DOI 10.36622/VSTU.2023.26.1.011
УДК 004.056.5

СОЗДАНИЕ «КИБЕРПОЛИГОНА»: РЕАЛИЗАЦИЯ ИНФОРМАЦИОННОГО КАРТОГРАФИРОВАНИЯ РИСКОВ, СВЯЗАННЫХ С ПУБЛИКАЦИЕЙ СВЕДЕНИЙ ОБ УЯЗВИМОСТЯХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А.Л. Сердечный, М.А. Булычев, А.А. Гончаров, М.И. Ярмонов, А.Ю. Егоров

Статья посвящена вопросам создания модуля информационного картографирования рисков, связанных с публикацией сведений об уязвимостях программного обеспечения в рамках проекта «Киберполигон». Потребность в данном проекте обусловлена необходимостью тренировки навыков противодействия как специалистов в сфере информационной безопасности, так и студентов данной предметной области. Наглядное представление различных классов уязвимостей, и связанных с ними рисков реализации угроз безопасности информации, позволяет проводить своевременный процесс приоритезации, аналитики и снижения ущерба информационным системам. Целью создания данного модуля является повышение качества и результативности учебного процесса при исследовании атак на информационные системы за счет применения метода информационного картографирования к источникам, содержащим сведения об уязвимостях программного обеспечения. Для этой цели был разработан облик блока информационного картографирования рисков с интегрированными модулями тренинга в сфере информационного противоборства, который представляется вниманию научной общественности.

Ключевые слова: информационная картография, киберполигон, платформа картографирования рисков, анализ, визуализация.

Введение

Задача систематизации сведений об уязвимостях программного обеспечения не теряет своей актуальности на протяжении не одного десятилетия, прошедшего с момента появления первых баз данных, агрегирующих информацию о недостатках программного обеспечения [1,2]. В связи с развитием информационных технологий каждый год появляется новый класс уязвимостей, о чем свидетельствует постоянное расширение номенклатуры стандарта CWE (Common Weakness Enumeration) [3]. Еженедельно в базах данных публикуются сведения о сотнях новых уязвимостях (в том числе уязвимостей «нулевого дня»), представляющих большую опасность защищаемой информации.

Наряду с базами данных уязвимостей существуют информационные ресурсы, аккумулирующие наборы данных об эксплоитах (эксплойт – средство использования уязвимости для реализации несанкционированного воздействия на какой-либо компонент информационной системы или обрабатываемую в ней информацию).

В связи с этим перед сообществом экспертов в области защиты информации остро стоит проблема систематизации и пиритизации такого потока информации об уязвимостях, а также проблема подготовки специалистов, которые могут выявлять, оценивать и устранять уязвимости программного обеспечения.

Немаловажным остается вопрос представления собранной информации в удобном виде для повышения эффективности работы аналитика сетевых рисков и администратора безопасности.

Одним из подходов решения обозначенных проблем является использование методов машинного обучения для автоматического анализа сведений об уязвимостях программного обеспечения. В настоящее время существуют проекты, позволяющие интерпретировать машинный код на языке, понятном человеку [4]. Однако в настоящее время нет данных о существовании эффективных аналитических инструментов для пиритизации сведений об уязвимостях программного обеспечения, а также для автоматического определения

принадлежности с приемлемой точностью уязвимостей к определённому классу по их текстовому описанию. Кроме того, использование автоматических алгоритмов не даёт понимания о системе отношений между различными уязвимостями и связи с особенностями защищаемых информационных систем, что крайне важно для решения задачи подготовки соответствующих специалистов.

В данных условиях для решения обозначенных вопросов наиболее рациональным представляется использование аппарата информационного картографирования. Ранее информационно-аналитическое картографирование было применено по отношению к сведениям о музыкальных предпочтениях, автономных системах и публикациях в сфере информационной безопасности. Опытным путем было установлено, что использование информационной картографии ускоряет процесс понимания проблематики того или иного инцидента [1-3].

Применение метода информационного картографирования [5] для систематизации и пиритизации уязвимостей предполагает создание соответствующего инструментального обеспечения, включающего подсистемы сбора, хранения и визуализации данных об уязвимостях и эксплойтах. Разработка облика и прототипа такого средства осуществлено в рамках реализации проекта «Киберполигон» (концепция данного проекта заключается в объединении вышеупомянутых составных частей процесса анализа инцидентов информационной безопасности и модулей для тренинга навыков противодействия деструктивному воздействию, представляемых в удобном виде для пользователя системы).

Создание подобного программно-прикладного комплекса позволит наглядным образом рассмотреть ареалы обитания (кластеры) уязвимостей программного обеспечения используемых в контексте нанесения ущерба целевой инфраструктуре за счет применения картографического подхода, повысить качество и результативность учебного процесса благодаря возможности выработки навыков противодействия инцидентам деструктивного воздействия. Функциональность комплекса также предполагает реализацию предложенной методики расчета риска наступления неблагоприятного события, связанного с эксплуатацией уязвимостей программного обеспечения.

Требования к информационному обеспечению проекта «Киберполигон» в части сбора, хранения и картографирования сведений об уязвимостях программного обеспечения

Требования к информационному обеспечению средства сбора, хранения и картографирования сведений об уязвимостях программного обеспечения разработаны с учётом опыта создания прототипа системы картографирования рисков защищаемого киберпространства, изложенных в работе [6].

Для задач сбора и хранения сведений об уязвимостях программного обеспечения определена модель данных, представленная в виде графа (рис. 1).

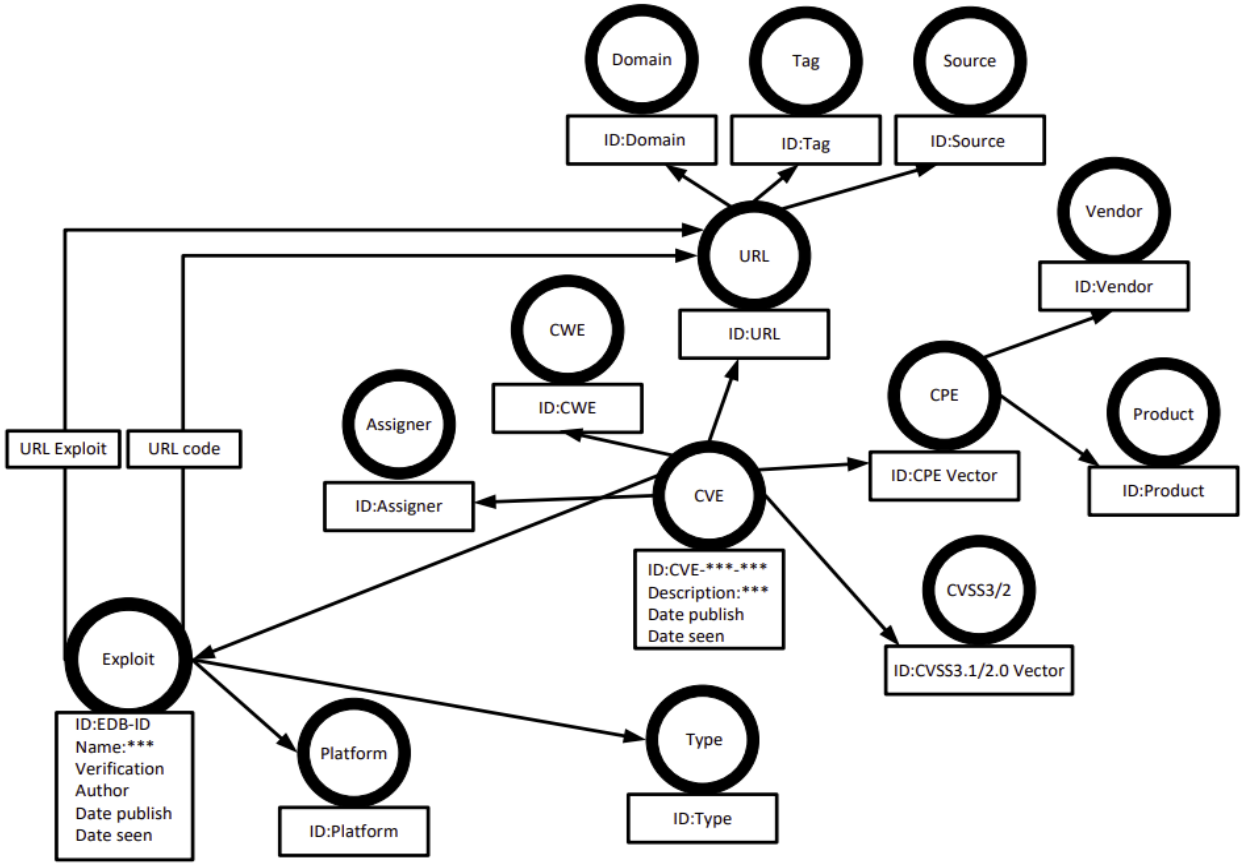

Рис. 1. Модель данных, использованная для представления сведений об уязвимостях программного обеспечения

В соответствии с обозначенной моделью данных разработаны средства сбора сведений об уязвимостях для следующих информационных источников:

- базы данных уязвимостей NVD [1];
- базы данных эксплойтов EDB [2].

Модули сбора представляют собой скрипты на языке программирования Python с использованием библиотеки для парсинга веб-ресурсов и файлов формата .json под названием Beautiful Soup4.

В вопросах картографирования рисков связанных с публикацией сведений об уязвимостях программного обеспечения необходимы следующие подходы:

– принцип совместного информационно-аналитического картографирования;

– возможность представления карты в виде удобного для пользователя системы модуля.

Принцип совместного подхода в вопросах картографирования заключается в размещении карты таким образом, чтобы n-е количество пользователей могли получать возможность взаимодействия с картой, не мешая друг другу.

Интерфейс, ориентированный на пользователя обусловлен тем, что каждый пользователь проекта «Киберполигон» без углубленных технических знаний мог использовать данный модуль.

Изучая аналоги, можно выяснить, что всем выдвинутым требованиям соответствует картографический сервис QGIS, который предоставляет как совместную модель картографирования, так и представление информационно-аналитической карты в виде удобного в использовании ресурса.

К плюсам системы можно отнести:

– большую библиотеку расширений, решающую все возможные вопросы и задачи в сфере картографирования;

– взаимодействие с серверной архитектурой на уровнях СХД;

– создание ландшафта картографирования без использования сторонних решений.

Обозначенные выше требований к подсистемам сбора, хранения и визуализации сведений об уязвимостях программного обеспечения были реализованы в прототипе, схема которого представлена на рис 2.

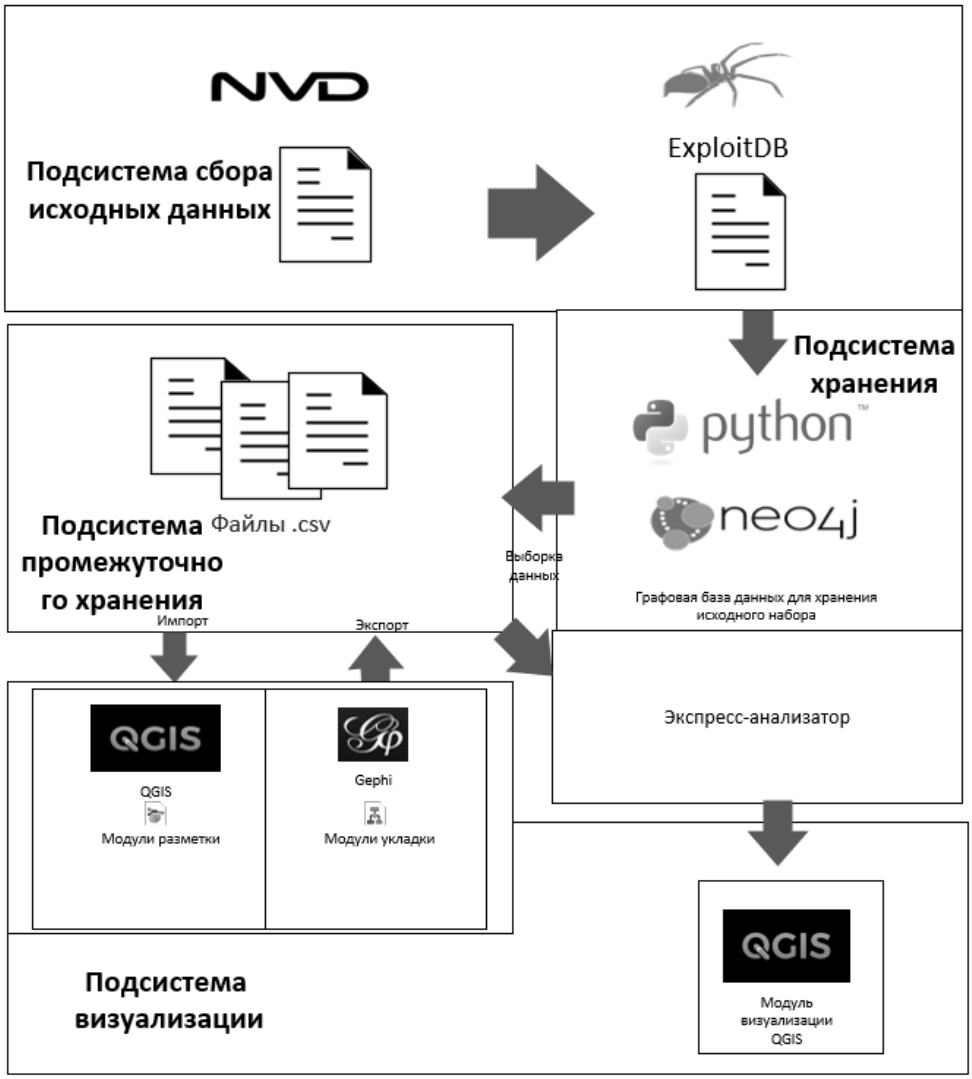

Рис. 2. Структурно-функциональная схема модуля информационно-аналитического картографирования

Методика оценки и визуализации рисков программного обеспечения, вызванных уязвимостями и эксплойтами программных продуктов в виде информационно-аналитической карты.

В настоящее время вопросу анализа рисков возникновения деструктивного воздействия посвящено множество научно-исследовательских работ [10-12]. В классическом понимании термина риск представляет следующую формулу:

$$Risk = P(U) \times U,$$

где Risk – риск наступления неблагоприятного события;

P(U) – вероятность реализации угрозы;

U – количественная мера ущерба от реализации угрозы.

Вышеописанный подход в подобной вариации не всегда позволяет получить достоверную количественную оценку опасности того или иного неблагоприятного события. Исходя из этого одним из вариантов развития событий будет использование альтернативного стандарта оценки рисков с применением качественного анализа критериев вектора уязвимостей, либо модернизация существующего подхода

Таким образом наиболее приемлемым вариантом оценки будет совместное использование стандарта количественной оценки CVSS 3.1 и метода экспресс-анализа в виде получения интегральной оценки рисков.

Переходя к конкретизации данного вопроса необходимо указать, что метод экспресс-анализа будет основан на тройственной системе представления проблематики объектов защиты «Тип атаки→Вид уязвимости→Разновидность атакуемых объектов» (рис. 3).

Обращаясь к тройственной модели, представленной на рис. 3 можно выделить, что анализ вероятности наступления ущерба в конкретном случае нацелен на частотный анализ возникновения инцидентов информационной безопасности.

Интересующими в данном контексте метриками частоты будут:

– P_{ay}- частота реализации атак через виды уязвимостей;

– P_{yo} – частота использования уязвимостей для успешных атак на объекты заданной разновидности;

– P_{oy}-частота наступления величин нормированного ущерба.

Обращаясь к требованиям к системе сбора информации, связанной с публикациями сведений о уязвимостях и эксплойтах программного обеспечения в централизованную базу данных, можно выявить, что частоты можно рассчитать с помощью применения математических операций над собранным массивом данных по отношению к метрикам, содержащимся в информационном хранилище по отношению к каждой уязвимости.

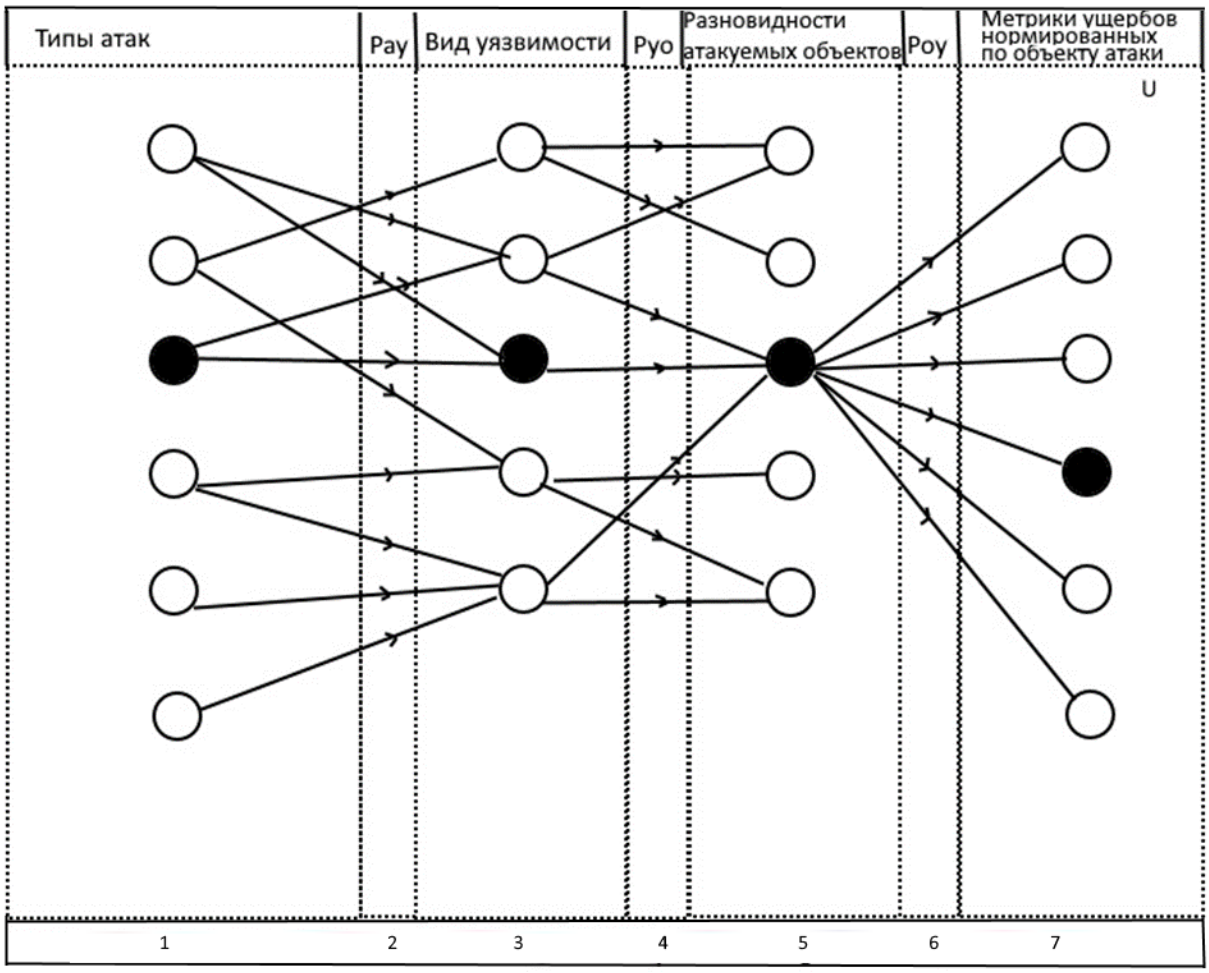

Рис. 3. Схема объектов оценки риска по тройке
«Тип атаки→Вид уязвимости→Разновидность атакуемых объектов»

Таким образом частота реализации атак через виды уязвимости P_{ay} может быть представлена в виде отношения количества атак по конкретному типу к общему количеству атак за выбранный промежуток времени.

$$Pay = \frac{n(type)}{n},$$

где Pay – частота реализации атак через виды уязвимостей;

n(type) – множество атак по конкретному типу за выбранный период времени;

n – множество всех атак за конкретный период времени.

Частота использования уязвимостей для успешных атак на объекты заданной разновидности в свою очередь подлежит наиболее детальному рассмотрению, поскольку является сложно структурированным операндом в данном случае.

Рассматривая частоту реализации атак по виду, не было необходимости в сборе информации об успешно совершенных атаках.

Зачастую уязвимости прикладного и системного программного обеспечения описываются в процессе изучения конечного устройства и не содержит в себе исходного кода деструктивного воздействия (самого эксплойта). Исходя из этого целесообразным будет суждение о том, что описанная уязвимость, рассматриваемая разрыве по отношении к исходному коду атаки не несет в себе никакой практической ценности в процессе деструктивного воздействия.

Иными словами уязвимость, внесенная в бюллетень отчета выявленных деструктивных сущностей, без описанного эксплойта не является показателем успешно проведённой атаки.

Беря во внимание все вышеописанные замечания и проведя структурный анализ метрик внутри информационной базы знаний об уязвимостях и эксплойтах программного обеспечения, частота успешно совершенных атак будет считаться как отношение количества эксплойтов к общему количеству уязвимостей за данный период.

$$Pyo = \frac{count(Exploit)}{count(CVE)},$$

где Pyo - частота использования уязвимостей для успешных атак на объекты заданной разновидности;

count (Exploit) – количество эксплоитов за конкретный период времени;

count (CVE) – количество всех уязвимостей за конкретный период времени.

Третья метрика частотного анализа при оценке рисков будет представлять собой частоту наступления величин нормированного ущерба. Оценить данный ущерб возможно с применением механизма совмещения вышеописанного стандарта CVSS 3.1 и методики частотного анализа. В выбранном направлении данная метрика может быть отражена в виде частоты величины Base Score представляющей собой количественную оценку ущерба от реализации атаки с использованием уязвимости программного обеспечения. Таким образом частота нормированного ущерба будет представлять собой среднее значение количественной оценки ущерба, описанной в стандарте CVSS 3.1:

$$Poy = \frac{\sum(BaseScore)}{count(cvss3.1)} \times 10,$$

где *Poy* – частота наступления величин нормированного ущерба;

BaseScore – количественная оценка ущерба от реализации атаки с использованием уязвимости программного обеспечения;

count(*cvss*3.1) – количество векторов оценки опасности уязвимостей стандарта CVSS.

Так же необходимо рассмотреть последний показатель для расчёта интегральной оценки рисков U представляющий собой метрику (функцию) нормированных ущербов по ресурсу (кластеру) объекта атаки.

Важным замечанием будет то, что ущерб в заданный промежуток времени может быть рассчитан исключительно в прямой зависимости от объекта оценки (организации и ее инфраструктуры, подвергаемой экспресс-риск анализу).

Беря во внимание вышеописанное и цели разработки проекта «Киберполигон» как систему для тренировки противодействия атакам, необходимым и доставочным решением данного противоречия будет применение метода экспертных оценок для присвоения количественного значения функции ущерба.

Расставив оценки опасности кластеров уязвимостей согласно методу экспертных оценок, можно приравнять их к значению функции U и вывести формулу расчета риска нанесения ущерба при совмещении события

$$Score = U,$$

где Score – оценка ущерба от реализации уязвимости программного обеспечения;

U – функция ущерба.

Таким образом, риск, как вероятность наступления ущерба в контексте экспресс анализа будет выглядеть следующим образом:

$$Risk(U) = Pay \times Pyo \times [Poy \times U],$$

где Risk(U)- риск при совмещении события;

P_{ay} - частота реализации атак через виды уязвимостей;

P_{yo} - частота использования уязвимостей для успешных атак на объекты заданной разновидности;

P_{oy} - частота наступления величин нормированного ущерба;

U - функция ущерба.

Реализация блока информационного картографирования в контексте проекта «Киберполигон»

По средствам сформированных, модулей сбора и хранения данных, а также произведенной интегральной оценки согласно разработанной методики экспресс-анализа, осуществляется процесс формирование блока информационно-аналитического картографирования.

Подсистема сбора и хранения исходных данных осуществляет аккумуляцию информации по средствам языка Python 3.10 и системы управления базой данных Neo4j [7,8].

Для формирования ландшафта карты выборка данных из базы выгружается из подсистемы хранения в промежуточные файлы формата .csv. Данная выборка загружается в модуль потока данных для представления исходной информации в виде ландшафта информационной карты. Исходные данные образуют собой ландшафт исследуемого пространства по средствам применения к ним силового алгоритма укладки, осуществленного в программном обеспечении Gephi. В последующем, ландшафт выгружается в модуль картографирования для нанесения разметки.

После разметки необходимых данных производится процесс нанесения интегральной оценки рисков возникновения деструктивного воздействия, рассчитанной по средствам экспресс-анализатора. Данные из подсистемы промежуточного хранения в табличном виде в итоге отражаются в виде информационной карты в подсистеме визуализации (рис 2).

Проведя все необходимые манипуляции для реализации данного модуля, по средствам инструментов разметки были нанесены следующие слои информационной карты (рис 4):

− ареалы обитания уязвимостей программного обеспечения;

− тепловая карта распространения уязвимостей по кластерам;

− интегральная оценка риска возникновения деструктивного воздействия;

− обучающие модули для тренировки навыков эксплуатации и противодействия инцидентам нарушения информационной безопасности;

− типы ошибок CWE;

− уязвимое программное обеспечение.

Рис. 4. Информационная карта рисков эксплуатации уязвимостей программного обеспечения для уязвимостей, сведения о которых опубликованы в период с 2020 по 2022 годы [1]

Заключение

В статье были представлены результаты реализации модуля информационного картог рафирования рисков, связанных с публикацией сведений об уязвимостях программного обеспечения в рамках проекта «Каберполигон».

Модуль реализует предложенную методику оценки и визуализации рисков программного обеспечения, вызванных уязвимостями и эксплойтами программных продуктов в виде информационной карты.

В контексте оценки вероятности наступления деструктивного воздействия была предложена методика экспресс-анализа рисков, основанная на расчете интегральной оценки с использованием метрик частотности атак и ущерба.

В процессе анализа сконфигурированного модуля картографирования рисков связанных с публикацией сведений об уязвимостях программного обеспечения выявились следующие направления совершенствования и модификации данного программно-прикладного продукта:

− подключение средств искусственного интеллекта и машинного обучения в контексте подсказок по противодействию уязвимостям программного обеспечения;

− конфигурация веб-версии картографического сервиса с поддержкой совместной модели ведения модуля.

Список литературы

1. National Vulnerability Database // URL: https://nvd.nist.gov.ru (дата обращения 15.01.23).

2. Exploit Database // URL: https://www.exploit-db.com/ (дата обращения 15.01.23).

3. CWE - Common Weakness Enumeration // URL: https://cwe.mitre.org/ (дата обращения 15.01.23).

4. When Neural Model Meets NL2Code: A Survey / D. Zan, B. Chen, F. Zhang, D. Lu, B.

Wu, B. Guan, Y. Wang, J.-G. Lou. // URL: https://www.researchgate.net/publication/366423884_When_Neural_Model_Meets_NL2Code_A_Survey (дата обращения 15.01.23).

5. Остапенко, А.Г. Картография защищаемого киберпространства / А.Г. Остапенко, А.Л. Сердечный, А.О. Калашников; под общ. ред. Д.А. Новикова // Воронеж: Горячая линия - Телеком. 2022. 276с.

6. Сердечный А.Л. К вопросу о создании платформы картографирования рисков защищаемого киберпространства / А.Л. Сердечный, А.А. Гончаров, М.А. Булычев и др. // Информация и безопасность 2021 Т. 24. Вып. 4. С. 593-600.

7. Neo4j // URL: https://ru.wikipedia.org/wiki/Neo4j (дата обращения 15.01.23).

8. Python // URL: https://ru.wikipedia.org/wiki/python (дата обращения 15.01.23).

Государственный научно-исследовательский испытательный институт
проблем технической защиты информации ФСТЭК России
State science research experimental institute of technical information protection
problem of Federal service of technical an export control

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 20.01.2023

Информация об авторах

Сердечный Алексей Леонидович – канд. техн. наук, начальник лаборатории, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России, e-mail: alex-voronezh@mail.ru

Булычев Максим Александрович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Гончаров Андрей Андреевич – аспирант, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Ярмонов Максим Иванович – старший преподаватель, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Егоров Анатолий Юрьевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

CREATION OF A "CYBERPOLYGON": IMPLEMENTATION OF INFORMATION MAPPING OF RISKS ASSOCIATED WITH THE PUBLICATION OF INFORMATION ABOUT SOFTWARE VULNERABILITIES

A.L. Serdecniy, M.A. Bulychev, A.A. Goncharov, M.I. Yarmonov, A.Yu. Egorov

The article is devoted to the issues of creating an information mapping module for risks associated with the publication of information about software vulnerabilities within the framework of the Cyberpolygon project. The need for this project is due to the need to train counteraction skills of both specialists in the field of information security and students of this subject area. A visual representation of various classes of vulnerabilities, and the associated risks of information security threats, allows for a timely process of prioritization, analytics and damage reduction to information systems. The purpose of creating this module is to improve the quality and effectiveness of the educational process in the study of attacks on information systems by applying the method of information mapping to sources containing information about software vulnerabilities. For this purpose, the image of the risk information mapping unit with integrated training modules in the field of information warfare was developed, which is presented to the attention of the scientific community.

Keywords: information cartography, cyberpolygon, risk mapping platform, analysis, visualization.

Submitted 20.01.2023

Information about the authors

Alexey L. Serdechnyy – Cand. Sc. (Technical), Chief of Laboratory, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: alex-voronezh@mail.ru

Maxim A. Bulychev – Student, Voronezh State Technical University, email: mnac@comch.ru

Andrei A. Goncharov – Graduate Student, Voronezh State Technical University, email: mnac@comch.ru

Maxim I. Yarmonov – Senior Lecturer, Voronezh State Technical University, email: mnac@comch.ru

Anatolii Yu. Egorov – Student, Voronezh State Technical University, email: mnac@comch.ru