10. SIEM i Log Management: obzor resheniy dlya upravleniya bezopasnost'yu [SIEM and Log Management: an overview of security management solutions]. Cloudnetworks.ru. Available at: https://cloudnetworks.ru/inf-bezopasnost/siem-log-management/ (accessed 10 December 2024).
11. *Lacity M.C., Willcocks L.P.* Robotic Process Automation and Risk Mitigation. Palgrave Macmillan, 2020, 213 p.
12. *Richards M*. Fundamentals of Software Architecture: An Engineering Approach. O'Reilly Media, 2020, 412 p.
13. *Weske M.* Business Process Management: Concepts, Languages, Architectures. 3rd ed. Springer, 2020, 03 p.
14. *van der Aalst W.M. et al.* Object-Centric Process Mining: Dealing with Divergence and Convergence in Data, *ACM Transactions on Management Information Systems,* 2023, Vol. 14, No. 2, pp. 1-35.
15. *Mansar S. L., Reijers H.A.* Best Practices in Business Process Redesign, *Business Process Management Journal,* 2023, Vol. 15, No. 4, pp. 38-50.
16. *Koci V., Horalek J., Kuchar M.* A review of license plate recognition methods based on deep learning, *IEEE Access,* 2023, Vol. 11, pp. 54311-54330.
17. *Syed R., Suriadi S., Adams M., Bandara W.* A systematic literature review of the challenges of implementing Robotic Process Automation (RPA), *Communications of the Association for Information Systems,* 2020, Vol. 47, No. 1, pp. 12.
18. Top Strategic Technology Trends 2024, *Gartner,* 2023. Available at: https://www.gartner.com/en/information-technology/insights/top-technology-trends (accessed 10 December 2024).
19. Gartner. BPM Trends. Available at: https://www.gartner.com (accessed 10 December 2024).
20. *Casino F., Dasaklis T. K., Patsakis C.* A systematic literature review of blockchain-based applications: Current status, classification and open issues, *Telematics and Informatics,* 2020, Vol. 52, pp. 101412.

Анпилогова Анастасия Евгеньева – ЮРИУ РАНХиГС; e-mail: abramoves.ae@gmail.com; г. Ростов-на-Дону, Россия; тел.: +79889402282; экономический факультет (экономическая безопасность); студент.

Анпилогов Виктор Александрович – Южный федеральный университет, e-mail: vanpilogov@sfedu.ru; г. Таганрог, Россия; тел.: +79885744400; кафедра вычислительной техники; магистрант.

Anpilogova Anastasia Evgenyeva – URUI RANEPA; e-mail: abramoves.ae@gmail.com; Rostov-on-Don, Russia; phone: +79889402282; Faculty of Economics (Economic Security); student.

Anpilogov Viktor Aleksandrovich – Southern Federal University; e-mail: vanpilogov@sfedu.ru; Taganrog, Russia; phone: +79885744400; the Department of Computer Science; master's student.

УДК 004.056 DOI 10.18522/2311-3103-2025-3-41-54

И.А. Ерёмин, А.Е. Якушина, И.Л. Щербов

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ ПОСТРОЕНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

В рамках данного исследования была детально проанализирована типовая структура объекта информатизации, что позволило квалифицированным специалистам глубже понять механизмы и аспекты, посредством которых различные категории объектов и субъектов обработки информации, которые могут подвергаться угрозам безопасности. Основным механизмом построения комплексной системы защиты информации является модель угроз. Данная модель направлена на выявление и идентификацию потенциальных угроз, их последующий анализ и минимизации рисков их реализации, связанных с нанесением ущерба объекту информатизации. В рамках настоящего исследования для построения модели угроз рассмотрены отечественная база знаний ФСТЭК и международные базы знаний ATT&CK и CAPEC, содержащие в себе исчерпывающую информацию о тактиках и техниках, применяемых злоумышленниками при осуществлении атак на объекты информатизации. В процессе исследования были детально классифицированы различные тактики, используемые злоумышленниками. Особое внимание уделялось определению основных тактик, определяющих точки входа объекта информатизации, которые используются для дальнейшего проведения атаки. В контексте разработки эффективной модели угроз представляется целесообразным проведение комплексного анализа данных, содержащихся в базах знаний, и их

последующего совместного использования в процессе построения модели угроз на объектах информатизации. Данный подход позволяет систематизировать и структурировать информацию, что способствует более точному и обоснованному построению модели осуществления потенциальных угроз на разных этапах атаки на объект информатизации. Для построения комплексной системы защиты информации была рассмотрена система поддержки принятия решений. Проведен анализ современных научных исследований, посвященных применяемым методам при построении систем поддержки. В результате работы была приведена взаимосвязь между базами знаний тактик и техник, а также общеизвестных уязвимостей методом онтологии, которая позволяет построить модель комплексной атаки угрозы, и определить объекты воздействия, на которые воздействует злоумышленник на различных этапах комплексной атаки, критичность применяемой уязвимости и платформы, на которой данная уязвимость реализуема, и определение негативных последствий.

Объект информатизации; комплексная система защиты информации; модель угроз; тактики и техники атак; неопределенность данных; система поддержки принятия решений.

I.A. Eremin, A.E. Yakushina, . I.L. Sherbov

MODELING OF SECURITY THREATS FOR BUILDING A COMPREHENSIVE INFORMATION PROTECTION SYSTEM AT OBJECT OF INFORMATIZATION

Within the framework of this study, the typical structure of the informatization facility was analyzed in detail, which allowed qualified specialists to better understand the mechanisms and aspects through which various categories of objects and subjects of information processing that may be subject to security threats. The main mechanism for building a comprehensive information security system is the threat model. This model is aimed at identifying and identifying potential threats, their subsequent analysis and minimizing the risks of their implementation associated with damage to the informatization facility. In the framework of this study, the domestic FSTEC knowledge base and the international ATT&CK and CAPEC knowledge bases are considered to build a threat model. They contain comprehensive information about the tactics and techniques used by intruders in carrying out attacks on informatization facilities. In the course of the research, various tactics used by the attackers were classified in detail. Special attention was paid to the definition of the main tactics that determine the entry points of the informatization object, which are used to further carry out the attack. In the context of developing an effective threat model, it seems advisable to conduct a comprehensive analysis of the data contained in knowledge bases and their subsequent joint use in the process of building a threat model at informatization facilities. This approach makes it possible to systematize and structure information, which contributes to a more accurate and reasonable construction of a model for the implementation of potential threats at different stages of an attack on an informatization facility. To build a comprehensive information security system, a decision support system was considered. The analysis of modern scientific research devoted to the applied methods in the construction of support systems is carried out. As a result of the work, the relationship between knowledge bases of tactics and techniques, as well as well-known vulnerabilities, was shown using the ontology method, which allows us to build a model of a complex threat attack, and identify the targets affected by an attacker at various stages of a complex attack, the criticality of the vulnerability used and the platform on which this vulnerability is implemented, and the definition of negative consequences.

Object of informatization, an integrated information security system, a threat model, tactics and techniques of attacks, data uncertainty, a decision support system.

Введение. Указом Президента Российской Федерации от 2 июля 2021 г. № 400 утверждена стратегия национальной безопасности Российской Федерации. Информационная безопасность впервые выделена в качестве одного из стратегических национальных приоритетов, направленных на обеспечение и защиту национальных интересов Российской Федерации. В стратегии целью обеспечения информационной безопасности определено укрепление суверенитета Российской Федерации в информационном пространстве [1].

Состояние информационной безопасности характеризуется постоянным, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности государства [2].

Защита информации на объектах информатизации (ОИ) с целью противодействия киберпреступности является составной частью обеспечения национальной безопасности. Решение данной задачи базируется на проведении детального анализа действующего ОИ и осуществлении оценки риска для обеспечения защиты уязвимостей активов от вероятных угроз [3].

Согласно ГОСТ Р 51275-2006, объект информатизации (ОИ) – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [4].

В общем виде структура ОИ представлена на рис. 1.

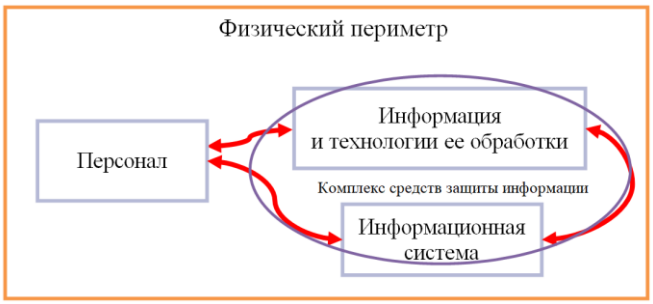

Рис. 1. Структура объекта информатизации

Учитывая, что построение комплексной системы защиты информации (КСЗИ) на ОИ начинается с инвентаризации активов, рассмотрим их более детально.

1. Физический периметр определяется как система, включающий в себя нормативно-правовые документы, инженерно-технические конструкции, структурные подразделения, целью которых является обеспечение физической безопасности объекта информатизации. Данная система направлена на предотвращение несанкционированного проникновения в здания (на территорию), минимизацию рисков повреждения инфраструктуры и нейтрализацию внешних угроз.

2. Информационная система представляют собой совокупность взаимосвязанных элементов и включает в себя аппаратные средства, сетевое оборудование, программно-аппаратные платформы и прикладное программное обеспечение. Её функциональное назначение заключается в выполнении основных задач, направленных на выполнение уставных функций организации.

3. Информация и технологии её обработки взаимосвязана с вычислительной системой, выступая ключевым активом для выполнения как производственных, так и управленческих функций организации. Эта взаимозависимость обусловлена тем, что процессы обработки, хранения и передачи данных реализуются исключительно через работу программных и аппаратно-программных компонентов вычислительной системы.

4. КСЗИ включает в себя специализированные технические устройства, программные обеспечения и программно-аппаратные компоненты выполняющие функции защиты информации от утечки по техническим каналам и защиты от несанкционированного доступа.

5. Персонал включает в себя, работников, связанных с организацией договорными отношениями (трудовой договор, контракт и т.п.). К этой категории следует относить как работников, числящихся по штатному расписанию организации, так и работников других учреждений, выполняющих в организации те или иные виды работ. Это могут быть работники частных охранных компаний, клиринговых компаний и т.д.

Каждый актив ОИ может иметь уязвимости, при условии внешнего воздействия (реализации угрозы), на которые возможно наступление негативных последствий, выраженных в нарушении конфиденциальности, целостности или доступности информации.

Противодействие подобным внешним воздействиям (угрозам) требует осуществление системного анализа и декомпозиции целей атакующего, исследования функциональных возможностей вредоносного программного обеспечения (ВПО) и реконструкцию последовательности его воздействия на активы ОИ, шаблонов атак и используемых тактик и техник, уязвимостей программного обеспечения и оборудования. Результатом данного анализа является формализованный документ – модель угроз (МУ). Данная модель является основополагающим этапом проектирования многоуровневых защитных механизмов, направленных на блокировку конкретных векторов атак, минимизацию реализации угроз и снижение рисков нанесения ущерба организации.

Методы и методики исследования. В данном исследовании проведен анализ тактик и техник атак на объекты информатизации применяемых злоумышленниками, с целью максимально эффективного использования предоставленной в них информации, для формирования модели угроз информации во время проектирования КСЗИ на ОИ.

В методическом документе ФСТЭК «Методика оценки угроз безопасности» от 5 февраля 2021 г. определен перечень тактик и техник угроз (ТТУ), который описывает возможную классификацию тактик и техник злоумышленника при применении им атак на объекты воздействий информационной инфраструктуры. Данная классификация адаптирована к национальным требованиям и регуляторным нормам, сохраняя концептуальное сходство с международными аналогами.

Тактика – это цель, которую ставит перед собой злоумышленник на различных этапах, при осуществлении атаки на информационную инфраструктуру. Техника описывает, конкретные методы и приемы того, как злоумышленник добиться цели применения выбранной тактики.

Проанализируем тактики, применяемые злоумышленниками отображенные в перечне ТТУ ФСТЭК (табл. 1) [5].

Таблица 1

Анализ тактик ТТУ ФСТЭК

№ П/п	Тактика	Цель	Описание
Т1	Сбор информации о системах и сетях	Получении информации для планирования последующих этапов атаки	Злоумышленник применяет пассивные и активные методы для сбора технических данных о целевой инфраструктуре
Т2	Получение первоначального доступа к компонентам систем и сетей	Создание точки входа для дальнейшего продвижения в сети	Предполагает эксплуатацию уязвимостей сетевых служб, фишинговых атак или подбора учетных данных для получения доступа к узлам инфраструктуры
Т3	Внедрение и исполнение ВПО в система и сетях	Эксплуатация ВПО и направлена на выполнение несанкционированных операций на локальных или удаленных ресурсах	Злоумышленник осуществляет инъекцию вредоносного кода в целевую систему через уязвимые интерфейсы или обманные методы

Окончание табл. 1

№ П/п	Тактика	Цель	Описание
Т4	Закрепление (сохранение доступа) в системе или сети	Получения постоянного доступа в целевую систему	После получения первоначального доступа, злоумышленник пытается закрепиться в системе посредством кражи существующих учетных данных или созданию новых учетных данных, добавление ВПО в автозагрузку
Т5	Управление ВПО и (или) компонентами, к которым ранее был получен доступ	Автоматизация управления ВПО и выполнения удаленных команд	После успешного закрепления на узле, злоумышленник, организует взаимодействие между скомпрометированным узлом и командным сервером злоумышленника
Т6	Повышение привилегий по доступу к компонентам систем и сетей	Выполнение действий требующих повышенных разрешений	Повышение привилегий состоит из методов, которые злоумышленники используют для получения разрешений более высокого уровня в системе или сети
Т7	Сокрытие действий и применяемых при этом средств от обнаружения	Скрытие действий атаки на всем этапе компрометации.	Скрытие от обнаружения и предотвращения средствами защиты
Т8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям	Распространение доступа на другие компоненты инфраструктуры	Злоумышленник может использовать различные методы для кражи данных с узла, при этом используя методы по предотвращению обнаружения и защиты
Т9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз	Нарушение конфиденциальности информации	Злоумышленник может использовать различные методы для кражи данных с узла, при этом используя методы по предотвращению обнаружения и защиты
Т10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Нарушение доступности, целостности, конфиденциальности	Достижение злоумышленником конечной цели по нарушению доступности узла или нарушении целостности данных

Из проведенного анализа тактик можно сделать вывод, что тактики сбора информации, получения первоначального доступа, закрепления и распространения, создают необходимые условия для реализации последующих тактик, которые будут направлены на реализацию таких целей, как нарушение целостности, доступности и конфиденциально-

сти. Матрица MITTRE ATT&CK, как и перечень ТТУ ФСТЭК описывает тактики и техники, применяемые злоумышленниками, но кроме того в ней еще представлены процедуры, которые описывают, конкретные инструменты для реализации угроз на разных платформах. Дополнительно в матрице приводится информация о преступных группировках (хакерские кампании) и ВПО, используемое ими, методы по отслеживанию реализации техник и снижения риска их реализации. Структура матрицы MITTRE приведена на рис. 2 [6].

Рис. 2. Структура матрицы MITTRE ATT&CK

В перечне ФСТЭК (Приложение 11 Методики оценки угроз безопасности информации) объединены некоторые тактические категории, представленные в матрице MITTRE ATT&CK. Так в перечне ФСТЭК три тактики из матрицы MITTRE, а именно подготовка ресурсов, сбор данных учетных данных и сбор информации о внутренней инфраструктуре, частично объединены с тактиками сбора информации (Т1), повышения привилегий (Т6) и распространения доступа (Т8). Тактика сбор и вывод информации (Т9) из перечня ФСТЭК в свою очередь включает в себя сразу две тактики ATT&CK – сбор данных и эксфильтрацию данных. Техники из перечня ТТУ ФСТЭК имеют некоторое пересечение с матрицей MITTRE. Так несколько аналогичных техник объединены в одну и сгруппированы по определенным тактикам, что упрощает анализ применяемых техник злоумышленниками при определенной тактике, но предоставляет меньшую детализацию возможных действий злоумышленника, и соответственно усложняет подбор смягчающих мер и способов обнаружения. Так одна техника описанная в ТТУ ФСТЭК может содержать в себе 10-15 аналогичных техник из матрицы MITTRE. При этом у ФСТЭК есть и свои уникальные техники (Т3.7 – Подмена файлов легитимных программ и библиотек непосредственно в системе), которые не встречаются в матрице MITTRE.

Рассмотрим, например технику Т4.1 ФСТЭК, которая описывает несанкционированное создание или кражу существующих учетных данных, и найдем ей аналогичные техники в матрице MITTRE. На рис. 3 приведены техники из матрицы MITTRE и тактики атак, при которых они могут быть применены. CAPEC – база описаний шаблонов последовательных атак, используемые злоумышленниками для негативного воздействия при использовании уязвимостей активов ОИ. Шаблоны классифицированы на 9 групп механизмов атак. В каждой группе механизма описаны соответствующие шаблоны атак.

Каждый шаблон имеет описание атаки, ближайшие атаки соответствующего механизма атак и объекты воздействия [7]. Объекты воздействия CAPEC частично соответствует модели объектов воздействия ФСТЭК. Анализ соответствия объектов воздействия приведен в табл. 2.

Для моделирования угроз безопасности необходимо сопоставление возможных негативных последствий угроз безопасности информации (УБИ), объектов воздействия угроз, общеизвестных уязвимостей, тактики и техники реализаций угроз, и шаблоны атак. Из проведенного анализа можно сделать вывод о целесообразности сочетания рассмотренных баз знаний о тактиках, техниках и шаблонов внешних воздействий злоумышленников. Основными исходными данными для общеизвестных уязвимостей и не-

достатков программного и аппаратного обеспечения выступают следующие источники: база данных угроз (БДУ) ФСТЭК, CWE и CVE [8-10]. Для оценки уязвимостей используется шкала CVSS [11], которая определяет их уровень критичности и числовую оценку – критический (9.0-10.0), высокий (7.0-8.9), средний (4.0-4.9), низкий (0.1-3.9).

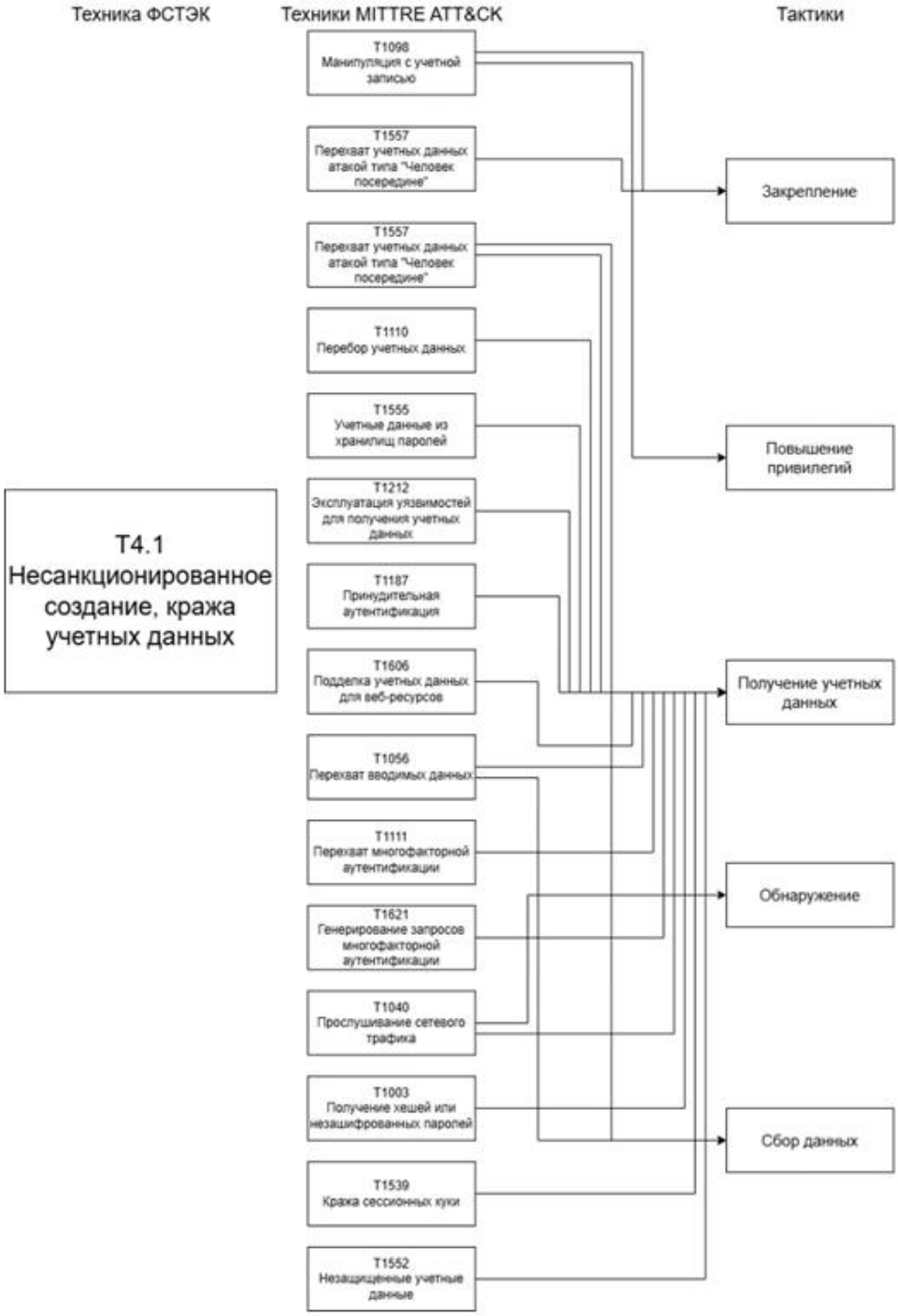

Рис. 3. Тактики и техники матрицы MITTRE

Таблица 2

Соответствия объектов воздействия ФСТЭК и CAPEC

Уровень воздействия ФСТЭК	Категория CAPEC	Примеры интерфейсов воздействия	Примечание
Аппаратный	Аппаратное обеспечение	USB порты, RJ-45	Полное соответствие. Охватывает физические устройства, микросхемы
Сетевой	Коммуникации	TCP/UDP порты	Полное соответствие. Фокус на сетевые протоколы и передачу данных
Системный	Программное обеспечение	Ядро ОС	Частичное соответствие. CAPEC включает системное ПО в общую категорию «Software»
Прикладной	Программное обеспечение	API	Частичное соответствие. CAPEC включает прикладное ПО в общую категорию «Software»
Пользовательский	Социальная инженерия	Электронная почта	Полное соответствие. Оба стандарта выделяют человеческий фактор как цель
-	Цепочка поставок	Библиотека обновления ПО	Описание объектов воздействия определяются с учетом состава и содержания услуг, предоставляемых поставщиком услуг
-	Физическая безопасность	Считыватели RFID	Нет соответствия в модели ФСТЭК

Учитывая вышеизложенное, можно сделать вывод, что для принятия обоснованного решения по организации защиты ОИ необходимо обработать и систематизировать значительный объём информации, охватывающей различные области знаний, на основе которой можно будет спроектировать эффективную систему защиты информации.

Для того, чтобы минимизировать вероятность принятия ошибочного решения, вызванного человеческим фактором, в условиях современного развития информационных технологий целесообразно при разработке системы защиты ОИ использовать системы поддержки принятия решений (СППР) [12]. При этом необходимо отметить, что некоторая часть информации, накопленной в базах знаний системы, имеет свойство неопределенности, что в целом характерно для задач, которые необходимо решать в условиях большого объема исходной информации, необходимой для принятия решения.

Условно источники неопределенности, возникающие при создании и эксплуатации СППР, можно разделить на следующие категории:

- недостаточная база знаний (данных) в предметной области;
- недостаточная информация о конкретной ситуации;
- неоднозначность в формулировании терминов (определений).

Рис. 4. Источники неопределенностей

Возникновение неопределенностей обусловлено, как объективными, так и субъективными факторами.

К объективным факторам можно отнести:

- несовершенство (пробелы) в действующем законодательстве;
- применение документов, носящих рекомендательный характер;
- неоднозначность (отсутствие единого подхода баз данных) в классификации применяемых действий злоумышленников;
- появление новых уязвимостей;
- существование уязвимостей нулевого дня и т.п.

К субъективным факторам можно отнести:

- отличающиеся мнения экспертов в области знаний;
- некорректное отображение информации при её передаче в цепочке знаний: эксперт-инженер программист;
- сложность систематизации инженером знаний большого объема исходной информации;
- сложность составления алгоритмов для написания программ из-за большого объема разнородной и противоречивой информации.

Учитывая рассмотренные факторы, для успешного решения задач в СППР, необходимо применять методы и алгоритмы, которые наиболее оптимально могут быть применены для использования возможностей современных систем обработки большого объема информации.

Проанализируем ряд методов, которые могут быть использованы для решения задач в СППР информационной безопасности.

В работах [13, 14] в рамках неопределенности и динамических изменений внешних воздействий на ОИ, рассматривается метод байесовской сети. Данная модель отражает функционирование вычислительной системы в условиях внешних воздействий и делит ее на 4 кластера, где формируются риски УБИ, ликвидация рисков угроз, формирование рисков и ликвидаций последствий инцидента (рис. 5). Модель представляет совместное распределение вероятностей, в котором каждое ребро является условной зависимостью, а каждый узел – отдельной случайной величиной, отражающей события информационной безопасности. Одним из ключевых преимуществ байесовских сетей является их способность к наглядному представлению причинно-следственных связей и выявлять вероятность наступления негативных последствий в рамках неопределнности. Несовершенство метода состоит в том,

что для построения вероятностной модели необходимо выбирать релевантные события ИБ и установления зависимостей между ними, что в рамках большой масштабируемости сети усложняет экспертную оценку распределения вероятностей.

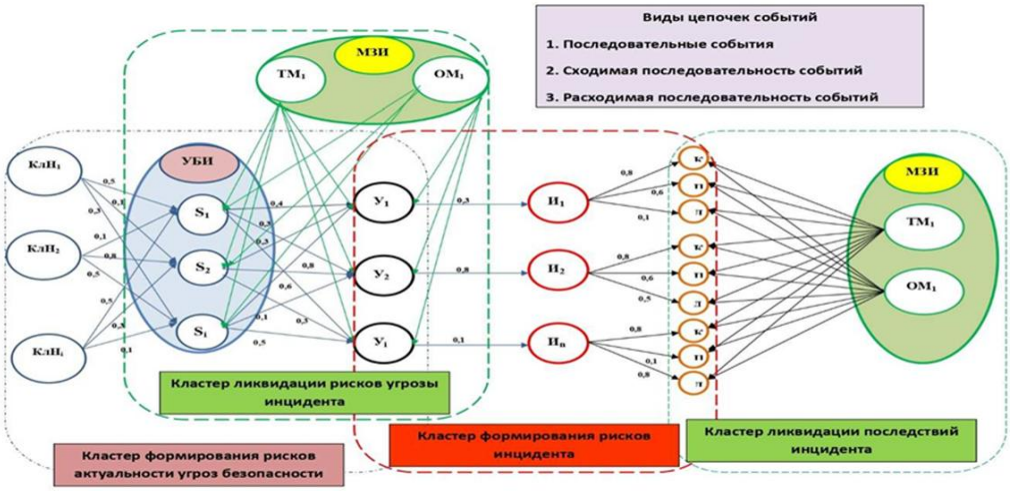

Рис. 5. Типовой модуль комплексной динамической модели функционирования защищенных информационных систем

В работе [15] рассматривается применение нечетких когнитивных карт и нейронных сетей. Нечеткая когнитивная карта является моделью ориентированного графа, где представляются концепты УБИ, объектов воздействия и применяемых средств защиты информации и связи между ними. Исходными данными являются экспертные оценки, формализованные и систематизированные шаблоны общедоступных баз знаний и практик. Коэффициент взаимосвязей между концептами определяется применением нечетких отношений, которые задаются на шкале от 0 до 1 [15–17]. Преимуществом использования нечетких когнитивных карт позволяет анализировать данные с их неопределенностью. Недостатком при использовании данного метода является, что оценка взаимосвязей между концептами УБИ проводят эксперты, что влечет за собой субъективность и при увеличении взаимосвязей концептов сложность такой оценки экспертами увеличивается.

Авторы приводят ряд критериев, на основе которых делают вывод, что нейронные сети являются эффективным инструментом по выявлению УБИ и уязвимостей. Достоинством нейронных сетей является то, что они обучаются на большем объеме данных и могут выявлять сложные паттерны, что обеспечивает высокую точность анализа, автоматизируют процесс анализа риска и адаптируются к изменениям актуальности УБИ. Соответственно эффективность нейронных сетей зависит от объема данных, на которых обучается сеть.

В работе [18–20] представлен метод онтологии, который позволяет сопоставить иерархически структурированного множества классов, описывающих предметную область и служащих основой для единой базы знаний, подчеркивает упорядоченный характер представления информации. В рамках исследования данная модель позволяет автоматизировать построение модели угроз, которая будет отражать связи негативных последствий УБИ, общеизвестных уязвимостей, сценарии реализации угроз, шаблоны атак. Систематизация знаний в виде классов и подклассов с определенными отношениями обеспечивает прозрачное понимание картины угроз, что позволяет выделить уязвимый интерфейс объекта воздействия, его критичность и корреляцию применяемых информационных технологий с уровнем компетенции злоумышленника, что соответственно способствует эффективной организации компенсирующих мер или применение средств защиты информации.

К негативным последствиям УБИ в следствии атаки на объекты воздействия {$ОБ_1$, $ОБ_2$,…, $ОБ_n$} может привести множество способов сценариев угроз {$ССУ_1$, $ССУ_2$,…, $ССУ_n$}, которые могут реализоваться множеством тактик {T_1, T_2,…, T_n} и техник {t_1, t_2,…, t_n}, а также множеством шаблонов {CAP_1, CAP_2,…, CAP_n}, в свою же очередь они реализуются через множество общеизвестных уязвимостей {{BDU_1, BDU_2,…, BDU_n}, {CWE_1, CWE_2,…, CWE_n}, {CVE_1, CVE_2,…, CVE_n}}. К тому же уязвимости могут иметь свойства критичности CVSS и множество платформ CPE {CPE_1, CPE_2,…, CPE_n}, под управлением которых функционирует программное обеспечение с обнаруженной уязвимостью. На рис. 6 приведен пример внешнего воздействия злоумышленника, где можно оценить актуальность уязвимостей посредством ее применимости к определенной платформе, критичность реализации уязвимости и отследить интерфейсы объектов воздействия.

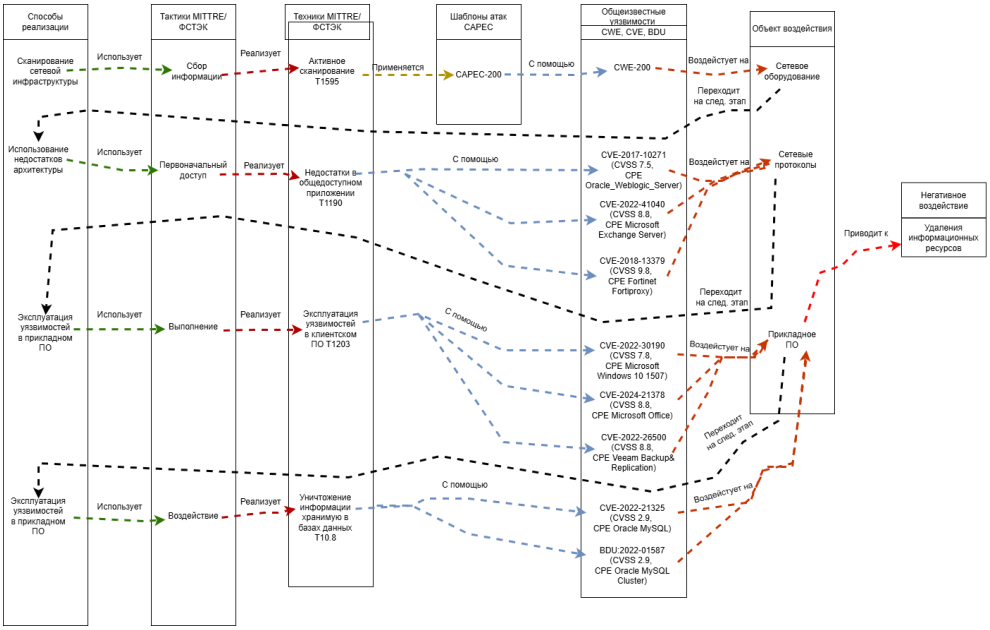

Рис. 6. Пример связей внешнего воздействия злоумышленника из различных баз знаний

Заключение. Применение эффективных методов и алгоритмов расчета защищенности активов ОИ от внешних воздействий позволяет противодействовать, как простым, так и комплексным компьютерным атакам.

В условиях постоянно усложняющихся угроз безопасности и расширения спектра потенциальных атак, обеспечение надежной защиты информационных активов остается первостепенной задачей. Рассмотренные в работе методы СППР, предназначенные для оценки угроз безопасности объектов информатизации, демонстрируют свои, как сильные стороны, так и недостатки в решении конкретных задач. На примере рассмотренных методов можно сделать вывод, что на различных стадиях проектирования КСЗИ на ОИ целесообразно применять именно те, которые наиболее точно и качественно отрабатывают поставленные задачи по подготовке варианта для принятия решения – построения модели угроз, модели нарушителя, технического задания и т.д.

Таким образом, при создании СППР выбор наиболее эффективных методов для решения задачи на определенных этапах проектирования КСЗИ на ОИ и разработка соответствующих алгоритмов, является актуальной научной технической задачей и требует дальнейшего исследования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 02.07.2021 г. № 400.
2. Доктрина информационной безопасности Российской Федерации: Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.
3. *Ягнина О.А., Щербов И.Л., Якушина А.Е.* Принятие решения по организации защиты информации на объектах информатизации // Информатика и кибернетика. – 2022. – № 1 (27). – С. 31-35. – EDN VYNLED.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
5. Методический документ «Методика оценки угроз безопасности информации»: Утвержден ФСТЭК России 5 февраля 2021 г.
6. MITTRE ATT&CK общедоступная база знаний о тактиках и техника злоумышленников, основанная на реальных наблюдениях. – Режим доступа: https://attack.mitre.org/ (дата обращения: 15.04.2025).
7. CAPEC словарь известных схем атак, используемых противниками для использования известных недостатков в возможностях кибербезопасности. – Режим доступа: https://capec.mitre.org/ (дата обращения: 15.04.2025).
8. CWE список общедоступных уязвимостей программного-аппаратного обеспечения, разработанный сообществом. – Режим доступа: https://cwe.mitre.org/ (дата обращения: 16.04.2025).
9. CVE база данных общеизвестных уязвимостей. – Режим доступа: https://www.cve.org/ (дата обращения: 16.04.2025).
10. Банк данных угроз безопасности информации ФСТЭК. Содержит сведения об основных угрозах и уязвимостях. – Режим доступа: https://bdu.fstec.ru/threat (дата обращения: 16.04.2025).
11. CVSS общая система оценки уязвимостей. – Режим доступа: https://nvd.nist.gov/vuln-metrics/cvss (дата обращения: 16.04.2025).
12. *Щербов И.Л., Якушина А.Е*. Применение систем поддержки принятия решений при ликвидации ЧС // Пожарная и техносферная безопасность: проблемы и пути совершенствования. – 2019. – № 3 (4). – С. 234-239. – EDN TNHWWV.
13. *Баранов В.В.* Интегральная модель оценки защищенности объектов информатизации в условиях деструктивного воздействия // Вестник СибГУТИ. – 2022. – № 3 (59). – Режим доступа: https://cyberleninka.ru/article/n/integralnaya-model-otsenki-zaschischennosti-obektov-informatizatsii-v-usloviyah-destruktivnogo-vozdeystviya (дата обращения: 25.03.2025).
14. *Баранов В.В., Шелупанов А.А.* Методика и алгоритмы расчета защищенности элементов распределенных информационных систем в условиях деструктивного воздействия // Доклады ТУСУР. – 2022. – Т. 25, № 4. – С. 88-100. – DOI: 10.21293/1818-0442-2022-25-4-88-100.
15. *Паршенкова Ю.А., Максимова Е.А., Матвеев А.В*. Анализ рисков информационной безопасности на объектах критической информационной инфраструктуры с помощью нейронных сетей и нечетких когнитивных карт // Вестник Санкт-Петербургского университета ГПС МЧС России. – 2024. – №. 3. – С. 86-97. – Режим доступа: https://doi.org/10.61260/2218-130X-2024-3-86-97 (дата обращения: 25.03.2025).
16. *Васильев В.И., Вульфин А.М., Кириллова А.Д., Кучкарова Н.В*. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. – 2021. – № 3. – С. 110-133.
17. *Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д.* Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт // Информационные технологии. – 2018. – Т. 24, № 10. – С. 657-664. – DOI: 10.17587/it.24.657-664. – EDN YLHRUT.
18. *Абрамов Е.С., Геворгян Р.А.* Построение онтологической модели компьютерного преступления // Системный синтез и прикладная синергетика: Сб. научных работ XI Всероссийской научной конференции, п. Нижний Архыз, 27 сентября – 01 2022 года. – Ростов-на-Дону – Таганрог: ЮФУ, 2022. – С. 147-153. – DOI: 10.18522/syssyn-2022-29. – EDN MEWLTW.
19. *Brazhuk A.* Threat modeling of cloud systems with ontological security pattern catalog // International Journal of Open Information Technologies. – 2021. – Vol. 9, No. 5. – P. 36-41. – EDN JGZXIC.
20. *Глухов Н.И., Наседкин П.Н.* Аналитика внутренних угроз информационной безопасности предприятий // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2021. – Т. 24, № 1. – С. 33-41. – DOI: 10.21293/1818-0442-2021-24-1-33-41. – EDN VRETNT.

REFERENCES

1. O Strategii natsional'noy bezopasnosti Rossiyskoy Federatsii: ukaz Prezidenta Rossiyskoy Federatsii ot 02.07.2021 g. № 400 [On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation dated 07/02/2021 No. 400].
2. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii: Utverzhdena Ukazom Prezidenta Rossiyskoy Federatsii ot 5 dekabrya 2016 g. № 646 [Information Security Doctrine of the Russian Federation: Approved by Decree of the President of the Russian Federation No. 646 dated December 5, 2016].
3. *Yagnina O.A., Shcherbov I.L., Yakushina A.E.* Prinyatie resheniya po organizatsii zashchity informatsii na ob"ektakh informatizatsii [Decision-making on the organization of information protection at informatization facilities], *Informatika i kibernetika* [Informatics and Cybernetics], 2022, No. 1 (27), pp. 31-35. EDN VYNLED.
4. GOST R 51275-2006. Zashchita informatsii. Ob"ekt informatizatsii. Faktory, vozdeystvuyushchie na informatsiyu. Obshchie polozheniya [GOST R 51275-2006. Information protection. The object of informatization. Factors influencing information. General provisions].
5. Metodicheskiy dokument «Metodika otsenki ugroz bezopasnosti informatsii»: Utverzhden FSTEK Rossii 5 fevralya 2021 g. [Methodological document "Methodology for assessing information security threats": Approved by the FSTEC of Russia on February 5, 2021].
6. MITTRE ATT&CK obshchedostupnaya baza znaniy o taktikakh i tekhnika zloumyshlennikov, osnovannaya na real'nykh nablyudeniyakh [MITTRE ATT&CK a publicly available knowledge base on the tactics and techniques of intruders based on real observations]. Available at: https://attack.mitre.org/ (accessed 15 April 2025).
7. CAPEC slovar' izvestnykh skhem atak, ispol'zuemykh protivnikami dlya ispol'zovaniya izvestnykh nedostatkov v vozmozhnostyakh kiberbezopasnosti [CAPEC dictionary of known attack schemes used by opponents to exploit known flaws in cybersecurity capabilities]. Available at: https://capec.mitre.org/ (accessed 15 April 2025).
8. CWE spisok obshchedostupnykh uyazvimostey programmnogo-apparatnogo obespecheniya, razrabotannyy soobshchestvom [CWE list of publicly available software and hardware vulnerabilities developed by the community]. Available at: https://cwe.mitre.org/ (accessed 15 April 2025).
9. CVE baza dannykh obshcheizvestnykh uyazvimostey [CVE database of well-known vulnerabilities]. Available at: https://www.cve.org/ (accessed 15 April 2025).
10. Bank dannykh ugroz bezopasnosti informatsii FSTEK. Soderzhit svedeniya ob osnovnykh ugrozakh i uyazvimostyakh [The FSTEC Information Security Threat Database. Contains information about the main threats and vulnerabilities]. Available at: https://bdu.fstec.ru/threat (accessed 15 April 2025).
11. CVSS obshchaya sistema otsenki uyazvimostey [CVSS general vulnerability assessment system]. Available at: https://nvd.nist.gov/vuln-metrics/cvss (accessed 15 April 2025).
12. *Shcherbov I.L., Yakushina A.E.* Primenenie sistem podderzhki prinyatiya resheniy pri likvidatsii ChS [Application of decision support systems in emergency response], *Pozharnaya i tekhnosfernaya bezopasnost': problemy i puti sovershenstvovaniya* [Fire and technosphere safety: problems and ways of improvement], 2019, No. 3 (4), pp. 234-239. EDN TNHWWV.
13. *Baranov V.V.* Integral'naya model' otsenki zashchishchennosti ob"ektov informatizatsii v usloviyakh destruktivnogo vozdeystviya [An integral model for assessing the security of informatization facilities under conditions of destructive influence], *Vestnik SibGUTI* [Bulletin of SibGUTI], 2022, No. 3 (59). Available at: https://cyberleninka.ru/article/n/integralnaya-model-otsenki-zaschischennosti-obektov-informatizatsii-v-usloviyah-destruktivnogo-vozdeystviya (accessed 25 March 2025).
14. *Baranov V.V., Shelupanov A.A*. Metodika i algoritmy rascheta zashchishchennosti elementov raspredelennykh informatsionnykh sistem v usloviyakh destruktivnogo vozdeystviya [Methods and algorithms for calculating the security of elements of distributed information systems under conditions of destructive influence], *Doklady TUSUR* [Reports of TUSUR], 2022, Vol. 25, No. 4, pp. 88-100. DOI: 10.21293/1818-0442-2022-25-4-88-100.
15. *Parshenkova Yu.A., Maksimova E.A., Matveev A.V.* Analiz riskov informatsionnoy bezopasnosti na ob"ektakh kriticheskoy informatsionnoy infrastruktury s pomoshch'yu neyronnykh setey i nechetkikh kognitivnykh kart [Analysis of information security risks at critical information infrastructure facilities using neural networks and fuzzy cognitive maps], *Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii* [Bulletin of the Saint Petersburg University of the Ministry of Emergency Situations of Russia], 2024, No. 3, pp. 86-97. Available at: https://doi.org/10.61260/2218-130X-2024-3-86-97 (accessed 25 March 2025).
16. *Vasil'ev V.I., Vul'fin A.M., Kirillova A.D., Kuchkarova N.V.* Metodika otsenki aktual'nykh ugroz i uyazvimostey na osnove tekhnologiy kognitivnogo modelirovaniya i Text Mining [Methods for assessing current threats and vulnerabilities based on cognitive modeling and Text Mining technologies], *Sistemy upravleniya, svyazi i bezopasnosti* [Management, communication and security systems], 2021, No. 3, pp. 110-133.

17. *Vasil'ev V.I., Vul'fin A.M., Guzairov M.B., Kirillova A.D*. Interval'noe otsenivanie informatsionnykh riskov s pomoshch'yu nechetkikh serykh kognitivnykh kart [Interval assessment of information risks using fuzzy gray cognitive maps], *Informatsionnye tekhnologii* [Information Technologies], 2018, Vol. 24, No. 10, pp. 657-664. DOI: 10.17587/it.24.657-664. EDN YLHRUT.
18. *Abramov E.S., Gevorgyan R.A.* Postroenie ontologicheskoy modeli komp'yuternogo prestupleniya [Construction of an ontological model of computer crime], *Sistemnyy sintez i prikladnaya sinergetika: Sb. nauchnykh rabot XI Vserossiyskoy nauchnoy konferentsii, p. Nizhniy Arkhyz, 27 sentyabrya – 01 2022 goda* [System synthesis and applied synergetics: Collection of scientific papers of the XI All-Russian Scientific Conference, Nizhny Arkhyz settlement, September 27 – 01, 2022]. Rostov-on-Don – Taganrog: YuFU, 2022, pp. 147-153. DOI: 10.18522/syssyn-2022-29. EDN MEWLTW.
19. *Brazhuk A.* Threat modeling of cloud systems with ontological security pattern catalog, *International Journal of Open Information Technologies,* 2021, Vol. 9, No. 5, pp. 36-41. EDN JGZXIC.
20. *Glukhov N.I., Nasedkin P.N.* Analitika vnutrennikh ugroz informatsionnoy bezopasnosti predpriyatiy [Analytics of internal threats to information security of enterprises], *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Reports of Tomsk State University of Control Systems and Radio Electronics], 2021, Vol. 24, No. 1, pp. 33-41. DOI: 10.21293/1818-0442-2021-24-1-33-41. EDN VRETNT.

Ерёмин Иван Александрович – Донецкий национальный технический университет; e-mail: Eremin-Ivan.TSI-20@yandex.ru; г. Донецк, Россия; тел.: +79498635241; магистрант.

Якушина Анна Евгеньевна – Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова; e-mail: yakuann@yandex.ru, г. Новочеркасск, Россия; тел.: +79494596928; магистрант.

Щербов Игорь Леонидович - Донецкий национальный технический университет; e-mail: scherbov@yandex.com; г. Донецк, Россия; тел.: +79493105787; к.т.н.; доцент.

Eremin Ivan Aleksandrovich – Donetsk National Technical University; e-mail: Eremin-Ivan.TSI-20@yandex.ru; Donetsk, Russia; phone: +79498635241; master’s student.

Yakushina Anna Evgenievna – Platov South Russian State Polytechnic University (NPI); e-mail: yakuann@yandex.ru; Novocherkassk, Russia; phone: +79494596928; master’s student.

Shcherbov Igor Leonidovich - Donetsk National Technical University; e-mail: scherbov@yandex.com; Donetsk, Russia; phone: +79493105787; cand. of eng. sc.; associate professor.