+\dfrac{1}{\mu_0}\right)\right)}; \\
P_3 = \dfrac{\lambda_0}{\beta}\dfrac{1}{\left(1+\lambda_0\left(\dfrac{1}{\beta_1}+\dfrac{1}{\beta_2}+\dfrac{1}{\beta}+\dfrac{1}{\beta_3}+\dfrac{1}{\beta_4}+\dfrac{1}{\beta_5}+\dfrac{1}{\beta_6}+\dfrac{1}{\mu_0}\right)\right)}; \\
P_4 = \dfrac{\lambda_0}{\beta_3}\dfrac{1}{\left(1+\lambda_0\left(\dfrac{1}{\beta_1}+\dfrac{1}{\beta_2}+\dfrac{1}{\beta}+\dfrac{1}{\beta_3}+\dfrac{1}{\beta_4}+\dfrac{1}{\beta_5}+\dfrac{1}{\beta_6}+\dfrac{1}{\mu_0}\right)\right)}; \\
P_5 = \dfrac{\lambda_0}{\beta_4}\dfrac{1}{\left(1+\lambda_0\left(\dfrac{1}{\beta_1}+\dfrac{1}{\beta_2}+\dfrac{1}{\beta}+\dfrac{1}{\beta_3}+\dfrac{1}{\beta_4}+\dfrac{1}{\beta_5}+\dfrac{1}{\beta_6}+\dfrac{1}{\mu_0}\right)\right)}; \\
P_6 = \dfrac{\lambda_0}{\beta_5}\dfrac{1}{\left(1+\lambda_0\left(\dfrac{1}{\beta_1}+\dfrac{1}{\beta_2}+\dfrac{1}{\beta}+\dfrac{1}{\beta_3}+\dfrac{1}{\beta_4}+\dfrac{1}{\beta_5}+\dfrac{1}{\beta_6}+\dfrac{1}{\mu_0}\right)\right)}; \\
P_7 = \dfrac{\lambda_0}{\beta_6}\dfrac{1}{\left(1+\lambda_0\left(\dfrac{1}{\beta_1}+\dfrac{1}{\beta_2}+\dfrac{1}{\beta}+\dfrac{1}{\beta_3}+\dfrac{1}{\beta_4}+\dfrac{1}{\beta_5}+\dfrac{1}{\beta_6}+\dfrac{1}{\mu_0}\right)\right)}; \\
P_8 = \dfrac{\lambda_0}{\mu_0}\dfrac{1}{\left(1+\lambda_0\left(\dfrac{1}{\beta_1}+\dfrac{1}{\beta_2}+\dfrac{1}{\beta}+\dfrac{1}{\beta_3}+\dfrac{1}{\beta_4}+\dfrac{1}{\beta_5}+\dfrac{1}{\beta_6}+\dfrac{1}{\mu_0}\right)\right)}.
\end{cases}
\tag{2}
$$

С помощью исходных данных из таблицы, являющихся экспертными оценками, были проведены контрольные решения оценки вероятности успешного воздействия атаки от времени идентификации уязвимости при различном времени, затрачиваемом на выбор атаки.

Вероятность успешного воздействия $P_в = P_0 + P_8$, так как состояние 8 является реализацией угрозы «Хищение данных», а в состоянии 0 нарушитель выбирает другую цель для атаки, поэтому возвращается к нему. В связи с этим вероятность успешного воздействия будет вычисляться с помощью выражения

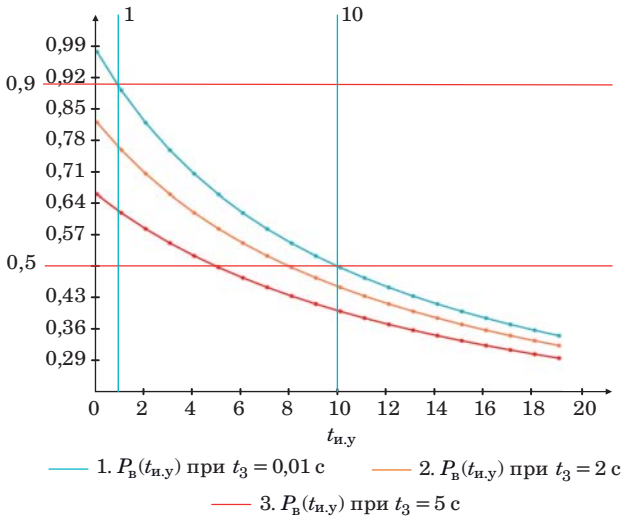
$$
P_в = \frac{\mu_0\lambda_0}{\mu_0\left(1+\lambda_0\left(\dfrac{1}{\beta_1}+\dfrac{1}{\beta_2}+\dfrac{1}{\beta}+\dfrac{1}{\beta_3}+\dfrac{1}{\beta_4}+\dfrac{1}{\beta_5}+\dfrac{1}{\beta_6}+\dfrac{1}{\mu_0}\right)\right)}. \tag{3}
$$

С применением (3) построим график зависимости вероятности успешного воздействия атаки от времени идентификации уязвимости при различном времени, затрачиваемом на выбор атаки (рис. 4). Из графика можно сделать вывод, что нарушитель должен действовать максимально быстро в ИВС при реализации всех атак, в которых присутствует этап идентификации уязвимости, поскольку любые задержки значительно увеличивают риск его обнаружения, поэтому необходимо обладать средствами, которые превосходят его по скорости.

■ Параметры процесса реализации угрозы типа DDoS-атаки с реализацией эксплуатации уязвимостей

■ Parameters of the process of implementing a threat of the type DDoS attack with the implementation of the attack Exploitation of vulnerabilities

Состояние S_n	Описание состояния S_n	Интенсивность перехода в состояние S_m	Параметр	Описание параметра	Значения параметров, с
S_0	Исходное состояние	$\lambda_0 = \frac{1}{\bar{t}_0}$	$\bar{t}_0$	Среднее время принятия решения на КА	10
S_1	Формирование ботнета	$\beta_1 = \frac{1}{\bar{t}_1}$	$\bar{t}_1$	Среднее время формирования ботнета	0,01
S_2	Подготовка к атаке	$\beta_2 = \frac{1}{\bar{t}_2}$	$\bar{t}_2$	Среднее время подготовки к атаке	0,01
S_3	Идентификация уязвимостей	$\beta = \frac{1}{\overline{t_{\text{и.у}}}}$	$\overline{t_{\text{и.у}}}$	Среднее время идентификации уязвимостей	25
S_4	Выбор метода атаки	$\beta_3 = \frac{1}{\bar{t}_3}$	$\bar{t}_3$	Среднее время выбора метода атаки	0,01 2 5
S_5	Приведение цифрового устройства или программы в состояние готовности к использованию атаки	$\beta_4 = \frac{1}{\bar{t}_4}$	$\bar{t}_4$	Среднее время приведения цифрового устройства или программы в состояние готовности к использованию атаки	0,01
S_6	Нарушение доступности к цели атаки	$\beta_5 = \frac{1}{\bar{t}_5}$	$\bar{t}_5$	Среднее время нарушения доступности к цели атаки	0,01
S_7	Проникновение в ИВС	$\beta_6 = \frac{1}{\bar{t}_6}$	$\bar{t}_6$	Среднее время проникновения в ИВС	0,01
S_8	Хищение данных	$\mu_0 = \frac{1}{\bar{t}_7}$	$\bar{t}_7$	Среднее время, затрачиваемое на хищение данных	0,01



■ ***Рис. 4.*** Зависимость вероятности успешного воздействия атаки от времени идентификации уязвимости при различном времени, затрачиваемом на выбор атаки

■ ***Fig. 4.*** Dependence of the probability of successful impact of an attack on the time of vulnerability identification at different times spent on the selection of an attack

Метод активной защиты информационно-вычислительной сети от кибератаки нарушителя

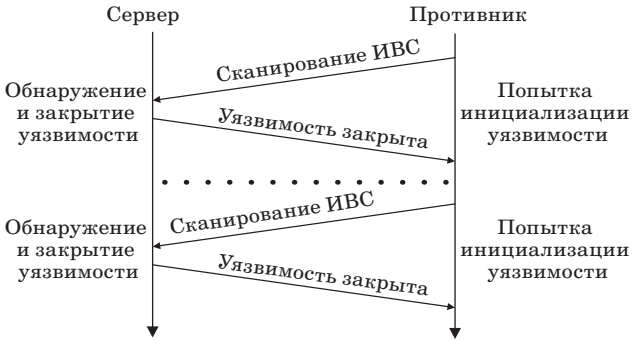
Анализ действий нарушителя [18] приводит к выводу, что самая ранняя возможность обнаружения и прерывания КА — это состояние 3, когда нарушитель пытается провести сканирование ИВС. Пример реализации прерывания цепочки КА на этапе сканирования представлен на рис. 5.

Для реализации прерывания цепочки КА предложен метод активной защиты ИВС (рис. 6) от всех типов КА, в которых нарушителю требуется предварительно проводить сканирование сети для обнаружения уязвимостей.

Суть алгоритма заключается в следующем.

1. Обнаруживается попытка сканирования нарушителем ИВС. Собирается информация о нарушителе и отправляется в центр управления ИБ [19, 20].

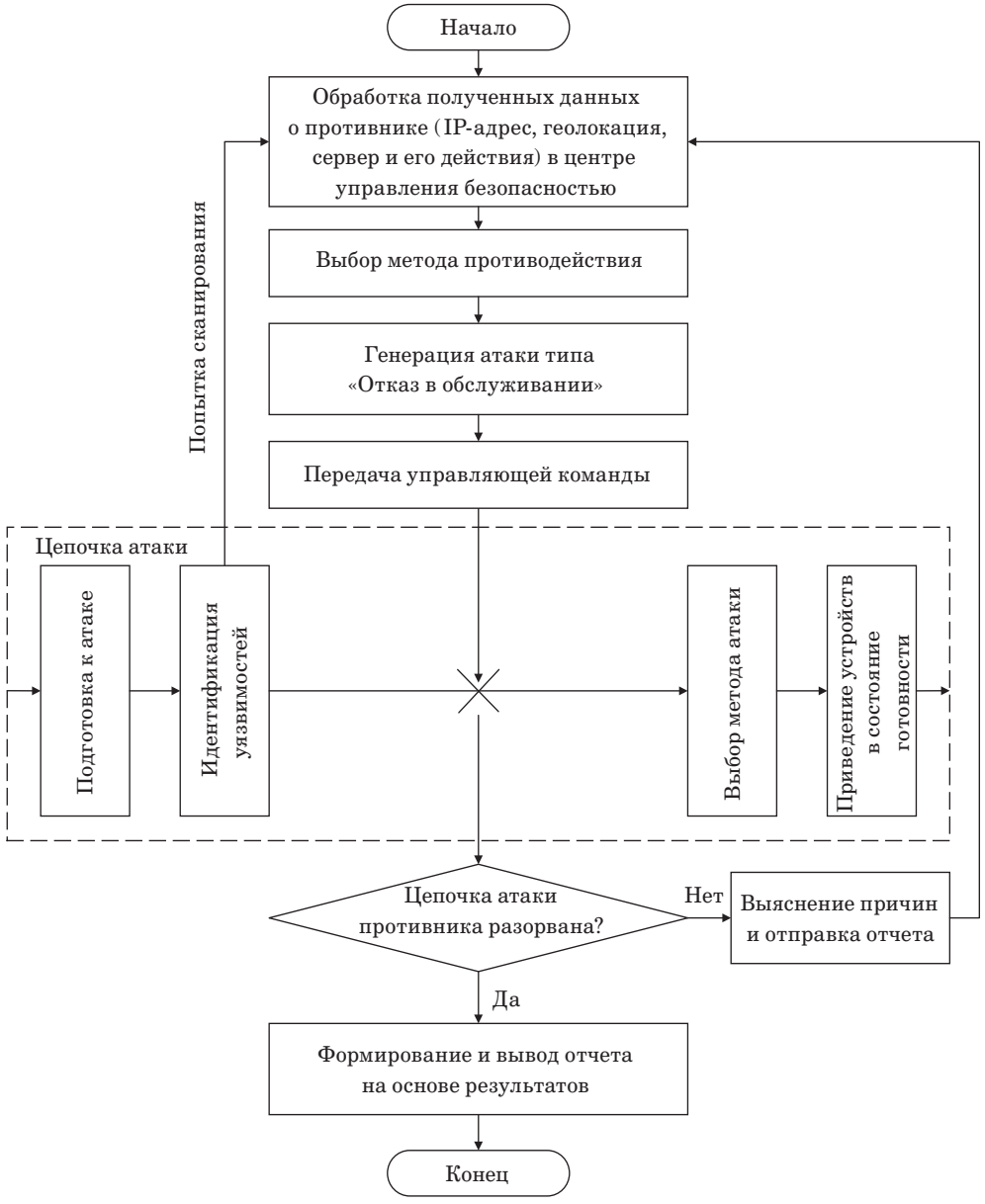
2. Полученная информация обрабатывается в центре управления ИБ. Происходит выбор и



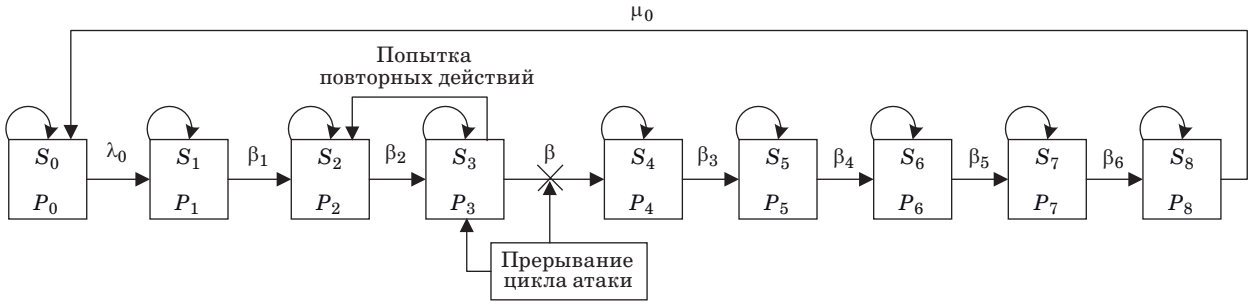
■ ***Рис. 5.*** Пример прерывания КА нарушителя
■ ***Fig. 5.*** Example of interrupting an attacker's cyberattack

передача управляющих команд на реализацию ответных мер для прерывания КА.

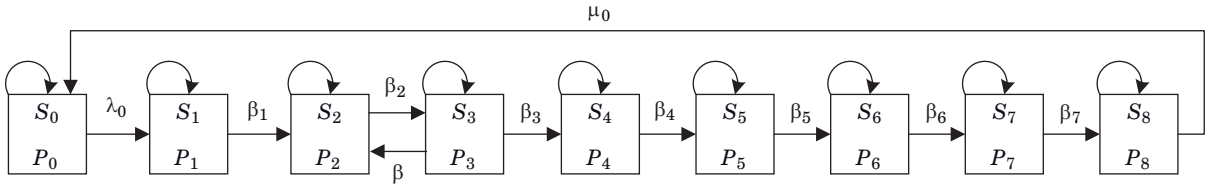
3. В конце проводится проверка, при которой выясняется, прервана КА или нет. Если атака не прервана, то анализируется неудачное прерывание атаки и отправляется отчет в центр ИБ. После принимается повторное решение об анализе сложившейся ситуации с дальнейшим выбором других ответных мер. При успешном же разрыве цепочки КА формируется отчет о результатах прерывания и отправляется администратору центра управления ИБ [21–23]. Граф прерывания КА нарушителя представлен на рис. 7.



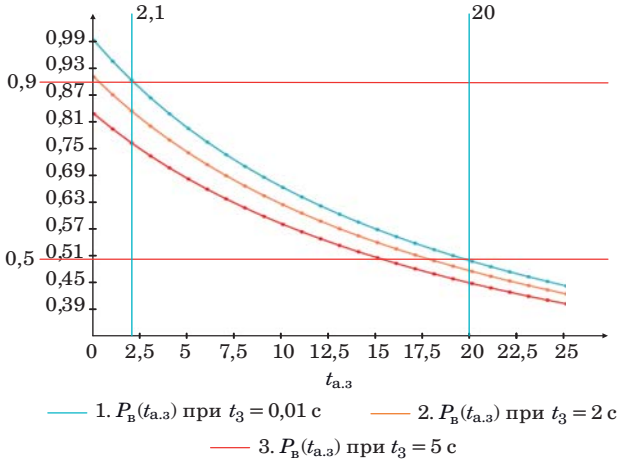
■ ***Рис. 6.*** Алгоритм прерывания КА нарушителя
■ ***Fig. 6.*** Flow diagram of the algorithm for interrupting an attacker's cyberattack



■ ***Рис. 7.*** Граф прерывания КА
■ ***Fig. 7.*** Cyberattack interrupt graph



■ ***Рис. 8.*** Граф состояний нарушителя с условием прерывания КА
■ ***Fig. 8.*** Graph of the state of the attacker with the condition of aborting the cyberattack



■ ***Рис. 9.*** Зависимость вероятности реализации нарушителем угрозы от времени активной защиты КА при различном времени, затрачиваемом на выбор атаки
■ ***Fig. 9.*** Dependence of the probability of the threat implementation by the intruder on the time of successful interruption of the active defense of a cyber attack with different times spent on choosing an attack

Если при попытке нарушителя по сканированию ИВС прервать его КА, то ему придется откатиться до состояния 2, в котором проводится подготовка новой атаки. Граф состояний нарушителя с условием прерывания КА представлен на рис. 8.

С использованием графа на рис. 8 и теории марковских случайных процессов получена зависимость вероятности реализации нарушителем угрозы от времени успешного прерывания КА

$$P_{в} = \frac{\mu_0\lambda_0}{\mu_0\left(1+\lambda_0\left(\frac{1}{\beta_1}+\frac{\beta+\beta_3}{\beta\beta_3}+\frac{1}{\beta_3}+\frac{1}{\beta_4}+\right.\right.} \\ \left.\left.+\frac{1}{\beta_5}+\frac{1}{\beta_6}+\frac{1}{\beta_7}+\frac{1}{\mu_0}\right)\right). \quad (4)$$

С учетом исходных данных, представленных в таблице, построен график зависимости вероятности реализации нарушителем угрозы от времени активной защиты КА при различном времени, затрачиваемом на выбор атаки (рис. 9).

Как видно из рис. 9, нарушителю необходимо выбрать метод КА за две секунды, чтобы повысить вероятность успешной реализации КА (кривая *1*). В случае, когда нарушитель принимает решение на реализацию КА за время более двух секунд, вероятность успешной реализации КА резко уменьшается (кривые *2* и *3*). Из вышесказанного можно сделать вывод, что система активной защиты должна реагировать на КА нарушителя в предельно короткий промежуток времени ($t_3 \le 2$ с).

Заключение

Разработана и исследована модель КА нарушителя на объект КИИ, отражающая обобщенный цикл атаки, вероятностно-временные характеристики и этапы реализации, а также предложен активный метод защиты ИВС. Работа направлена на повышение защищенности ИВС от КА.

В ходе работы достигнуты следующие результаты.

1. Структурирован процесс реализации КА, который включает в себя три основные фазы: анализ и внедрение, активное воздействие и завершение с выводом данных. Каждая фаза дополнительно разбита на этапы, такие как разведка, начальная эксплуатация, выполнение команд и повышение привилегий. Эта структура позволяет детализировать действия нарушителя и выделить ключевые точки для противодействия.

2. Проведен анализ современных типов атак, включая DDoS, SQL-инъекции, эксплуатацию уязвимостей и атаки на IoT-устройства. Проанализированы программы, которые использует нарушитель, такие как Nmap, Metasploit, Havij, Mirai и др.

3. Разработана временная диаграмма цикла атак, а также граф состояний действий нарушителя, который отражает ключевые этапы подготовки и реализации угроз, что позволяет рассчитывать вероятностно-временные характеристики успешного воздействия.

4. Разработан алгоритм прерывания КА на этапе сканирования сети, который предполагает:

— выявление попыток сканирования ИВС нарушителем;

— сбор и обработку информации о действиях нарушителя;

— формирование ответных мер для прерывания атаки, включая активные действия, направленные на затруднение последующих попыток проникновения;

— автоматизированный контроль эффективности прерывания атаки с возможностью корректировки мер защиты.

5. Проведено моделирование процесса реализации активной защиты ИВС от КА, которое продемонстрировало эффективность предложенного метода защиты. На основании моделирования можно утверждать, что система защиты должна работать в предельно короткий промежуток времени ($t \leq 2$ с), так как задержка даже в несколько секунд значительно увеличивает шансы нарушителя на успех при реализации угрозы типа DDoS-атаки с эксплуатацией уязвимостей.

Новизной предлагаемого метода является внедрение в алгоритм обеспечения защиты объектов КИИ активных мер противоборства, основанных на реализации процесса прерывания воздействия нарушителя, заключающегося в выявлении попытки сканирования ИВС нарушителем, сборе и обработки информации о нем и формировании ответных мер противодействия.

Практическая значимость заключается в том, что предложен и протестирован метод прерывания КА на этапе сканирования, который может быть внедрен в современные системы ИБ, а также использован для создания автоматизированных систем мониторинга и защиты, способных действовать в режиме реального времени. Представленные результаты обеспечивают повышение устойчивости ИВС к КА, снижая вероятность их успешной реализации.

Литература

1. **Osipov V., Kuleshov S., Zaytseva A., Levonevskiy D., Miloserdov D.** Neural network forecasting of news feeds. *Expert Systems with Applications*, 2021, vol. 169, iss. 4, Article 114521. doi:10.1016/j.eswa.2020.114521
2. **Котенко И. В., Саенко И. Б., Лаута О. С., Юрьев А. С., Запруднов М. С.** Протестное программное обеспечение: анализ и подход к обнаружению, основанный на машинном обучении. *Вопросы кибербезопасности*, 2024, № 6, с. 42–52. doi:10.21681/2311-3456-2024-6-42-52, EDN: VCJRVW
3. **Котенко И. В., Саенко И. Б., Бортникер П. В.** Методика обнаружения сетевых вторжений на основе интеграции методов вейвлет-анализа и математической статистики. *Правовая информатика*, 2024, № 4, с. 23–31. doi:10.24412/1994-1404-2024-4-23-31, EDN: TYLWLM
4. **Amma N. G. B., Selvakumar S., Velusamy R. L.** A statistical approach for detection of denial-of-service attacks in computer networks. *IEEE Transactions on Network and Service Management*, 2020, vol. 17, no. 4, pp. 2511–2522. doi:10.1109/TNSM.2020.3022799
5. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». https://gossopka.ru/doc/npa/federalnye-zakony/federalnyy-zakon-ot-26072017-n-187-fz-o-bezopasnosti-kriticheskoy-informacionnoy-infrastruktury-ross-37407.html (дата обращения: 12.10.2024).
6. **Kumar A., Singh R., Sharma P.** A Comprehensive study on web application firewalls: Technologies, challenges, and future directions. *International Journal of Web Information Systems*, 2021, vol. 17, iss. 4, pp. 393–415. doi:10.1108/IJWIS-01-2021-0005
7. Пат. 2758997 C1 Российская Федерация, МПК H04L 29/02, G06F 21/50. Способ защиты информа-

ционно-вычислительной сети от вторжений, С. С. Чайковский. № 2021107965; заявл. 25.03.2021; опубл. 11.08.2021.

8. **Липатников В. А., Задбоев В. А., Мелехов К. В., Шевченко А. А.** Метод повышения защищенности информационно-телекоммуникационной сети с учетом использования средств определения геолокации нарушителя. *Труды учебных заведений связи*, 2023, № 9(4), с. 86–96. doi:10.31854/1813-324X-2023-9-4-86-96, EDN: FWQHUC
9. Методика оценки угроз безопасности информации. https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g.html (дата обращения: 05.11.2024).
10. **Задбоев В. А., Беседин М. Д., Антонов А. С.** Определение цикла атаки противника в информационно-вычислительной сети. Проблемы стандартизации, унификации и метрологии систем и средств связи специального назначения в аспекте их цифровой трансформации: науч.-техн. сб./под ред. В. А. Гаврина. СПб., ВАС, 2024, с. 47–51.
11. **Липатников В. А., Шевченко А. А., Мелехов К. В., Ткачев Д. Ф.** Методика повышения защищенности сети передачи данных объектов критической информационной инфраструктуры при многоэтапных атаках. *Информационно-управляющие системы*, 2024, № 1, с. 44–55. doi:10.31799/1684-8853-2024-1-44-55, EDN: MVWIFR
12. **Липатников В. А., Мелехов К. В., Мелихов И. А.** Особенности сетевого контроля в сети передачи данных в условиях многоэтапных атак. *Технологии. Инновации. Связь: материалы научно-практической конференции*, Санкт-Петербург, 12 апреля 2023 г. СПб., 2023, с. 171–174.
13. **Sarhan M., Layeghy S., Moustafa N., Portmann M.** *Netflow datasets for machine learning-based network intrusion detection systems*. Big Data Technologies and Applications. Springer International Publishing, 2021, pp. 117–135.
14. **Новикова Е. С., Голубев С. А.** Подход к обнаружению вторжений на основе федеративного обучения. *Международная научная конференция по проблемам управления в технических системах: материалы конференции*, Санкт-Петербург, 26–28 сентября 2023 г. СПб., 2023, с. 200–203. doi:10.1109/CTS59431.2023.10289088, EDN: XPCAUO
15. **Patil N. V., Krishna C. R., Kumar K.** Distributed frameworks for detecting distributed denial of service attacks: A comprehensive review, challenges and future directions. *Concurrency and Computation: Practice and Experience*, 2021, vol. 33, no. 10, p. e6197. doi:10.1002/cpe.6197
16. **Shukla P., Krishna C. R., Patil N. V.** Kafka-Shield: Kafka streams-based distributed detection scheme for IoT traffic-based DDoS attacks. *Security and Privacy*, 2024, vol. 7, no. 12. doi:10.1002/spy2.416
17. **Nasereddin M., ALKhamaiseh A., Qasaimeh M.** A systematic review of detection and prevention techniques of SQL injection attacks. *Information Security Journal: A Global Perspective*, 2023, vol. 32, no. 4, pp. 252–265. doi:10.1080/19393555.2021.1995537
18. **Jiang Y., Wu S., Yang H., Luo H., Chen Z., Yin S., Kaynak O.** Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022, vol. 52, no. 12, pp. 7799–7809. doi:10.1109/TSMC.2022.3164024
19. **Gong C., Zheng Z., Wu F., Shao Y., Li B., Chen G.** To store or not? Online data selection for federated learning with limited storage. *ACM Web Conference*, 2023, pp. 3044–3055. doi:10.1145/3543507.3583426
20. **Mulay A., Gaspard B., Naidu R., Gonzalez-Toral S., Semwal T., Manish Agrawal A.** FedPerf: A practitioners' guide to performance of federated learning algorithms. *NeurIPS 2020 PMLR*, 2021, vol. 148, pp. 302–324.
21. **Saputra F. A., Salman M., Hasim J. A. 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*, 2022, vol. 6, iss. 1, p. 19. doi:10.3390/bdcc6010019
22. **Chen J., Gao X., Deng R., He Y., Fang C., Cheng P.** Generating adversarial examples against machine learning-based intrusion detector in industrial control systems. *IEEE Transactions on Dependable and Secure Computing*, 2022, vol. 19, no. 3, pp. 1810–1825. doi:10.1109/TDSC.2020.3037500
23. **Мурашов Д. А., Ушакова В. А.** Постановка и анализ путей решения задачи синтеза программ управления и параметров информационно-вычислительной сети на основе полимодельного описания. *Авиакосмическое приборостроение*, 2022, № 8, с. 23–32. doi:10.25791/aviakosmos.8.2022.1293, EDN: UJXAWV

UDC 004.056.53
doi:10.31799/1684-8853-2025-2-37-49
EDN: PVFXDP

Active protection method against cyberattacks for the objects of critical information infrastructure based on the interruption of the process of an intruder's impact

V. A. Lipatnikov[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-3736-4743, lipatnikovanl@mail.ru
A. A. Shevchenko[a], PhD, Tech., Senior Researcher, orcid.org/0000-0001-9113-1089
K. V. Melekhov[a], Post-Graduate Student, orcid.org/0009-0007-3474-412X
V. A. Zadboev[a], Junior Researcher, orcid.org/0009-0003-9362-1307
[a]S. M. Budenny Military Academy of Communications, 3, Tikhoretskii Pr., 190064, Saint-Petersburg, Russian Federation

Introduction: The development of IT-technologies and the specifics of dynamic interaction of the parties within the conflict between critical information infrastructure objects and intruders lead to the emergence of new cyberattacks. **Purpose:** To develop a new approach to monitoring, analyzing and interrupting the attack chain even before it achieves the goal of invasion at early stages of attacks, with the results of confrontation modeling taken into account. **Results:** We structure the process of implementing a cyberattack, including the main phases: analysis and implementation, active impact and completion with data output. The features of modern methods of multi-stage attacks and the programs used by an intruder are taken into account. We develop a time model of a multi-stage attack and a state graph of an intruder's actions, which makes it possible to calculate the probabilistic and time characteristics of a successful intruder's impact on the network. We propose an algorithm for interrupting a cyberattack at the network scanning stage, which involves identifying attempts to scan the network, collecting and processing information about the intruder, as well as forming countermeasures to interrupt the attack and implementing an automated control of the system's effectiveness with the ability to adjust protection measures. As a result, we model the process of implementing active protection against cyberattacks for the information and computing network, which demonstrates the effectiveness of the proposed protection method. **Practical relevance:** The use of the method of interrupting the cyberattack cycle at critical information infrastructure objects will increase the efficiency of suppressing the impact of a cyberattack at early stages of penetration.

Keywords — information and computing network, cyberattack, threat modeling, attack interruption.

For citation: Lipatnikov V. A., Shevchenko A. A., Melekhov K. V., Zadboev V. A. Active protection method against cyberattacks for the objects of critical information infrastructure based on the interruption of the process of an intruder's impact. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 2, pp. 37–49 (In Russian). doi:10.31799/1684-8853-2025-2-37-49, EDN: PVFXDP

References

1. Osipov V., Kuleshov S., Zaytseva A., Levonevskiy D., Miloserdov D. Neural network forecasting of news feeds. *Expert Systems with Applications*, 2021, vol. 169, iss. 4, Article 114521. doi.org/10.1016/j.eswa.2020.114521
2. Kotenko I. V., Saenko I. B., Lauta O. S., Yuryev A. S., Zaprudnov M. S. Protest software: analysis and detection approach based on machine learning. *Cybersecurity Issues*, 2024, no. 6, pp. 42–52 (In Russian). doi:10.21681/2311-3456-2024-6-42-52, EDN: VCJRVW
3. Kotenko I. V., Saenko I. B., Bortniker P. V. Methodology for detecting network intrusions based on the integration of wavelet analysis methods and mathematical statistics. *Legal Informatics*, 2024, no. 4, pp. 23–31 (In Russian). doi:10.24412/1994-1404-2024-4-23-31, EDN: TYLWLM
4. Amma N. G. B., Selvakumar S., Velusamy R. L. A Statistical approach for detection of denial-of-service attacks in computer networks. *IEEE Transactions on Network and Service Management*, 2020, vol. 17, no. 4, pp. 2511–2522. doi:10.1109/TNSM.2020.3022799
5. *Federal'nyj zakon ot 26.07.2017 N 187-FZ "O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii"* [Federal Law of 26.07.2017 N 187-FZ "On the Security of Critical Information Infrastructure of the Russian Federation"]. Available at: https://gossopka.ru/doc/npa/federalnye-zakony/federalnyy-zakon-ot-26072017-n-187-fz-o-bezopasnosti-kriticheskoy-informacionnoy-infrastruktury-ross-37407.html (accessed 12 October 2024).
6. Kumar A., Singh R., Sharma P. A comprehensive study on web application firewalls: Technologies, challenges, and future directions. *International Journal of Web Information Systems*, 2021, vol. 17, iss. 4, pp. 393–415. doi:10.1108/IJWIS-01-2021-0005
7. Tchaikovsky S. S., *Sposob zashchity informacionno-vychislitel'noj seti ot vtorzhenij* [Method of protecting an information and computing network from intrusions]. Patent Russian Federation, no. 2758997, 2021.
8. Lipatnikov V. A., Zadboev V. A., Melekhov K. V., Shevchenko A. A. Method of increasing the security of information and telecommunications networks taking into account the use of means for determining the geolocation of an intruder. *Proceedings of Telecommunication Universities*, 2023, vol. 9, no. 4, pp. 86–96 (In Russian). doi:10.31854/1813-324X-2023-9-4-86-96, EDN: FWQHUC
9. *Metodika ocenki ugroz bezopasnosti informacii* [Information security threats assessment methodology]. Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g.html (accessed 5 November 2024).
10. Zadboev V. A., Besedin M. D., Antonov A. S. *Opredelenie cikla ataki protivnika v informacionno-vychislitel'noj seti*. In: *Problemy standartizacii, unifikacii i metrologii sistem i sredstv svyazi special'nogo naznacheniya v aspekte ih cifrovoj transformacii* [Determining the adversary attack cycle in the information and computing network. In: Scientific and technical collection "Problems of standardization, unification and metrology of special-purpose communication systems and means in terms of their digital transformation"]. Eds. V. A. Gavrin. Saint-Petersburg, Military Academy of Communications Publ., 2024, pp. 47–51 (In Russian).
11. Lipatnikov V. A., Shevchenko A. A., Melekhov K. V., Tkachev D. F. Methodology for increasing the security of the data transmission network of critical information infrastructure objects during multi-stage attacks. *Informacionno-upravlyayushchie sistemy* [Information and Control Systems], 2024, no. 1, pp. 44–55. doi:10.31799/1684-8853-2024-1-44-55, EDN: MVWIFR
12. Lipatnikov V. A., Melekhov K. V., Melikhov I. A. Features of network control in a data transmission network under conditions of multi-stage attacks. *Materialy nauchno-prakticheskoj konferencii "Tekhnologii. Innovacii. Svyaz'"* [Materials of the scientific and practical conference "Technologies. Innovations. Communications"]. Saint-Petersburg, 2023, pp. 171–174 (In Russian).
13. Sarhan M., Layeghy S., Moustafa N., Portmann M. *Netflow datasets for machine learning-based network intrusion detection systems*. In: *Big Data Technologies and Applications*. Springer International Publishing, 2021, pp. 117–135.
14. Novikova E. S., Golubev S. A. A federated learning approach to intrusion detection. *Materialy konferencii "Mezhdunarodnaya nauchnaya konferenciya po problemam upravleniya v tekhnicheskih sistemah"* [Conference materials "International Scientific Conference on Control Problems in Technical

Systems"]. Saint-Petersburg, 2023, pp. 200–203 (In Russian). doi:10.1109/CTS59431.2023.10289088, EDN: XPCAUO
15. Patil N. V., Krishna C. R., Kumar K. Distributed frameworks for detecting distributed denial of service attacks: A comprehensive review, challenges and future directions. *Concurrency and Computation: Practice and Experience*, 2021, vol. 33 no. 10, p. e6197. doi:10.1002/cpe.6197
16. Shukla P., Krishna C. R., Patil N. V. Kafka-Shield: Kafka streams-based distributed detection scheme for IoT traffic-based DDoS attacks. *Security and Privacy*, 2024, vol. 7, no. 12. doi:10.1002/spy2.416
17. Nasereddin M., ALKhamaiseh A., Qasaimeh M. A systematic review of detection and prevention techniques of SQL injection attacks. *Information Security Journal: A Global Perspective*, 2023, vol. 32, no. 4, pp. 252–265. doi:10.1080/19393555.2021.1995537
18. Jiang Y., Wu S., Yang H., Luo H., Chen Z., Yin S., Kaynak O. Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022, vol. 52, no. 12, pp. 7799–7809. doi:10.1109/TSMC.2022.3164024
19. Gong C., Zheng Z., Wu F., Shao Y., Li B. Chen G. To store or not? Online data selection for federated learning with limited storage. *ACM Web Conference*, 2023, pp. 3044–3055. doi:10.1145/3543507.3583426
20. Mulay A., Gaspard B., Naidu R., Gonzalez-Toral S., Semwal T., Manish Agrawal A. FedPerf: A practitioners' guide to performance of federated learning algorithms. *NeurIPS 2020 PMLR*, 2021, vol. 148, pp. 302–324.
21. Saputra F. A., Salman M., Hasim J. A. 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*, 2022, vol. 6, iss. 1, p. 19. doi:10.3390/bdcc6010019
22. Chen J., Gao X., Deng R., He Y., Fang C., Cheng P. Generating adversarial examples against machine learning-based intrusion detector in industrial control systems. *IEEE Transactions on Dependable and Secure Computing*, 2022, vol. 19, no. 3, pp. 1810–1825. doi:10.1109/TDSC.2020.3037500
23. Murashov D. A., Ushakova V. A. Statement and analysis of ways to solve the problem of synthesizing control programs and parameters of an information and computing network based on a polymodel description. *Aerospace Instrument-Making*, 2022, no. 8, pp. 23–32 (In Russian). doi:10.25791/aviakosmos.8.2022.1293, EDN UJXAWV

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.