**DOI 10.36622/1682-7813.2024.27.2.007**
**УДК 004.056**

# МОДЕРНИЗАЦИЯ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННОГО СЕРВИСА АГРЕГАЦИИ ДАННЫХ И РИСК-АНАЛИЗА УЯЗВИМОСТЕЙ

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

В порядке модернизации методического обеспечения автоматизированного сервиса агрегации данных и риск-анализа уязвимостей, предложена усовершенствованная адаптированная версия описания векторов атак CAPEC, а также переход от иностранных баз знаний CVE NIST и CVE KEV, поддерживаемых Государственным департаментом США, к отечественной разработке базы знаний БДУ ФСТЭК и базы знаний НКЦКИ, которая охватывает весь спектр уязвимостей, эксплуатация которых зарегистрирована на территории Российской Федерации. Также представлен модернизированный блок калькуляции рисков, включающий в себя рассмотрение массированной атаки, когда тот или иной вектор реализуется многократно. Модернизация позволяет адаптировать методическое обеспечение под реалии современного киберпротивоборства.

Ключевые слова: информация, безопасность, уязвимость, вектор атаки, поточные кибератаки, риск.

## Введение

В условиях давления на Российскую Федерацию и перехода государственной политики на мобилизационные рельсы, использование открытых иностранных баз знаний, таких как CVE NIST, CVE KEV несет в себе потенциальные угрозы для автоматизированных информационных систем (АИС). Базы знаний не обновляются должным образом и не удовлетворяют требованиям специалистов. В связи с сокращением финансирования страдает качество и своевременность представления информации. Исходя из вышеизложенного, становится невозможным эффективное управление рисками в области информационной безопасности (ИБ) по средствам вышеупомянутых репозиториев данных.

Информационное противоборство кибердержав – это не миф, а реалии современного мира, в связи с чем становятся актуальны проблемы оценки рисков успешности реализации компьютерных атак на АИС, решение которых видится на пути глубокой модернизации методического обеспечения автоматизированного сервиса агрегации данных и рисканализа уязвимостей.



Её достижение возможно в ходе решения следующих задачи:

1) адаптация базы знаний CAPEC, исходя из реалий отечественного рынка информационной безопасности;

2) проведение анализа актуальности представления уязвимостей в БДУ ФСТЭК и полноты описания выявленных слабостей и заключение о применимости;

3) осуществление выборки реально эксплуатируемых уязвимостей посредством базы знаний об уязвимостях НКЦКИ;

4) модернизация методического обеспечения калькуляции рисков с учетом проводимых поточных кибератак.

## Адаптация базы знаний CAPEC

CAPEC – представляет собой общедоступный каталог общих векторов атак, который помогает специалистам в области ИБ и пользователям сервиса понять, как злоумышленник использует слабые места АИС в киберинцидентах. Данный каталог представляет собой веб-ресурс на английском языке, что затрудняет работу отечественных специалистов и увеличивает время, затраченное на ликвидацию последствий и реагирование на инциденты ИБ, что негативно влияет на потенциальный ущерб [1].

Вектора атаки описывают общие атрибуты и подходы, применяемые злоумышленниками для использования известных слабостей в киберинцидентах. Они определяют проблемы, с которыми может столкнуться злоумышленник и способы их решения. Вектора атак основаны на концепции разработки шаблонов, применяемых в деструктивном контексте.

Каждый вектор атаки содержит знания о том, как разрабатываются и выполняются определенные этапы деструктивного воздействия на АИС. Данная база знаний помогает разработчикам программного обеспечения и специалистам по управлению инцидентам лучше понять конкретные элементы атаки и способы предотвращения ее успеха.

В ходе адаптации базы знаний было рассмотрено все множество векторов атак на данный момент (559). Все вектора адаптировались в форме таблицы вектора атаки (табл. 1). Для примера остановимся на одном из них, в частности на CAPEC-15: Инъекция в команды с разделительными символами.

Таблица 1

CAPEC-15: Инъекция в команды с разделительными символами

| ID CAPEC | 15 |
|---|---|
| Наименование | Инъекция в команды с разделительным символом |
| Описание | Атаки этого типа используют уязвимости ПО, позволяющие добавлять команды злоумышленника к легитимным командам с целью воздействия на другие ресурсы, такие как файловая система или база данных. Система, использующая проверку ввода по фильтру или листам отказа, в отличие от проверки по списку разрешений, уязвима для злоумышленника, который распознает разделительные символы (или комбинации разделительных символов), не присутствующие в фильтре или листе отказа. Как и в других инъекционных атаках, злоумышленник использует полезную нагрузку разделительных символов в качестве точки входа, чтобы пройти через приложение и активировать дополнительные атаки с помощью SQL-запросов, команд оболочки, сканирования сети. |
| Атакуемый объект | Программное обеспечение |
| Класс атаки | Внедрение неожиданных элементов |
| Тип ошибки CWE | 146 – неправильная обработка разделителей выражений<br>77 – неправильная обработка символов, встречающихся в команде<br>184 – неполный список запрещенных исходных материалов<br>78 – неправильная обработка специальных элементов в ОС<br>185 – неправильное регулярное выражение<br>93 – неправильная обработка последовательности CRLF<br>140 – неправильная обработка разделительных символов<br>157 – невозможность проверки парных разделительных символов<br>138 – неправильная обработка специальных элементов<br>154 – неправильная обработка переменных разделительных символов<br>697 – неправильное сравнение |
| Предусловия | Проверка или фильтрация входных данных в программе не должна обнаруживать и блокировать наличие дополнительной вредоносной команды. |

Продолжение табл. 1

| ID CAPEC | 15 | |
|---|---|---|
| Сценарий атаки | Исследование | **Оценка среды выполнения:** в ситуациях, когда среда выполнения явно не известна, злоумышленник устанавливает соединение с целевой системой и пытается определить ее среду выполнения. Знание среды очень важно для выбора правильных разделителей.<br>**Техники:** сканирование портов с помощью программного обеспечения на основе сетевых соединений;<br>цифровой отпечаток TCP/IP; преднамеренный вызов ошибок, для поиска информации об ошибках.<br>**Исследование ПО:** Злоумышленник проводит анализ целевого ПО в качестве аутентифицированного пользователя.<br>**Техники:** поиск на веб-сайтах всех доступных ссылок, учет всех возможных входов в ПО. |
| | Подготовка к реализации | **Разделительные символы во входных данных**: злоумышленник систематически пробует внедрение разделительных символов на известных входных данных, каждый раз наблюдая за реакцией ПО.<br>**Техники:** инъекция разделителей команд с помощью инструментов инъекции сетевых пакетов; ввод разделители команд с помощью фреймворков для веб-тестирования; ввод разделителей команд непосредственно в поля ввода. |
| | Реализация | **Использование вредоносных разделителей команд:** злоумышленник использует комбинации полезной нагрузки и тщательно размещенных разделителей команд для атаки на программное обеспечение. |
| Ущерб | Нарушение конфиденциальности, целостности, доступности | |
| Превентивные меры защиты информации | Выполнить проверку разрешительного списка на соответствие длины, типа и параметров команды.<br>Ограничить привилегии ПО, чтобы если команды обходят проверку ввода или процедуры фильтрации, то не выполняются под привилегированной учетной записью.<br>Использовать преобразования типов, такие как подготовленные операторы JDBC. | |

В результате адаптации базы знаний, появляется возможность связать сценарий атаки с конкретными уязвимости из базы знаний БДУ ФСТЭК.

Для улучшения пользовательской эксплуатации сервиса агрегации данных и рисканализа уязвимостей был разработан паспорт вектора атак. Приведен пример (табл. 2) для CAPEC-15.

Также было внедрено поле соотношения идентификатора типа ошибки и статуса типа ошибки, в виду того, что некоторые типы не могут применяться в реальных атаках на АИС.

Модернизация данной базы позволит российским разработчикам и специалистам в области обеспечения ИБ глубже понимать намерения злоумышленника, что в свою очередь приведет к повышению защищенности АИС. Разграничение типов ошибок по классам позволит не учитывать при оценке критичности уязвимостей общие классы ошибок (родительские), которые могут привести к рассмотрению ошибочных уязвимостей и ввести в заблуждение специалистов по ИБ.

Таблица 2

Паспорт вектора атаки CAPEC-15

<table>
<tr><td>Идентификатор системы CAPEC</td><td colspan="2">CAPEC-15: Инъекция в команды с разделительными символами</td></tr>
<tr><td>Описание вектора атаки</td><td colspan="2">Злоумышленник использует полезную нагрузку разделительных символов в качестве точки входа, чтобы пройти через приложение и активировать дополнительные атаки с помощью SQL-запросов, команд оболочки, сканирования сети.</td></tr>
<tr><td>Тип атаки</td><td colspan="2">Внедрение неожиданных элементов</td></tr>
<tr><td rowspan="12">Соотношение типа ошибки CWE и статуса типа ошибки CWE</td><td>138 – неправильная обработка специальных элементов</td><td rowspan="2">Не рекомендовано для использования в реальных уязвимостях</td></tr>
<tr><td>697 – недостаточное сравнение</td></tr>
<tr><td>77 – неправильная обработка символов, встречающихся в команде</td><td rowspan="10">Разрешены для использования в реальных уязвимостях</td></tr>
<tr><td>78 – неправильная обработка специальных элементов в ОС</td></tr>
<tr><td>93 – неправильная обработка последовательности CRLF</td></tr>
<tr><td>146 – неправильная обработка разделителей выражений/команд</td></tr>
<tr><td>184 – неполный список запрещенных исходных материалов</td></tr>
<tr><td>185 – неправильное регулярное выражение</td></tr>
<tr><td>140 – неправильная обработка разделительных символов</td></tr>
<tr><td>157 – невозможность проверки парных разделительных символов</td></tr>
<tr><td>154 – неправильная обработка переменных разделительных символов</td></tr>
</table>

**Исследование базы знаний BDU ФСТЭК**

BDU ФСТЭК (Банк Данных Уязвимостей) – это список выявляемых уязвимостей и дефектов безопасности [2].

Цель BDU – выявлять, описывать и структурировать информацию об уязвимостях. BDU позволяет специалистам по безопасности, сканерам уязвимостей и другим базам данных уязвимостей (например, НКЦКИ) получать и обмениваться информацией о конкретных слабых местах систем.

**Актуальность использования базы знаний BDU**

База знаний BDU играет ключевую роль в индустрии отечественной ИБ, предлагая стандартизированный список уязвимостей. Банк данных поддерживается ГНИИ ПТЗИ ФСТЭК России, пополняется и обновляется несколько раз в неделю. Ведение базы знаний является задачей, затрагивающей национальные, экономические и политические интересы РФ, поэтому в последние несколько лет регулятор максимально интенсивно ведет работу по разработке и поддержанию информационного обеспечение базы в актуальном состоянии.

База BDU включает в себя паспорт уязвимостей, назначение уникального идентификатора и ссылки на дополнительную информацию. На сегодняшней день на информационном ресурсе размещено 57,039 уязвимостей [3].

BDU имеет связь с оценками уязвимостей CVSS и информацию CWE. Такая интеграция обогащает базу BDU, делая её более полезной для анализа угроз и управления рисками. Таким образом, вырисовывается смысловая последовательность «адаптированный шаблон атаки CAPEC – тип ошибки программного обеспечения CWE – уязвимость BDU».

База BDU предоставляет оценки CVSS, включающие в себя базовые метрики, временные метрики и контекстные метрики. Эти данные могут быть использованы для качественной и количественной оценки критичности, что важно для планирования мер по оценке и регулированию рисков, а также управления угрозами.

В виду того, что идентификатор BDU связывает выявленную уязвимость с идентификатором CVE, принято решение оставить унифицированный идентификатор CVE для дальнейшей работы. В свою очередь полностью отказываться от идентификатора BDU не является адекватным, так как некоторые уязвимости явно не связываются с CVE. Таких уязвимостей на данный момент 1364, и чтобы охватывать полное множество уязвимостей оставим идентификатор ФСТЭКа для выявленного множества.

Используя информацию со страницы уязвимости, формируется паспорт уязвимости (табл. 3).

Информационный ресурс ФСТЭК предоставляет полное описание уязвимости начиная с унифицированного идентификатора, заканчивания ссылками на источники. База позволяет связать адаптированный шаблон атаки CAPEC с уязвимостями через идентификатор кода ошибки CWE.

**База знаний НКЦКИ**

НКЦКИ (Национальный координационный центр по компьютерным инцидентам) обеспечивает координацию деятельности субъектов Российской Федерации по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты [4].

В базе знаний представлены уязвимости, которые были зарегистрированы при реальных инцидентах на инфраструктуру субъекта РФ и представляют наибольшую угрозу безопасности информации. База знаний обновляется несколько раз в неделю.

Основываясь на данных, представленных в базе знаний будем выявлять такие уязвимости, успешная эксплуатация которых подтверждена реальными инцидентами, то есть уязвимость, имеющееся в паре с вектором атаки является успешной реализаций сценария атаки. Исходя из этого утверждения становится возможным модернизация методического обеспечения оценки рисков, включающая в себя такие показатели как успешность реализации сценария и критичность.

База НКЦКИ включает в себя идентификатор уязвимости CVE, описание уязвимости, категорию уязвимого продукта, уровень опасности по CVSS, возможные последствия, метод эксплуатации, а также идентификатор программной ошибки CWE. Всего в базе НКЦКИ на сегодняшний день насчитывается 7666 уязвимостей.

Для удобства дальнейшей работы и агрегации данных проведем парсинг всей базы НКЦКИ с помощью использования специального скрипта. Так как ценность для нас представляет непосредственно

идентификатор уязвимости, его и будем заносить в нашу базу данных.

Таблица 3

Паспорт уязвимости

| | |
|---|---|
| **Идентификатор уязвимости** | CVE-2024-1480 |
| Описание уязвимости | Уязвимость микропрограммного обеспечения программируемых логических контроллеров Unitronics Vision, связанная с хранением паролей в восстанавливаемом формате. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить пароль «Информационного режима» (Information Mode) в виде открытого текста |
| Производитель | Unitronics |
| Наименование и версии ПО | Unitronics Vision (версии 230, 280, 290, 530, 120) |
| Тип ПО | ПО АСУ ТП |
| Тип ошибки | Хранение паролей в восстанавливаемом формате |
| **Идентификатор ошибки** | CWE-257 |
| Класс уязвимости | Уязвимость архитектуры |
| Дата выявления | 18.04.2024 |
| **Базовый вектор уязвимости** | CVSS 3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |
| **Уровень опасности уязвимости** | Высокий уровень опасности (базовая оценка CVSS 3.0 составляет 7,5) |
| Возможные меры по устранению уязвимости | Компенсирующие меры:<br>- изменение пароля "Информационного режима" (Information Mode) с помощью SI 253;<br>- реализация многофакторного доступа к ПЛК с помощью SB 314;<br>- применение многофакторной VPN для защиты службы от удаленного доступа;<br>- ограничение доступа к ПЛК по протоколу TCP/20256, либо путем изменения порта программатора по умолчанию, либо путем применения многофакторной VPN для защиты службы от удаленного доступа;<br>- ограничение доступа к оборудованию из внешних телекоммуникационных сетей; |
| **Статус уязвимости** | Подтверждена производителем |
| Способ эксплуатации | Нарушение аутентификация |
| **Наличие эксплойта** | - |
| **Способ устранения** | - |
| Информация об устранении | - |
| Ссылки на источники | https://www.dragos.com/advisory/unitronics-vision-standard/<br>https://www.cybersecurity-help.cz/vdb/SB2024041916 |

Рассмотрим карточку уязвимости CVE-2023-49606 в качестве примера и выделим наиболее ценные информационные поля (рис. 1-2).

В карточке уязвимости имеется идентификатор уязвимости, через который можно связать базу знаний НКЦКИ и BDU ФСТЭК.

В виду того, что карточка уязвимостей имеет для нас не информативный формат, продолжим работу с новой созданной базой данных на основе выборки уязвимостей с НКЦКИ из базы знаний BDU.

Таким образом, имеется уверенное подспорье для проведения рисканализа уязвимостей, реально эксплуатируемых в кибератаках.

На данном этапе представляется возможным составить дерево проектной деятельности, на основе вышеописанных баз знаний и агрегации данных (рис. 3). Данное дерево позволяет рассмотреть для множества шаблонов атак CAPEC, соответствующие им типы ошибок CWE, которые могут быть проэксплуатированы в уязвимостях из базы знаний BDU и провести выборку тех уязвимостей НКЦКИ, факт успешной эксплуатации которых был зарегистрирован.

В виду информативности и удобства использования формы паспорта уязвимостей и калькулятора рисков из базы знаний БДУ, после выборки целесообразно перейти к информационному ресурсу, поддерживаемому ФСТЭК России.

Таким образом, следующим шагом можно провести описание пар вектор-уязвимость, а также сформировать риск-ландшафт для пар вектор атаки-уязвимость.

| | |
|---|---|
| Дата бюллетеня | 13 мая 2024 |
| Идентификатор уязвимости | MITRE CVE-2023-49606 |
| Описание уязвимости | Выполнение произвольного кода в tinyproxy |
| Наименование ПО | tinyproxy |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уровень опасности | Критический (9.8) |
| Вектор атаки | Сетевой |
| Возможные последствия | ACE - Выполнение произвольного кода (Arbitrary Code Execution) |

Рис. 1. Карточка уязвимости НКЦКИ

| | |
|---|---|
| Программная ошибка | (416) Использование после освобождения |
| Метод эксплуатации уязвимости | Отправка специально созданного HTTP-запроса. |
| Взаимодействие с пользователем | Нет |
| Дата выявления | 2 мая 2024 |
| Дата последнего обновления информации об уязвимости | 2 мая 2024 |
| Наличие обновления | Нет |
| Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами. | |
| Источники | http://talosintelligence.com/vulnerability_reports/TALOS-2023-1889 |

Рис. 2. Карточка уязвимости НКЦКИ

**Модернизация методического обеспечения калькуляции рисков**

Для обеспечения оценки рисков используем формулу расчета для каждой из пар «вектор атаки – уязвимость».

$$Risk_{ij} = P_{ij} \times U_{ij},$$

где $Risk_{ij}$– это риск сочетания *i*-го вектора атаки с используемой *j*-ой уязвимостью;

$P_{ij}$– вероятность успешности сочетания *i*-го вектора атаки и *j*-ой уязвимости;

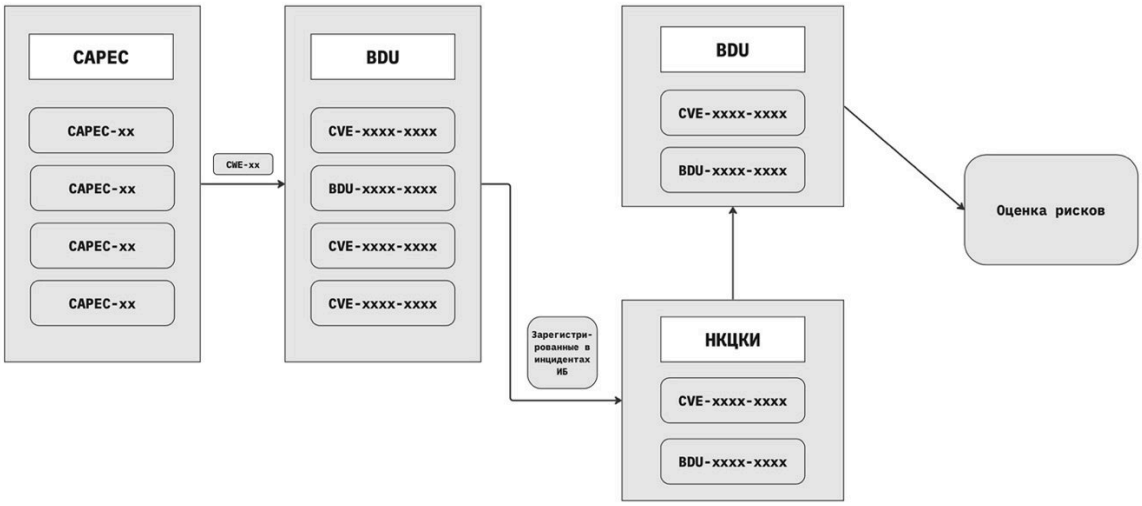



Рис. 3. Дерево проектной деятельности

Реальный практический интерес представляет собой рассмотрение массированной атаки, когда тот или иной вектор реализуется многократно. Допустим, что такой сценарий реализуется в отношении одной из уязвимостей защищаемой системы. Тогда вероятность успеха единичной атаки может быть выражена через частоту данного события, значение которой предлагает Банк данных угроз безопасности информации [3].

$$p_{ij} = \frac{F_{ij}}{\sum_S F_{iS}},$$

где: $F_{ij}$ – частота успешного использования *j-ой* уязвимости при реализации атаки посредством *i-го* вектора;

$\sum_S F_{iS}$ – сумма частот всех уязвимостей, которые могут быть использованы для успешной атаки вектором *i*.

Пусть за исследуемый период в отношении избранной или единственной уязвимости защищаемой системы осуществляется *n* атак *i-ым* вектором. Тогда согласно биномиальному распределению [5] вероятность $k$ успешных атак может быть определена следующим выражением:

$$P_{ij}(k) = \binom{n}{k} p_{ij}^k \left(1 - p_{ij}\right)^{n-k} = \frac{n!}{(n-k)!k!} p_{ij}^k \left(1 - p_{ij}\right)^{n-k}, \quad (1)$$

где наиболее ожидаемый случай, когда $k$ составляет целую часть $nP_{ij}$.

В том случае, когда вероятность успеха единичной атаки вектора *i* на *j-ю* уязвимость имеет весьма невысокое значение, злоумышленник старается организовать поток таких атак с интенсивностью $\lambda = np_{ij}$, где $n$ – количество атак в этой серии. Фактически успешность реализации атаки достигается наращиванием $n$ и тогда вероятность *k-раз* поразить атакуемую систему определяется пуассоновским распределением [6]:

$$P(k) = \frac{\lambda^k}{k!} e^{-\lambda}, \quad (2)$$

где наиболее ожидаемое значение $k$ стремится к $\lambda$.

В свою очередь, если ставится задача определения вероятности использования уязвимости в результате n атак в заданном векторе *i*, то целесообразно применять геометрическое распределение [7]:

$$P(n) = p_{ij}\left(1 - p_{ij}\right)^{n-1}, \qquad (3)$$

где наиболее ожидаемое количество атак приближается к $1/p_{ij}$.

Эффективно построенный сценарий *i-го* вектора потребует минимальное количество атак для использования *j-ой* уязвимости.

В свою очередь возникающий при таком раскладе ущерб может быть оценен через коэффициент критичности данной уязвимости для защищаемой системы, определяемый через Методику оценки критичности уязвимостей [8]. Здесь представляется возможным использование следующего подхода:

$$U_{ij}(\xi) = \xi \frac{K_{ij}}{\sum_S K_{iS}} U_{ij}, \qquad (4)$$

где: $U_{ij}$ – ущерб, наносимый вектором *i* через уязвимость *j* в результате единичной атаки.

Этот параметр представляется возможным оценить с использованием данных сконцентрированных в UNSW-NB15 [9]. Причем, необходимо учитывать вид наносимого ущерба. При нарушении доступности уместно оценивать время простоя $\Delta t_{ij}$ и тогда:

$$U_{ij} = \frac{\Delta t_{ij}}{\sum_S \Delta t_{iS}},$$

В иных случаях, а именно при нарушении конфиденциальности или целостности, следует учитывать долю утраченных или утекших данных.

Наиболее ожидаемым является случай, когда это происходит пропорционально критичности уязвимостей:

$$\xi_{i1} = \left[\frac{K_{i1}}{\sum_{j=1}^{m} K_{ij}}\right],$$

где [...] – оператор извлечения целой части рассчитанного значения.

Для оценки ущерба уместно воспользоваться выражениями (2) и (3), где параметр $\xi$ будет заменяться значениями из выражения (4). В результате получим:

$$U_{ij}(\xi) = \left[\frac{K_{im}}{\sum_{j=1}^{m} K_{ij}}\right] \frac{K_{ij}\Delta t_{ij}}{\sum_S K_{iS} \sum_S \Delta t_{iS}}, \qquad (5)$$

Исходя из всего вышеизложенного для оценки риска для k успешных реализаций набора сценариев n воспользуемся выражениями (1) и (5). В результате чего получим:

$$Risk_{ij} = \frac{n!}{\left(n - np_{ij}\right)! np_{ij}!} p_{ij}^{np_{ij}} \left(1 - p_{ij}\right)^{n - np_{ij}} \left[\frac{K_{im}}{\sum_{j=1}^{m} K_{ij}}\right] \frac{K_{ij}\Delta t_{ij}}{\sum_S K_{iS} \sum_S \Delta t_{iS}}.$$

Для оценки риска, когда вероятность успеха единичной атаки вектора *i* на *j-ю* уязвимость имеет весьма невысокое значение воспользуемся выражениями (2) и (5). В результате чего получим:

$$Risk_{ij} = \frac{np_{ij}{}^{k}}{k!} e^{-np_{ij}} \left[\frac{K_{im}}{\sum_{j=1}^{m} K_{ij}}\right] \frac{K_{ij}\Delta t_{ij}}{\sum_S K_{iS} \sum_S \Delta t_{iS}}.$$

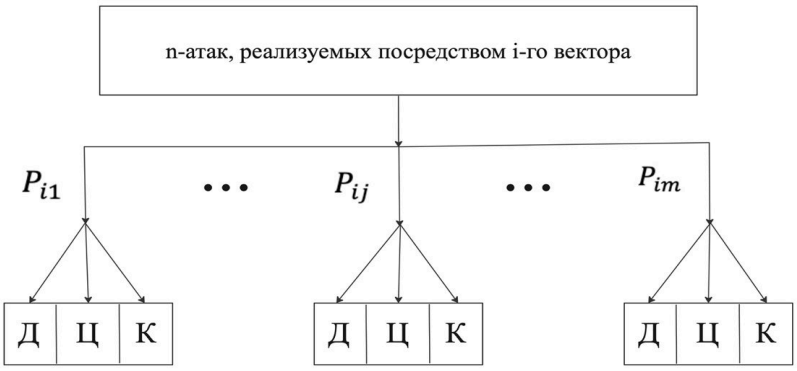
Для оценки риска в результате n атак в заданном векторе *i* воспользуемся выражениями (3) и (5). В результате чего получим:

$$Risk_{ij} = p_{ij}\left(1 - p_{ij}\right)^{n-1}\left\lfloor\frac{K_{im}}{\sum_{j=1}^{m} K_{ij}}\right\rfloor\frac{K_{ij}\Delta t_{ij}}{\sum_S K_{iS}\sum_S \Delta t_{iS}}.$$

Для обобщения и визуализации процедур рисканализа потока кибератак, разложим все действия по этапам и сущностям реализуемых процедур (табл. 4).

Таблица 4

Иллюстрация процедур риск-анализа потока кибератак

| Этап риск-анализа | Сущность реализуемых процедур риск-анализа кибератак |
|---|---|
| Этап оценки вероятности $P_{ij}$ успеха атаки посредством i-го вектора на j-ую уязвимость по видам Д-, Ц- и К-ущерба |  <br>m-количество уязвимостей, используемых i-ым вектором атаки;<br>Д – нарушение доступности информации;<br>Ц – нарушение целостности информации;<br>К – нарушение конфиденциальности информации.<br>Атаки «падают», как шары, в 3m ячеек их исходов по видам уязвимостей и разновидностям наносимого ущерба. |
| Этап оценки Д-, Ц- и К- ущербов от атак i-го вектора на j-ю уязвимость | $U_{ijД}$<br>$= (\text{время простоя}) \times (\text{ценность единицы времени простоя});$<br>$U_{ijЦ} = (\text{объем утраченной информации}) \times$<br>$\times (\text{ценность единицы утраченной информации});$<br>$U_{ijК} = (\text{объем скомпрометированной информации}) \times$<br>$\times (\text{ценность единицы скомпрометированной информации})$ |
| Этап оценки риска успешной реализации i-го вектора на j-ю уязвимость | $Risk_{ij} = \sum_{j=1}^{m} n_{ij}\left(\alpha_{ij}U_{ijД} \oplus \beta_{ij}U_{ijЦ} \oplus \gamma_{ij}U_{ijК}\right),$<br>где $n_{ij}$ - количество успехов атаки i-ым вектором на j-ую уязвимость и $\sum_{j=1}^{m} n_{ij} = n$;<br>$\alpha_{ij}, \beta_{ij}, \gamma_{ij}$- коэффициенты, принимающие значения 1 или 0 в зависимости от наличия или отсутствия Д-, Ц- и К- ущербов при реализации атаки i-ым вектором на j-ю уязвимость |

**Заключение**

Таким образом, при модернизации методического обеспечения сервиса агрегации данных и рисканализа уязвимостей, были предприняты шаги для адаптации проектной деятельности под нынешние реалии отечественного рынка программных и программно-аппаратных изделий. Произведена адаптация базы знаний CAPEC под русскоязычную аудиторию и выявление векторов, атакующих АИС. Также был выполнен переход от иностранных ресурсов к отечественным базам знаний БДУ ФСТЭК и НКЦКИ, которые полностью охватывает весь спектр уязвимостей, выявляемых непосредственно в эксплуатируемых программных и программно-аппаратных средствах на

территории РФ.

Проведена модернизация методического обеспечения калькуляции рисков, включающее в себя рассмотрение массированной атаки, когда тот или иной вектор реализуется многократно, в том числе уделено внимание случаю, когда вероятность успеха единичного сценария весьма мала. Также решена задача определения вероятности использования уязвимости в результате n атак заданным вектором. Оценка ущерба, включает в себя: коэффициент критичности уязвимости, а также вовлечение таких параметров как время простоя и ценность единицы времени простоя – при нарушении доступности; объем утраченной информации и ценность единицы утраченной информации – при нарушении целостности; объем скомпрометированной информации и ценность единицы скомпрометированной информации – при нарушении конфиденциальности.

## Список литературы

1. The Common Attack Pattern Enumeration and Classification (CAPEC). URL: https://capec.mitre.org/ (дата обращения 28.04.2024).

2. Угрозы безопасности информации. URL: https://bdu.fstec.ru/vul (дата обращения 28.04.2024).

3. Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat

4. База знаний уязвимостей НКЦКИ. URL: https://safe-surf.ru/specialists/bulletins-nkcki/ (дата обращения 29.04.2024).

5. Остапенко Г.А. Оценка рисков и защищенности компьютерных систем для биномиального дискретного распределения вероятностей ущерба / Г.А. Остапенко, О.А. Казьмин, Е.В. Субботина, В.И. Неверко // Информация и безопасность. 2006. Т. 9. № 1. С. 86-91.

6. Андреев, Д. А. Концепция управления рисками информационных атак на основе распределения Пуассона / Д. А. Андреев, А. К. Пичугин // Информация и безопасность. 2008. Т. 11. № 3. С. 407-412.

7. Остапенко Г.А. Компьютерные системы: рисканализ для геометрического дискретного распределения вероятностей ущерба / Г.А. Остапенко, О.А. Казьмин, Е.В. Субботина, А.А. Переславцева // Информация и безопасность. 2006. Т. 9. № 1. С. 64-69.

8. Методический документ от 28.10.2022г. ФСТЭК России. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2 (дата обращения 30.04.2024).

9. UNSW_NB15.URL: https://www.kaggle.com/datasets/ (дата обращения 30.04.2024).

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 05.05.2024

**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

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

**Покудин Данила Сергеевич** – студент, Воронежский государственный технический университет, e-mail: danila.pokudin@inbox.ru
**Ноздрюхин Александр Александрович** – студент, Воронежский государственный технический университет, e-mail: sfrvvv@yandex.ru

# MODERNIZATION OF METHODOLOGICAL SUPPORT FOR AUTOMATED DATA AGGREGATION AND VULNERABILITY RISK ANALYSIS SERVICE

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

In order to modernize the methodological support of the automated service of data aggregation and vulnerability risk analysis, an improved adapted version of the CAPEC attack vector description is proposed. Transition from foreign knowledge bases CVE NIST and CVE KEV, supported by the U.S. Department of State, to the domestic development of knowledge base BDU FSTEC and knowledge base NCIRCC, which covers the entire range of vulnerabilities, the exploitation of which is registered in the territory of the Russian Federation. A modernized risk calculation block is also presented, which includes consideration of a massive attack when one or another vector is implemented multiple times. Modernization allows to adapt the methodological support to the realities of modern State policy of the Russian Federation.

Keywords: information, security, vulnerability, attack vector, inline cyberattacks, risk.

Submitted 05.05.2024

**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
**Nikita N. Korvyakov** – student, Voronezh State Technical University, e-mail: korvyakov48@yandex.ru
**Danila S. Pokudin** – student, Voronezh State Technical University, e-mail: danila.pokudin@inbox.ru
**Alexander A. Nozdryukhin** – student, Voronezh State Technical University, e-mail: sfrvvv@yandex.ru