Научная статья
УДК 004.056; DOI: 10.61260/2218-13X-2024-2-70-79

МОДЕЛИРОВАНИЕ НАРУШИТЕЛЯ, ИНФРАСТРУКТУРЫ И АТАК В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

✉**Чечулин Андрей Алексеевич.**
Санкт-Петербургский федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Россия
✉***andreych@bk.ru***

Аннотация. Предложены формальные модели субъектов, инфраструктуры и атак для систем информационной безопасности. Модели включают в себя описание операторов информационной безопасности, администраторов, пользователей и нарушителей, учитывая их знания, квалификацию и начальные условия. Представлена комплексная модель нарушителя, включающая начальные знания и права доступа, начальное расположение, квалификацию и цели. Также рассматриваются модели инфраструктуры, уязвимостей и методов сбора информации, что позволяет более точно прогнозировать поведение нарушителей и разрабатывать эффективные стратегии защиты. Результаты исследования показывают, что предложенные модели значительно улучшают точность оценки рисков и планирования мер безопасности, что особенно важно для критически важных информационных систем. Практическая значимость заключается в возможности применения моделей для разработки и улучшения систем защиты информационных сетей. Также представлены результаты практической реализации модели на реальных данных.

Ключевые слова: информационная безопасность, модель нарушителя, кибератаки, оценка рисков, защита сети

Для цитирования: Чечулин А.А. Моделирование нарушителя, инфраструктуры и атак в системах информационной безопасности // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 2. С. 70–79. DOI: 10.61260/2218-13X-2024-2-70-79.

Scientific article

MODELING OF THE INTRUDER, INFRASTRUCTURE AND ATTACKS IN INFORMATION SECURITY SYSTEMS

✉**Chechulin Andrey A.**
Saint-Petersburg federal research center of the Russian academy of sciences, Saint-Petersburg, Russia
✉***andreych@bk.ru***

Abstract. Formal models of subjects, infrastructure and attacks for information security systems are proposed. The models include descriptions of information security operators, administrators, users and violators, taking into account their knowledge, qualifications and initial conditions. A comprehensive intruder model is presented, including initial knowledge and access rights, initial location, qualifications and goals. Infrastructure models, vulnerabilities, and information collection methods are also considered, which makes it possible to more accurately predict the behavior of violators and develop effective protection strategies. The results of the study show that the proposed models significantly improve the accuracy of risk assessment and security planning, which is especially important for mission-critical information systems. The practical significance lies in the possibility of using models to develop and improve information network

security systems. The results of the practical implementation of the model иon real data are also presented.

Keywords: information security, intruder model, cyber attacks, risk assessment, network protection

For citation: Chechulin A.A. Modeling of the intruder, infrastructure and attacks in information security systems // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 2. P. 70–79. DOI: 10.61260/2218-13X-2024-2-70-79.

Введение

В современном мире информационные системы играют ключевую роль в функционировании большинства организаций и учреждений. Вместе с развитием технологий растут и угрозы, связанные с кибератаками. За последние годы количество и сложность кибератак значительно возросло [1], что повышает важность стоящей перед специалистами по информационной безопасности задачи по разработке эффективных методов защиты компьютерных сетей и данных, хранящихся в них.

Для обеспечения надежной защиты необходимо глубокое понимание поведения потенциальных злоумышленников и их возможных действий в различных сценариях. Одним из возможных решений для этого является моделирование поведения нарушителей. Тем не менее традиционные подходы к моделированию нарушителей часто не учитывают весь комплекс характеристик нарушителя, инфраструктуры, где он проявляет свою активность, и способов атак. Игнорирование любой из характеристик может привести к недооценке угроз и, как следствие, к недостаточной защищенности системы. В статье предлагаются формальные модели нарушителя, инфраструктуры и атак, которые учитывают все эти аспекты, что позволяет более точно прогнозировать поведение злоумышленников и разрабатывать эффективные стратегии защиты от них.

Научная новизна данной работы заключается в разработке комплексных моделей нарушителя, инфраструктуры и атак, которые включают учет новых типов виртуальных и контейнерных сетей, начальных знаний и прав доступа нарушителя, формализацию целей прочих субъектов компьютерной сети и т.д. Этот подход позволяет создавать более реалистичные и точные сценарии атак, что значительно улучшает точность оценки рисков и планирования мер безопасности. В отличие от традиционных моделей, предлагаемый подход учитывает множество факторов, влияющих на поведение нарушителя, что делает модель более гибкой и адаптивной к различным условиям.

Практическая значимость предложенной модели заключается в её применимости для разработки и улучшения систем защиты информационных сетей. Модель позволяет повысить эффективность средств защиты за счет более точного понимания поведения нарушителей и разработать целенаправленные меры противодействия на основе вероятных сценариев атак. Это особенно важно для защиты критически важных информационных систем, где последствия успешной атаки могут быть катастрофическими. Предполагается, что применение модели в реальных условиях позволит улучшить процессы оценки рисков и планирования безопасности, что приведет к созданию более надежной и устойчивой системы защиты.

Важным аспектом данного исследования является также разработка моделей инфраструктуры, уязвимостей и методов сбора информации. Эти модели дополняют основную модель нарушителя, предоставляя более полное представление о возможных сценариях атак и мерах защиты. Модель инфраструктуры описывает защищаемые компьютерные сети, включая хосты, связи между ними и системы защиты информации. Модель уязвимостей включает информацию о необходимых условиях для их реализации, а модель методов сбора информации определяет типы сбора данных и типы знаний, которые можно получить в результате.

Таким образом, предлагаемая модель нарушителя в сочетании с моделями инфраструктуры, уязвимостей и методов сбора информации представляет собой мощный инструмент для повышения уровня безопасности информационных систем. Она позволяет не только лучше понимать поведение злоумышленников [2], но и разрабатывать более эффективные стратегии защиты, что особенно важно в условиях постоянно меняющихся угроз. Актуальность данного исследования обусловлена необходимостью повышения уровня защиты информационных систем в условиях постоянно меняющихся угроз, и предлагаемые модели могут стать важным элементом обеспечения безопасности критически важных информационных систем.

Методы исследования

Аналитическое моделирование нарушителей в компьютерных сетях и атак на них представляет собой важную область исследований, направленную на защиту информационных систем. В работе [3] предлагается математическая модель имитации компьютерной атаки на распределенную информационную систему, включающая безопасные и потенциально опасные состояния системы и учитывающая вероятности реализации конкретных угроз безопасности для такой системы с заданными структурно-функциональными характеристиками и особенностями ее функционирования. В статье [4] описана графовая модель атак в беспроводных сенсорных сетях для их обнаружения.

Работа [5] предлагает гибридный подход к моделированию поведения кибер-нарушителей, комбинируя когнитивное моделирование и теорию принятия решений. В исследовании [6] представлена структура для моделирования нарушителей в анализе протоколов безопасности, что позволяет выявлять атаки автоматически. В работе [7] исследуется влияние одновременных атак на надежность сетевых систем и показано, что такие атаки могут значительно повлиять на динамику и устойчивость сетей.

Эти исследования подчеркивают важность разработки сложных моделей для анализа и защиты компьютерных сетей от разнообразных и всё более сложных кибератак.

В данном исследовании для разработки комплексной модели нарушителя, инфраструктуры и атак в системах информационной безопасности были использованы современные методологии и подходы, обеспечивающие глубокий анализ и точное описание всех компонентов модели. В работе особое внимание уделено формализации ключевых элементов, влияющих на поведение субъектов, их взаимодействие с инфраструктурой и потенциальные сценарии атак. Основной целью было создание такой модели, которая бы позволила более точно прогнозировать действия злоумышленников и разрабатывать эффективные меры защиты.

Основой для построения модели послужили данные о реальных кибератаках, статистика уязвимостей, а также информация о методах и средствах защиты информационных систем. Для систематизации и анализа этих данных использовались методы математического моделирования, включая теорию графов для описания сетевой инфраструктуры и связи между узлами. Также были применены элементы теории игр для обеспечения возможности моделирования взаимодействия между защитниками и атакующими, что позволило учесть стратегическое поведение обеих сторон.

При разработке модели нарушителя учитывались его начальные знания, права доступа, начальное расположение в сети и квалификация. Это позволило создать более детализированное и точное представление о возможностях и ограничениях злоумышленника. Для описания этих аспектов использовались методы классификации и ранжирования, что помогло выделить ключевые параметры, влияющие на успешность атакующих действий.

Модель инфраструктуры, включающая описание защищаемых компьютерных сетей, хостов, связей между ними и систем защиты информации, была разработана с использованием стандарта Common Platform Enumeration (CPE) [8]. Это позволило интегрировать данные, полученные от активных и пассивных автоматизированных средств

сбора информации, а также связать конфигурацию хостов с данными из баз уязвимостей. В результате была создана детализированная модель инфраструктуры, отражающая реальные условия эксплуатации информационных систем.

Для моделирования уязвимостей и методов их эксплуатации были использованы данные из известных баз уязвимостей, таких как Common Vulnerabilities and Exposures (CVE) [9]. На их основе были сформулированы условия для реализации уязвимостей, определены необходимые права доступа, типы доступа и уровни знаний, необходимые для их эксплуатации. Это позволило создать модель уязвимостей, включающую информацию о потенциальных последствиях их использования.

Методы сбора информации, используемые злоумышленниками, также были формализованы в рамках предлагаемой модели. Для этого были проанализированы различные техники, такие как сканирование портов, анализ программного обеспечения и другие методы, позволяющие получать информацию о состоянии системы и ее уязвимостях. Эти методы были классифицированы и описаны в модели, что позволило более точно прогнозировать поведение нарушителей на начальных этапах атаки.

Комплексная модель атак включает в себя множество сценариев, описывающих возможные последовательности действий злоумышленников. Для построения этих сценариев были использованы методы анализа сценариев и построения деревьев атак, что позволило учесть различные пути развития событий и их вероятностные характеристики, создать модель, способную учитывать множество возможных вариантов атак и их последствий.

Предлагаемый подход к моделированию нарушителей, инфраструктуры и атак позволяет более точно оценивать риски и разрабатывать эффективные меры защиты. В последующих разделах будут подробно рассмотрены все компоненты модели, описаны используемые методологии и приведены результаты практической реализации предложенных методов на реальных данных.

Модели субъектов

S – все активные субъекты, то есть сущности имеющие цели. Множество всех активных субъектов задается как $S = S_o \cup S_a \cup S_u \cup S_m$, где:

$S_o \subset S$ – множество операторов информационной безопасности. Цель операторов – минимизировать риски нарушения безопасности в защищаемой компьютерной сети. Таким образом, цель операторам информационной безопасности можно задать как $f_{se}(N) \rightarrow min$, для чего минимизируются функции защищенности компьютерной сети для всех нарушителей: $\forall s_m \in Sm \mid f_{se}(N, s_m) \rightarrow min$. Для этого оператор на основе своих знаний о проблемах безопасности компьютерной сети принимает решения, в части настроек системы безопасности, а также обновления программного и аппаратного обеспечения $N' = f_{mod}(N)$ таким образом, чтобы $f_{se}(N') < f_{se}(N)$. При этом необходимо отметить, что качество принимаемых оператором информационной безопасности решений напрямую зависит от его знаний о проблемах безопасности компьютерной сети.

$S_a \subset S$ – множество администраторов компьютерной сети. Цель администраторов – поддерживать работоспособность компьютерной сети и повышать эффективность выполняемых в ней бизнес-процессов. Администраторы чаще всего не учитывают безопасность при выполнении операций, тем не менее в большинстве случаев обновление программного обеспечения приводит к повышению защищенности компьютерной сети. Администратор на основе регламента проведения работ выполняет установку нового или обновление существующего программного и аппаратного обеспечения $N' = f_{mod}(N)$.

$S_u \subset S$ – множество пользователей компьютерной сети. Цель пользователей – выполнять действия, связанные с бизнес-процессами. Пользователи чаще всего не учитывают безопасность при выполнении операций, что в ряде случаев приводит к тому, что они могут способствовать тем или иным способом выполнению задач нарушителей.

Кроме того, необходимо отметить, что решения по безопасности практически никогда не способствуют выполнению бизнес-процессов, а иногда и мешают им.

$S_m \subset S$ – множество нарушителей. Цель нарушителя – нанести ущерб защищаемой компьютерной сети за счет несанкционированного получения прав доступа, а также нарушения конфиденциальности, целостности и доступности информации, хранящейся на хостах компьютерной сети. Модель нарушителя устанавливает ограничения на возможные атакующие действия из общего множества. Эти ограничения включают:

– знания нарушителя. Определяют сложность уязвимостей, которые нарушитель способен использовать. Эта характеристика также включает список уязвимостей нулевого дня, известных нарушителю;

– начальное расположение нарушителя в сети. Определяет доступные атакующему хосты на основе модели защищаемой сети. Существует два основных типа нарушителя по этому параметру – внешний и внутренний;

– начальные права нарушителя. Ограничивают множество атак на основе требуемых условий для их выполнения. Например, некоторые атаки могут быть осуществлены только при наличии у нарушителя прав обычного пользователя.

Элемент множества нарушителей задается как $s_m = <S_0, H_0, K, Kn>$, где S_0 – начальные знания нарушителя о каждом хосте анализируемой компьютерной сети и права доступа, которыми этот нарушитель обладает; $H_0 \subset H$ – хосты, к которым нарушитель имеет физический или удаленный доступ до начала атак. Если нарушитель является внешним, то H_0 представляет собой список хостов, доступных из внешних сетей, например, из сети Интернет; K – квалификация нарушителя, включающая классы или списки доступных ему атакующих действий, основанных на уязвимостях разной сложности и различных методах сбора информации.

Рассмотрим элементы модели нарушителя более подробно.

Модель нарушителя должна содержать информацию о начальных условиях и квалификации нарушителя. Начальные условия задаются как список хостов ($H_0 \subset H$), с которых нарушитель может начать выполнение атакующих действий (если нарушитель начинает свои действия не с компьютера, которым он владеет, первые атаки направлены на этот же хост) и как список прав нарушителя для каждого хоста: $S_0 = H \times <V_{m,h}, Rights>$, где $V_{m,h} \subset V$ – список уязвимостей хоста h известных нарушителю; $Rights = \{None, User, Administrator\}$). Квалификация нарушителя обозначается как K и определяется как $K = <Kl, V_m, V0_m>$, где Kl – уровень квалификации нарушителя ($Kl = \{high, medium, low\}$; $V_m \subset V$ – список известных уязвимостей, которые нарушитель может эксплуатировать; $V0_m \subset V$ – список известных нарушителю уязвимостей нулевого дня.

Модели инфраструктуры

N – это множество компьютерных сетей, каждая из которых содержит информацию о хостах и связях между ними. Множество защищаемых компьютерных сетей задается как $N = <H_n, C_n, P_n>$, где H_n – множество хостов сети n; C_n – множество связей между хостами, отражающих возможные способы взаимодействия в сети n.

H – это множество хостов, каждый из которых содержит информацию об установленном программно-аппаратном обеспечении (операционная система, сервисы и т.д.), о вложенных компьютерных сетях (например, для гипервизоров и систем оркестрами контейнеров) и о системах безопасности. Данная модель учитывает стандарт (CPE), что позволяет использовать для построения модели данные, полученные от активных и пассивных автоматизированных средств сбора информации, а также связать конфигурацию хоста с данными из баз уязвимостей. Множество хостов задается как $H = <CN_h, N_h, P_h>$, где:

CN – это множество всего известного программно-аппаратного обеспечения; $CN_h \subset CN$ – это программно-аппаратное обеспечение, используемое в конкретном хосте h. Элемент множества программно-аппаратного обеспечения $cn_i \in CN$, описывающий один

из элементов программно-аппаратной конфигурации, имеет вид: $cn_i = <vendor, product, version, productType>$, где $vendor \in Vendors$ и определяет имя разработчика продукта; $product \in Products$ – название продукта; $version \in Versions$ – версию продукта; $productType \in ProductTypes$ – тип продукта ($ProductTypes = \{Software, Hardware, OS\}$). Множества *Vendors*, *Products* и *Versions* определяют словари возможных разработчиков, программно-аппаратных продуктов, созданных этими разработчиками, и версии продуктов соответственно.

N_h – компьютерная сеть, вложенная в хост. Такая ситуация возникает, когда на хосте установлен гипервизор или оркестратор с виртуальными хостами.

C – это множество связей между хостами, каждая из которых содержит информацию о том, какие хосты ей связаны, типах связей, отражающих возможные способы взаимодействия и о системах безопасности. Множество хостов задается как $C = <H_c, CT_c, P_c>$, где:

$H_c \subset H$ – это множество хостов, связанных связью c.

CT – это множество типов связей (например, обычный сетевой доступ, отношения функциональной зависимости и отношения доверия), $CT_c \subset CT$ – множество типов связей конкретной связи c. $CT = \{physical, functional, trust\}$.

P – это множество всех известных систем защиты информации, каждая из которых содержит информацию о том, использование каких атак, использующих уязвимости или методы сбора информации, она может заблокировать. $P_h \subset P$ – это системы безопасности, установленные на хосте h и действие которых распространяется только на этот хост. $P_c \subset P$ – это системы безопасности, установленные на связь c и действие которых распространяется только на эту связь. $P_n \subset P$ – это системы безопасности, установленные в сети n и действие которых распространяется только на эту сеть и на все входящие в нее хосты и связи. Множество всех систем защиты информации задается как $P = <V_p, SC_p>$, где $V_p \subset V$ – это множество заблокированных уязвимостей; $SP_p \subset SP$ – это множество заблокированных методов сбора информации.

V – это множество уязвимостей, каждая из которых содержит информацию о необходимых условиях для реализации уязвимости (квалификация нарушителя, доступные тип доступа и права доступа), а также результат ее использования (полученные права доступа и уровень нарушения конфиденциальности, целостности и доступности информации). Элемент множества уязвимостей $v_i \in V$, описывающий одну уязвимость, имеет вид: $v_i = <required\_rights, required\_access, required\_knowledge, gained\_rights, impact>$, где $required\_rights \in Rights$ и $gained\_rights \in Rights$ ($Rights = \{None, User, Administrator\}$) определяют необходимые для реализации и получаемые в результате ее права доступа соответственно; $required\_access \in Access$ ($Access = \{Physical, Local, AdjacentNetwork, Network\}$) определяет необходимый для реализации уязвимости тип доступа; $required\_knowledge \in Knowledge$ определяет необходимый для реализации уязвимости уровень знаний; *impact* – версию продукта; $productType \in ProductTypes$ – тип продукта ($ProductTypes = \{Software, Hardware, OS\}$). Множества *Vendors*, *Products* и *Versions* определяют словари возможных разработчиков, программно-аппаратных продуктов, созданных этими разработчиками, и версии продуктов, соответственно.

SP – это множество методов сбора информации, каждый из которых содержит информацию о том, какой тип сбора он реализует, и какие типы знания можно получить в итоге выполнения этого метода. Элемент множества методов сбора $sp_i \in SP$, описывающий один метод сбора, имеет вид: $sp_i = <collection\_type, required\_access, knowledge\_type>$, где $collection\_type \in CollectionType$ ($CollectionType = \{ping, port\_scan, software\_analysis, ..\}$) определяет тип сбора данных; $required\_access \in Access$ ($Access = \{Physical, Local, AdjacentNetwork, Network\}$) определяет необходимый для реализации сбора информации тип доступа; $knowledge\_type \in KnowledgeType$ ($KnowledgeType = \{connected\_hosts, software\_recognition\}$) определяет тип знаний, которые можно получить.

Модели атак

Модель атаки включает множество сценариев возможных атак на сеть. Для каждого сценария описываются его составляющие атакующие действия, использующие уязвимости и методы атак.

AA – это множество атакующих действий, каждое из которых содержит информацию об используемых уязвимостях и методах сбора информации. Множество всех атакующих действий задается как $AA = AA_v \cup AA_{sp}$, где:

AA_v – это множество атакующих действий, использующих уязвимость. Элемент множества атакующих действий, использующий уязвимость, задается как $aa_v = <h1, h2, v>$, где h_1 – хост-источник атаки; h_2 – хост-цель атаки; v – используемая в рамках этой атаки уязвимость. Необходимо отметить, что хост-источник атаки и хост-цель атаки могут совпадать, и тогда данное атакующее действие будет являться внутренним для данного хоста.

AA_{sp} – это множество атакующих действий, использующих методы сбора информации. Элемент множества атакующих действий, использующий метод сбора информации задается как $aa_{sp} = <h1, h2, sp>$, где h_1 – хост-источник атаки; h_2 – хост-цель атаки; *sp* – используемый в рамках этой атаки метод сбора информации.

AP – это множество всех возможных путей атаки, где каждый элемент представляет собой упорядоченную последовательность атакующих действий, которая задается как $ap = \{aa_1, aa_2, \ldots, aa_m\}$.

Основные результаты

Практическая реализация предложенной модели нарушителя, инфраструктуры и атак была проведена с целью оценки её эффективности в реальных условиях и подтверждения её применимости для улучшения систем защиты информационных сетей. В этом разделе представлены основные шаги по внедрению модели, а также результаты её применения на практике.

Для практической реализации модели были использованы данные из реальной компьютерной сети научной организации, включающей несколько сотен хостов и разнообразные связи между ними. Данные о конфигурации сети и установленных программных и аппаратных средствах безопасности были собраны с использованием автоматизированных средств мониторинга и анализа, соответствующих стандарту CPE. Это позволило создать детализированную модель инфраструктуры, которая точно отражает текущие условия эксплуатации системы.

С помощью разработанной модели нарушителя, включающей начальные знания, права доступа, начальное расположение в сети, квалификацию и цели, были сформированы различные сценарии возможных атак. Например, был смоделирован внешний нарушитель, имеющий ограниченные права доступа и начальные знания о публично доступных хостах. На основе этой модели были разработаны сценарии атак, включающие сбор информации, эксплуатацию уязвимостей и получение доступа к критическим системам.

Собранные данные о системе безопасности были использованы для актуализации модели уязвимостей. Были проанализированы известные уязвимости из базы данных CVE, что позволило определить потенциальные угрозы и необходимые условия для их эксплуатации. Внедрение этой информации в модель позволило создать более точные и реалистичные сценарии атак, которые учитывают текущие уязвимости системы.

На основе разработанных сценариев атак были проведены тестирования системы с использованием методов тестирования на проникновение (пентест). Это позволило выявить ранее неучтенные уязвимости и оценить последствия их эксплуатации. Например, в одном из сценариев была смоделирована атака внешнего нарушителя. Атака включала сбор

информации о конфигурации системы, выявление уязвимостей в используемом программном обеспечении и получение административных прав доступа.

Результаты тестирования показали, что предложенная модель позволяет выявить уязвимости, которые могли бы остаться незамеченными при использовании традиционных методов оценки безопасности. Это подтвердило эффективность предложенной модели в реальных условиях.

Применение предложенной модели позволило не только выявить уязвимости, но и разработать меры по их устранению. Например, на основе полученных данных была обновлена политика безопасности и проведено обновление уязвимого программного обеспечения. В результате этих действий уровень защищенности организации значительно повысился.

Предполагается, что долгосрочное использование предложенной модели приведет к общему повышению эффективности обеспечения безопасности информационных систем организации. Регулярное обновление данных о конфигурации системы и уязвимостях, а также периодическое проведение тестирования на основе разработанных сценариев атак позволят поддерживать высокий уровень защиты и оперативно реагировать на новые угрозы.

Примеры успешного применения модели в реальных условиях подтверждают её практическую значимость. Модель нарушителя, инфраструктуры и атак позволяет не только выявлять существующие уязвимости, но и прогнозировать потенциальные угрозы, что является ключевым фактором в обеспечении информационной безопасности.

Заключение

В данной статье были предложены комплексные модели нарушителя, инфраструктуры и атак для систем информационной безопасности. Модели включают формализацию ключевых элементов, влияющих на поведение субъектов, их взаимодействие с инфраструктурой и возможные сценарии атак. Разработанные модели субъектов, нарушителей, инфраструктуры, уязвимостей и методов сбора информации позволяют более точно прогнозировать поведение злоумышленников и разрабатывать эффективные стратегии защиты.

Важным достижением данной работы является интеграция моделей нарушителей с моделями инфраструктуры и уязвимостей. Такой подход позволяет получать более точные оценки рисков и разработать меры противодействия, адаптированные к конкретным условиям и особенностям защищаемых систем. Модель инфраструктуры, основанная на стандарте CPE, обеспечивает возможность актуализации данных о конфигурации системы и уязвимостях с помощью традиционных средств сбора данных, что повышает оперативность и точность реагирования на угрозы.

В дальнейшем планируется расширение предложенной модели за счет включения новых параметров и элементов, что позволит еще более точно моделировать поведение нарушителей и прогнозировать потенциальные угрозы. Также будет разработан комплекс автоматизированных инструментов для упрощения процесса применения моделей в реальных условиях и повышения её эффективности. Кроме того, планируется проведение анализа возможностей применения полученных моделей для решения смежных задач, например, безопасной разработки программного и аппаратного обеспечения [10].

Список источников

1. Актуальные киберугрозы: I квартал 2024 года: отчет компании Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (дата обращения: 04.04.2024).

2. Проблемные вопросы информационной безопасности киберфизических систем / Д.С. Левшун [и др.] // Информатика и автоматизация. 2020. № 5 (19). С. 1050–1088.

3. Моделирование компьютерных атак на распределенную информационную систему / А.А. Корниенко [и др.] // Известия Петербургского университета путей сообщения. 2018. Т. 15. № 4. С. 613–628.

4. Жукабаева Т.К., Десницкий В.А., Марденов Е.М. Аналитическое моделирование атакующих воздействий в беспроводных сенсорных сетях для решения задач обнаружения атак // Информатизация и связь. 2023. № 3. С. 98–105.

5. Hybrid Modeling of Cyber Adversary Behavior: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation / A. Sliva [et al.] // Lecture Notes in Computer Science. 2017. P. 133–138.

6. Basin D., Cremers C. Modeling and Analyzing Security in the Presence of Compromising Adversaries: Proceedings of the 15th European Symposium on Research in Computer Security, 2010. P. 340–356.

7. Da G., Xu M., Zhao P. Modeling Network Systems Under Simultaneous Cyber-Attacks: IEEE Transactions on Reliability. 2019. Vol. 68. P. 971–984.

8. Common Platform Enumeration (CPE). URL: https://nvd.nist.gov/products/cpe (дата обращения: 04.04.2024).

9. Common Vulnerabilities and Exposures (CVE). URL: https://cve.mitre.org/ (дата обращения: 04.04.2024).

10. Desnitsky V.A., Kotenko I.V., Chechulin A.A. Configuration-based approach to embedded device security // Lecture Notes in Computer Science. 2012. Vol. 7531. LNCS. P. 270–285.

References

1. Aktual'nye kiberugrozy: I kvartal 2024 goda: otchet kompanii Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (data obrashcheniya: 04.04.2024).

2. Problemnye voprosy informacionnoj bezopasnosti kiberfizicheskih sistem / D.S. Levshun [i dr.] // Informatika i avtomatizaciya. 2020. № 5 (19). S. 1050–1088.

3. Modelirovanie komp'yuternyh atak na raspredelennuyu informacionnuyu sistemu / A.A. Kornienko [i dr.] // Izvestiya Peterburgskogo universiteta putej soobshcheniya. 2018. T. 15. № 4. S. 613–628.

4. Zhukabaeva T.K., Desnickij V.A., Mardenov E.M. Analiticheskoe modelirovanie atakuyushchih vozdejstvij v besprovodnyh sensornyh setyah dlya resheniya zadach obnaruzheniya atak // Informatizaciya i svyaz'. 2023. № 3. S. 98–105.

5. Hybrid Modeling of Cyber Adversary Behavior: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation / A. Sliva [et al.] // Lecture Notes in Computer Science. 2017. P. 133–138.

6. Basin D., Cremers C. Modeling and Analyzing Security in the Presence of Compromising Adversaries: Proceedings of the 15th European Symposium on Research in Computer Security, 2010. P. 340–356.

7. Da G., Xu M., Zhao P. Modeling Network Systems Under Simultaneous Cyber-Attacks: IEEE Transactions on Reliability. 2019. Vol. 68. P. 971–984.

8. Common Platform Enumeration (CPE). URL: https://nvd.nist.gov/products/cpe (data obrashcheniya: 04.04.2024).

9. Common Vulnerabilities and Exposures (CVE). URL: https://cve.mitre.org/ (data obrashcheniya: 04.04.2024).

10. Desnitsky V.A., Kotenko I.V., Chechulin A.A. Configuration-based approach to embedded device security // Lecture Notes in Computer Science. 2012. Vol. 7531. LNCS. P. 270–285.

Информация о статье:
Статья поступила в редакцию: 28.04.2024; одобрена после рецензирования: 10.05.2024;
принята к публикации: 25.05.2024

The information about article:
The article was submitted to the editorial office: 28.04.2024; approved after review: 10.05.2024;
accepted for publication: 25.05.2024

Информация об авторах:
Чечулин Андрей Алексеевич, ведущий научный сотрудник Санкт-Петербургского федерального исследовательского центра Российской академии наук (199178, Санкт-Петербург, 14 линия В.О., д. 39), кандидат технических наук, доцент, e-mail: andreych@bk.ru, https://orcid.org/0000-0001-7056-6972, SPIN-code: 1632-0938

Information about the authors:
Chechulin Andrey A., leading researcher at the Saint-Petersburg federal research center of the Russian academy of sciences (199178, Saint-Petersburg, 14 line V.O., ave. 39), candidate of technical sciences, associate professor, e-mail: andreych@bk.ru, https://orcid.org/0000-0001-7056-6972, SPIN: 1632-0938