DOI 10.36622/1682-7813.2024.27.2.008
УДК 004.056

ФОРМАЛИЗАЦИЯ ЗНАНИЙ И ДАННЫХ КИБЕРАТАК И УЯЗВИМОСТЕЙ

Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко,
Д.С. Покудин, Н.Н. Корвяков, А.А. Ноздрюхин

В статье рассматриваются противоречия при использовании CAPEC как источника сведений о шаблонах атак. Обосновывается выбор отечественной базы уязвимостей в качестве источника информации об уязвимостях. Осуществляется создание банка знаний и данных о кибератаках и уязвимостях, агрегированных в специально разработанные форматы, такие как паспорт вектора атаки, паспорт уязвимости, форма сведений об инцидентах и регламентах киберпротивоборства. Описываются методики работы с этими форматами и правила их заполнения. Обсуждаются перспективы улучшения механизма присвоения типа ошибки CWE к шаблону атак CAPEC.

Ключевые слова: база знаний и данных, уязвимость, вектор атаки, агрегация, угрозы, регламенты

Введение

Цунами кибератак, систематически обрушивающихся на отечественное информационное пространство [1], объективно требует обеспечения необходимой технической и организационно-правовой защиты современных автоматизированных информационных систем (далее – АИС) и телекоммуникационных сетей (далее – ТКС) от сочетаний векторов (сценариев) реализации атак и уязвимостей АИС и ТКС, используемых злоумышленниками [2-5].

В этой связи, персоналу, защищающему АИС и ТКС, приходится иметь дело с сотнями известных злоумышленных сценариев и тысячами выявленных уязвимостей, порождающими десятки тысяч их сочетаний, каждое из которых имеет свою специфику реагирования средств и органов защиты [2-6]. Поэтому для формирования основы построения системы защиты, способной адаптироваться к постоянно изменяющимся угрозам, ставиться задача сбора и систематизации информации о многообразии векторов атак и связанных с ними уязвимостях [3-6].

Агрегация данных – это процесс, включающий в себя сбор, организацию и анализ обширного объема информации.

В контексте обеспечения кибербезопасности осуществляется сбор данных о различных видах атак, их источниках, целях и последствиях, а также об уязвимостях в системах и программном обеспечении (далее – ПО), которые потенциально могут быть использованы злоумышленниками.

Это потребовало глубоких знаний в области кибербезопасности и навыков работы с большими объемами данных. В результате был получен ценный информационный ресурс, который можно будет использовать для разработки политик безопасности, регламентов и инструкций [1].

Адаптация сведений о векторах атак

В качестве источника сведений об известных векторах атак используется CAPEC. CAPEC (с англ. перечень и классификация распространенных шаблонов атак). Это общедоступный каталог распространенных шаблонов атак, который помогает пользователям и специалистам по информационной безопасности понять, как злоумышленники используют слабые места в приложениях и другие возможности кибератак [2].

Шаблон атаки представляет собой описание общих атрибутов и методов, которые злоумышленники применяют для эксплуатации известных уязвимостей в системах. Он основывается на концепции шаблонов проектирования, но используется в деструктивном контексте. Создание

шаблона атаки происходит на основе глубокого анализа реальных случаев [2].

Каждый шаблон атаки содержит информацию о том, как разрабатываются и выполняются конкретные части атаки, и дает рекомендации о способах снижения эффективности атаки. Шаблоны атак помогают разработчикам приложений или администраторам лучше понимать конкретные элементы атаки и способы предотвращения их успешной реализации [2].

CAPEC был создан Министерством внутренней безопасности США в рамках стратегической инициативы Управления кибербезопасности и коммуникаций (CS&C) по обеспечению безопасности программного обеспечения (SwA). Первоначально опубликованный в 2007 году список CAPEC продолжает совершенствоваться при участии общественности в формировании стандартного механизма выявления, сбора, уточнения и распространения атак среди сообщества кибербезопасности [2].

CAPEC имеет иерархическую структуру, где на верхнем уровне иерархии шаблоны атак структурированы по механизмам и доменам их применения; на среднем уровне иерархии выделяются группы шаблонов, которые объединены по общим характеристикам; на низком уровне иерархии находятся абстрактные описания методов выполнения атак [5].

Структурно шаблоны атак на CAPEC представлены следующим образом (рис. 1) [2].

В ходе анализа шаблонов атак CAPEC возникли следующие трудности.

1. Информация о векторах атак на сайте представлена только на английском языке. Это затрудняло анализ шаблонов атак, поскольку для выполнения этой задачи недостаточно машинного перевода; необходимо использовать накопленные знания в области технического английского.

2. Анализ шаблонов атак осуществлялся в условиях недостатка информации по шаблонам, так как некоторые вектора атак не содержат никаких сведений. В качестве примера можно выделить «CAPEC – 434: Воздействие на цель посредством интервью и допроса» (рис.2), где у данного шаблона отсутствуют базовые сведения.

3. В качестве отдельной проблемы стоит указать, что не у всех шаблонов на сайте были указаны соответствующие им типы ошибок CWE, а без этой информации невозможно произвести дальнейшее формирование сценария вектора атаки. В интересах решения данной проблемы проводился анализ шаблонов, которые находятся с ним в одном в меташаблоне. На основании полученной информации определилась закономерность присваивания CWE, что позволили, практически безошибочно, определить необходимый тип ошибки.

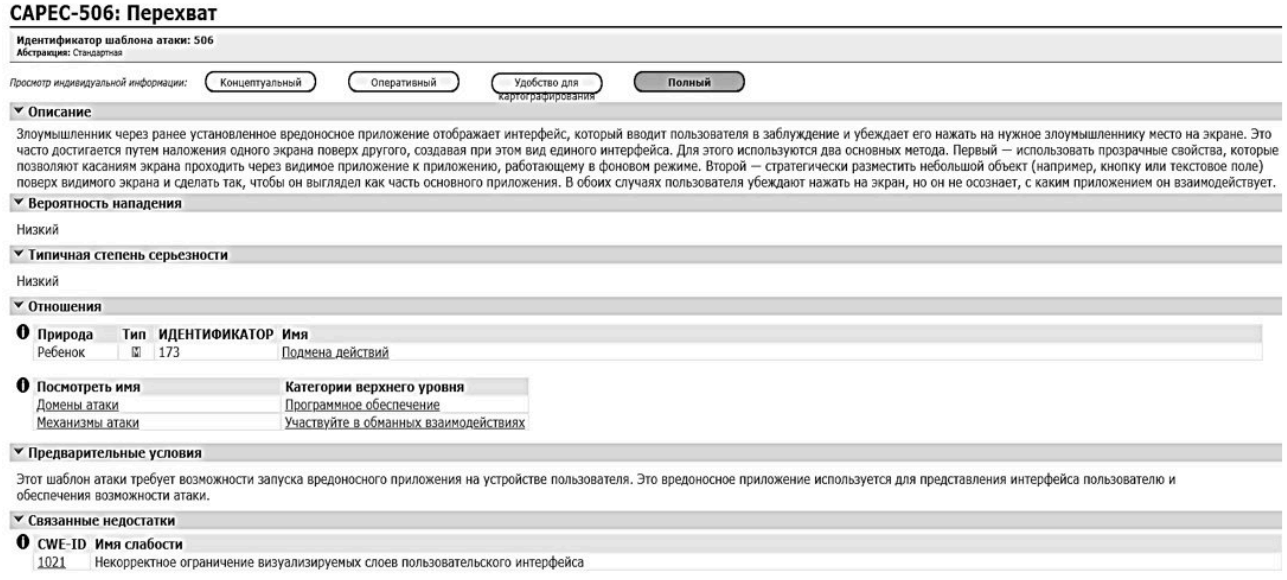

Рис. 1. Пример структуры шаблона атак на CAPEC

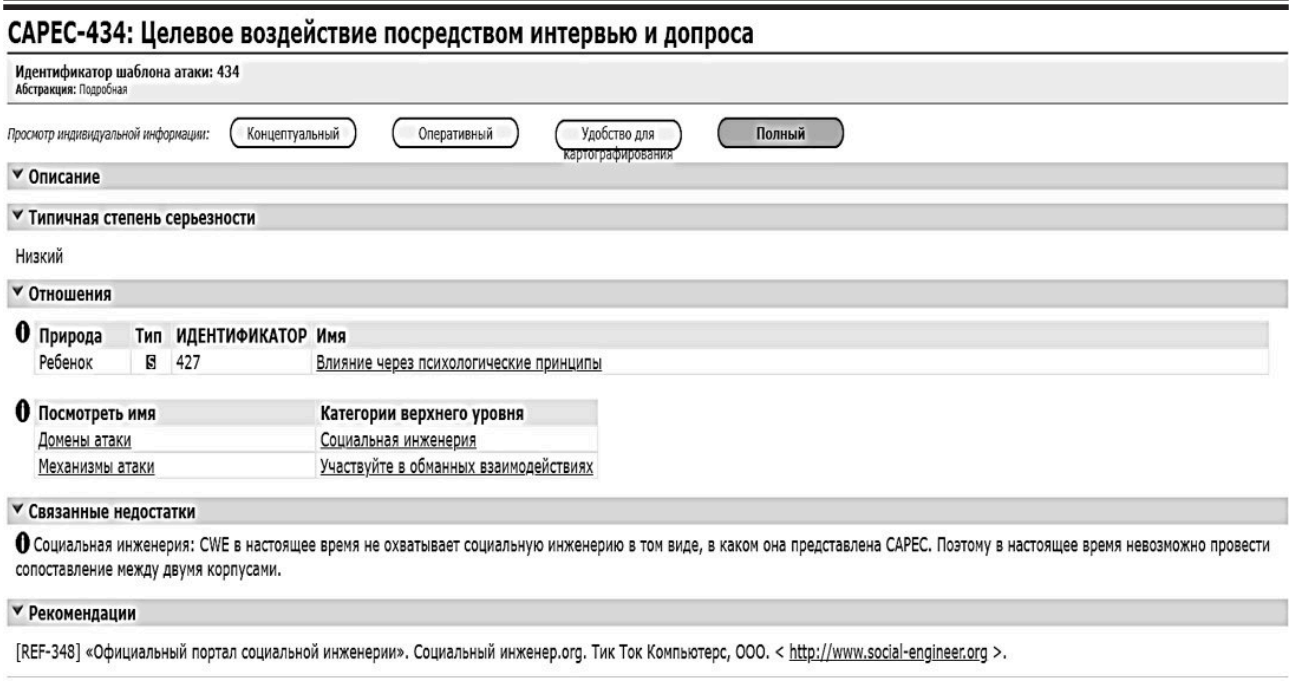

Рис. 2. Пример наполняемости шаблона CAPEC-434

4. Большинство описаний шаблонов атак лишено конкретики и представляет из себя «тексты – лозунги», по которым затруднительно понять, что из себя представляет шаблон, как он реализуется и каким негативным последствиям приводит результат атаки.

В результате анализа шаблонов атак CAPEC составлен паспорт вектора атаки (табл. 1), в котором отражена суть шаблона атаки и текст описания приведен к единому виду.

Таблица 1

Пример паспорта вектора атаки

Идентификатор системы CAPEC	CAPEC-***: ***	
Описание вектора атаки	***	
Тип атаки	***	
Соотношение типа ошибки CWE и статуса типа ошибки CWE	CWE - ***: *** CWE - ***: ***	***

Паспорт вектора атаки содержит следующую информацию:

1) идентификатор системы CAPEC – уникальный идентификатор и название вектора атаки;

2) описание вектора атаки – краткое описание вектора атаки, включая цель атаки;

3) тип атаки – механизм атаки;

4) соотношение типа ошибки CWE и статуса типа ошибки CWE – связанные с вектором атаки CWE и их статус.

Особое внимание стоит обратить на поле «Соотношение типа ошибки CWE и статуса типа ошибки CWE». В нем вводится такое понятие как «статус типа ошибки CWE», которое может иметь 3 значения: разрешен для использования в реальных уязвимостях; не рекомендован для использования в реальных уязвимостях; запрещен для использования в реальных уязвимостях. Эти метки предназначены для обеспечения того, чтобы сопоставление первопричин обеспечивало достаточно адекватную корреляцию между записями CWE и CVE [6].

Агрегация сведений об уязвимостях

Для мониторинга уязвимостей можно использовать следующие базы знаний об уязвимостях: NVD, CISA KEV и БДУ ФСТЭК России. В ходе выборочной их проверки, было установлено, что некоторые уязвимости из американских баз (примерно 10 из 30) не связаны с корпоративными сетями. Также в таких базах знаний об уязвимостях, как NVD и CISA KEV, не содержатся сведения об отечественном ПО, что значительно увеличивает процент ошибок в ходе эксплуатации продукта в отечественных корпоративных сетях. В связи с этим в данной статье рассматриваются уязвимости из БДУ ФСТЭК России, так как она содержит детально расписанные паспорта уязвимостей, в отличие от западных аналогов.

В БДУ ФСТЭК России содержатся банк уязвимостей и каталог угроз. Ресурс включает информацию о 57 564 уязвимостях и 222 угрозах, особенно актуальных для ГИС, ИСПДн и АСУ ТП на объектах КИИ [4].

Цель создания БДУ ФСТЭК России - предоставление информационной и методической поддержки государственным органам и организациям в деятельности по определению, оценке и моделированию угроз безопасности информации, а также в выявлении, анализе и устранении уязвимостей в АИС и ТКС, в том числе в ПО и СЗИ. Также база данных используется для подтверждения соответствия этих систем и средств обязательным требованиям и поддержания программных средств контроля защищенности информации [4].

БДУ ФСТЭК России взаимосвязана: с ресурсами производителей ПО, которые публикуют уязвимости своих продуктов, такими как Microsoft Corp., Google Inc., Mozilla Corp., Red Hat Inc., Adobe Systems Inc., ООО «РусБИТех- Астра», Ростелеком-Солар, Positive Technologies и другие; другими базами уязвимостей, такими как NVD, CERT и другие, а также с частными исследователями уязвимостей. Такая взаимосвязь расширяет возможности базы БДУ ФСТЭК России, что дает возможность точно сопоставить шаблон атаки CAPEC с соответствующими ему уязвимостями [4].

За основу при составлении паспорта уязвимости брался формат уязвимостей БДУ ФСТЭК России.

Паспорт уязвимости в БДУ ФСТЭК России включает следующие структурные поля, которые наиболее важны для дальнейшего использования в риск-анализе [4]: идентификатор типа ошибки, метрики оценки критичности, степень подтверждения существования уязвимости, наличие эксплойта и способ устранения.

Сформировав необходимые базы знаний, можно приступить к описанию сценария атаки, который определяет пара, включающая вектор атаки и уязвимость, связанную с ним. В ходе анализа уязвимостей было установлено, что охватить все их множество не представляется возможным, так как порой на один вектор атаки приходится около сотни уязвимостей. В результате чего было предложено сделать выборку уязвимостей по следующим параметрам: участие уязвимости в реальных инцидентах; наличие эксплойта на уязвимость; уровень опасности уязвимости.

Алгоритм выборки имеет следующий вид:

1) из всего множества уязвимостей отбираются те, которые были задействованы в реальных атаках;
2) отбираются уязвимости, которые имеют эксплойт;
3) из сформированного пула уязвимостей отбираются те, которые имеют критичный и/или высокий уровень опасности реализации.

Тем самым, обеспечивается рассмотрение уязвимостей, которые могут быть задействованы вновь и на которые стоит обратить внимание в первую очередь.

Непосредственно сам процесс построения сценария вектора атаки выглядит следующим образом:

- выбирается пара вектор - уязвимость;
- описываются действия злоумышленника.

Действия злоумышленника, в рамках выбранной пары, раскладываются на 14 этапов, в соответствии последовательностью реализации кибератак, рекомендованной MITRE ATT&CK [5].

Важно обратить внимание, что не всегда все этапы присутствуют при описании действий злоумышленника. Например, этап "Подготовка ресурсов" часто отсутствует.

Конечной целью вектора атаки является эксплуатация уязвимости, которая может произойти на этапах: эксфильтрация данных (данный этап при успешной реализации несет следующий ущерб - нарушение конфиденциальности) или деструктивное воздействие (данный этап при успешной реализации несет следующие ущербы - нарушение целостности, нарушение доступности).

Зная сценарий действий злоумышленника, можно определить, на каких действиях будет фиксироваться инцидент и на какие действия можно ответить мерами по реагированию и мерами по ликвидации последствий.

Формализация сведений об инцидентах и регламентах киберпротивоборства (далее - Форма) представлена в табл. 2 [3].

Ключевым условием следует считать наличие сквозной горизонтали, обеспечивающей точное соответствие между злоумышленными действиями, мерами реагирования на них и мерами ликвидации негативных последствий. Только при выполнении этого условия можно построить структурно и функционально сбалансированную систему защиты, обладающую необходимой эффективностью для противодействия различным кибератакам [1].

С момента регистрации и классификации атаки защитники объекта должны поступательно внедрять меры реагирования. При этом, к радикальным средствам (например, отключение от сети Интернет) следует прибегать только в исключительных случаях, так как это полностью нарушает работу корпоративной сети. Частое использование стандартных мер (фильтрация и т.п.) без необходимости указывает на низкую квалификацию проектировщика, что снижает эффективность сетевой защиты [1].

Рекомендации по заполнению формы приведены в табл. 3.

Вышеописанное можно изложить в краткой форме:

1) рассматривая шаблон атаки CAPEC, следует привести его к формату паспорта вектора атаки (табл. 1);

2) выделить, через тип ошибки CWE, связанные с вектором атаки уязвимости;

3) произвести выборку уязвимостей по следующим критериям: участие уязвимости в реальных инцидентах; наличие эксплойта на уязвимость; уровень опасности уязвимости;

4) отобранные уязвимости привести к формату паспорта уязвимости;

5) сформировать пары вектор - уязвимость;

6) по сформированным парам вектор – уязвимость построить сценарий атаки (сколько сформировалось пар вектор-уязвимость, столько следует и строить сценариев вектора атаки);

7) в сценарии необходимо выделить действия, на которых будут регистрироваться инциденты и занести их в табл.2;

8) на зарегистрированные инциденты необходимо предложить адекватные меры по реагированию и меры по ликвидации последствий.

Заключение

Вышеприведенные формализмы стали основой для агрегирования сведений о кибератаках и используемых ими уязвимостях для последующего машинного обучения нейросети, генерирующей регламенты обеспечения кибербезопасности АИС и ТКС.

Используя предложенную формализацию, впервые удалось создать столь масштабную и детализированную базу знаний и данных о кибератаках и уязвимостях, которую можно будет интегрировать в образовательный процесс, включая обучение специализированных нейросетей.

Таблица 2

Формализация сведений об инцидентах и регламентах киберпротивоборства

Этапность реализации кибератак, рекомендованная MITRE ATT&CK		В соответствии с MITRE-этапностью регистрируемые инциденты пары атака-уязвимость	Меры реагирования на регистрируемые инциденты, порожденные парой атака-уязвимость	Меры ликвидации последствий инцидентов, порожденных парой атака-уязвимость
1	Разведка			
2	Подготовка ресурсов			
3	Перовоначальный достуцп			
4	Выполнение			
5	Закрепление			
6	Повышение привилегий			
7	Предотвращение обнаружения			
8	Получение учетных данных			
9	Изучение			
10	Перемещение внутри периметра			
11	Сбор данных			
12	Организация управления			
13	Эксфильтрация данных			
14	Деструктивное воздействие			

Таблица 3

Рекомендации по заполнению формы

	Поэтапно регистрируемые инциденты, порожденные парой атака-уязвимость	Меры реагирования на регистрируемые инциденты, порожденные парой атака-уязвимость	Меры ликвидации последствий инцидентов, порожденных парой атака-уязвимость
Сущность формализации инцидентов и регламентов противодействия кибератакам	Описание инцидента как зарегистрированного события, угрожающего конкретным ущербом на данном этапе реализации заданного вектора атаки исключительно в отношении рассматриваемой уязвимости	На этапе регистрации инцидента пресечение или конкретная локализация атаки за счет обоснованно избранны проектантом мер, четко специализированных под рассматриваемую уязвимость	На этапе регистрации инцидента устранение или ослабление конкретного ущерба от реализации атаки за счет обоснованно избранных проектантом мер, четко специализированных под рассматриваемую уязвимость

Продолжение таблицы 3

	Поэтапно регистрируемые инциденты, порожденные парой атака-уязвимость	Меры реагирования на регистрируемые инциденты, порожденные парой атака-уязвимость	Меры ликвидации последствий инцидентов, порожденных парой атака-уязвимость
Пример формализации, требующий своей конкретизации в отношении ПО и АО для пары вектор - уязвимость	Резкий рост количества деструктивных запросов, угрожающий нарушением доступности информации при уязвимости, обусловленной ограничением объема буфера…	Срочный «останов» переполнения буфера за счет переключения потока деструктивных запросов на «зеркальный сервер», поглощающий угрожающие нарушением доступности запросы…	Оперативное устранение переполнения буфера за счет его чистки от деструктивных запросов, и нивелирование угрозы на будущее за счет блокировки адресов, генерирующих деструктивные запросы…

В данной статье не удалось учесть некоторые аспекты, такие как механизм присвоения типа ошибки CWE к шаблону атак CAPEC, что важно для правильного формирования сценария для пары вектора атаки и уязвимости. Авторы планируют обратиться к этой проблеме на стадии программной реализации и внедрения рассматриваемого сервиса, чтобы получить заслуживающие внимания результаты.

По большому счету, развернутая в приведенных выше таблицах формализация обусловлена противоречиями, выявленными в текстах описаний инцидентов и регламентов, предлагаемых известными базами данных. К ним можно отнести попытки представить инцидент не как событие, а ввиде некоторого процесса, что снижает оперативность последующего реагирования. Кроме того, предлагаемые разработчиками меры зачастую слабо учитывают специфику рассматриваемой уязвимости, что может снизить эффективность использования рекомендуемых регламентов. При этом, нечеткость формулировок предлагаемых действий также способна снизить эффективность борьбы с кибератаками и их последствиями.

Поэтому вышеперечисленные противоречия необходимо разрешить на стадии формулирования баз знаний о кибератаках и используемых ими уязвимостях. Эту задачу ставят перед собой авторы в плане развития своих исследований в части создания инструментария автоматизации противодействия кибервторжениям в качестве интеллектуального помощника для администратора сетевой безопасности.

Список литературы

1. Организационно-правовая защита сетей / Г.А. Остапенко, Д.В. Щербакова, А.О. Калашников [и др.].; Под ред. Академика РАН Д. А. Новикова. Сер. Теория сетевых воин. Вып. 8. М.: Горячая линия Телеком, 2023. 228с.

2. CAPEC - Common Attack Pattern Enumeration and Classification // URL: https://capec.mitre.org/ (дата обращения: 06.05.2024)

3. MITRE ATT&CK // URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 06.05.2024)

4. Банк данных угроз безопасности информации ФСТЭК России // URL: https://bdu.fstec.ru/threat. (дата обращения: 06.05.2024)

5. Сравнительный анализ баз данных MITRE ATT&CK и CAPEC // URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-baz-dannyh-mitre-att-ck-i-capec/viewer (дата обращения: 06.05.2024)

6. CWE - Common Weakness Enumeration // URL: https://cwe.mitre.org/index.html (дата обращения: 06.05.2024)

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 07.05.2024

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, проректор, Финансовый университет при Правительстве Российской Федерации, e-mail: ostg@mail.ru

Васильченко Алексей Павлович – аспирант, Финансовый университет при Правительстве Российской Федерации, e-mail: zainichek@yandex.ru

Остапенко Александр Алексеевич – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

Покудин Данила Сергеевич – студент, Воронежский государственный технический университет, e-mail: danila.pokudin@inbox.ru

Корвяков Никита Николаевич – студент, Воронежский государственный технический университет, e-mail: korvyakov48@yandex.ru

Ноздрюхин Александр Александрович – студент, Воронежский государственный технический университет, e-mail: sfrvvv@yandex.ru

FORMALIZATION OF KNOWLEDGE AND DATA OF CYBER ATTACKS AND VULNERABILITIES

G.A. Ostapenko, A.P. Vasilchenko, A.A. Ostapenko, D.S. Pokudin, N.N. Korvyakov, A.A. Nozdriukhin

The article discusses the contradictions when using CAPEC as a source of information about templates as well. The choice of the domestic vulnerability database as a source of information about vulnerabilities is justified. A knowledge bank and data on cyber attacks and vulnerabilities are being created, aggregated into specially designed formats such as an attack vector passport, vulnerability passport, an incident information form and cyber warfare regulations. The mechanisms of working with these formats and the rules for filling them are described. The prospects for improving the mechanism for assigning the CWE error type to CAPEC attack patterns are discussed, as well as integrating the generated knowledge and data into the educational process, including training specialized neural networks, in particular for the module of neural network regulation of measures to counter cyber attacks..

Keywords: knowledge and data base, vulnerability, attack vector, aggregation, threats, regulations.

Submitted 07.05.2024

Information about the authors

Grigory A. Ostapenko – Dr. Sc. (Technical), Vice-Rector, Financial University under the Government of the Russian Federation, e-mail: ostg@mail.ru.

Alexey P. Vasilchenko – graduate student, Financial University under the Government of the Russian Federation, e-mail: zainichek@yandex.ru.

Alexander A. Ostapenko – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com

Danila S. Pokudin -–student, Voronezh State Technical University, e-mail: danila.pokudin@inbox.ru

Nikita N. Korvyakov – student, Voronezh State Technical University, e-mail: korvyakov48@yandex.ru

Alexander A. Nozdryukhin – student, Voronezh State Technical University, e-mail: sfrvvv@yandex.ru