DOI 10.36622/VSTU.2022.25.2.013
УДК 004.41

СИСТЕМАТИЗАЦИЯ СВЕДЕНИЙ ОБ ОШИБКАХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННОЙ КАРТЫ И ОЦЕНКА ИХ ЗНАЧИМОСТИ

А.А. Гончаров, М.А. Тарелкин, А.Л. Сердечный

В статье представляются результаты построения и анализа информационной карты, систематизирующей сведения об ошибках программного обеспечения. В качестве исходных данных была рассмотрена информация, содержащаяся в базе данных уязвимостей National Vulnerability Database. Информационная карта позволила установиться взаимосвязи между классами программного обеспечения и характерными для них типами ошибок. Систематизация сведений об ошибках программного обеспечения в виде информационной карты позволяет оценить роль соответствующего фактора при определении приоритета обработки сведений о соответствующих уязвимостях с учётом их уровня опасности. Результатом является разработка рекомендаций по приоритизации уязвимостей в целях их первоочередной обработки и применения мер защиты для минимизации ущерба от их эксплуатации. Информационная карта сведений об ошибках программного обеспечения может являться основой для наглядного отображения рисков эксплуатации уязвимостей программного обеспечения.

Ключевые слова: информационная карта, уязвимость программного обеспечения, тип ошибки программного обеспечения, CWE.

Введение

Согласно сведениям, содержащимся в базах данных уязвимостей программного обеспечения (ПО), (таких как nvd.nist.gov [1] и bdu.fstec.ru [2]) количество обнаруживаемых уязвимостей в различных программных и аппаратных продуктах ежегодно растет. По данным национальной базы данных США NVD в 2019 году было опубликовано 16 518, а за 2021 год – 18 875. Аналогичный отечественный ресурс – Банк данных угроз безопасности информации (БДУ) ФСТЭК России, ориентирующийся на уязвимости в программных и аппаратных продуктах, которые используются в отечественных государственных информационных системах (ГИС) и на объектах критической информационной инфраструктуры (КИИ), также фиксирует существенный рост сведений об уязвимостях (за 2019 год было опубликовано 4892 уязвимости, за 2020 год – 5907, за 2021 год – 6431) [1,2].

В связи со значительным объемом сведений, которые необходимо проанализировать разработчикам программного обеспечения и администраторам безопасности информационных систем, чтобы учесть их при реализации защитных мер, возникает потребность определения приоритетов обработки поступающих сведений, что в свою очередь требует разработки критериев, позволяющих проранжировать уязвимости по уровню опасности или степени актуальности для конкретной информационной системы (ИС).

Выработка таких критериев невозможна без глубокого понимания свойств уязвимости программного обеспечения, основным из которых, пожалуй, является тип ошибки, из-за которой такая уязвимость существует. Комбинация данного фактора с классом программного обеспечения во многом определяется негативные последствия, к которым может привести успешная эксплуатация соответствующих уязвимостей.

При этом необходимо отметить, что количество различных типов ошибок также, как и количество классов программного обеспечения достаточно велико, что приводит к большому числу комбинаций, которые необходимо учесть при определении

© Гончаров А.А., Тарелкин М.А., Сердечный А.Л., 2022

корреляции указанных факторов с уровнем опасности уязвимостей.

В связи с этим в настоящей работе с целью систематизации сведений об ошибках программного обеспечения и возможности их анализа в контексте ранжирования уязвимостей программного обеспечения был применен картографический подход [3]. Благодаря ему разработана информационная карта, позволившая сформировать рекомендации по очередности обработки сведений об уязвимостях и применению мер защиты для минимизации ущерба от их эксплуатации. Данный подход целесообразно применять специалистам, занимающимся процессами управления уязвимостями (специалисты по защите информации, системные администраторы и др.).

Построение информационной карты

Для достижения поставленной цели были поставлены и решены следующие задачи.

Первая задача – построение информационной карты уязвимостей. Для ее построения была использована технология картографического поиска, подробно изложенная в работах [3-8]. В качестве исходных данных при построении графа и информационной карты уязвимостей использовалась информация, опубликованная в базе данных NVD. Выбор данного источника обуславливается тем, что NVD является наиболее крупной базой данных уязвимостей, так как она ориентирована на добавления программного обеспечения различного предназначения, в отличии от БДУ, которая ориентирована в основном на уязвимости, затрагивающие ГИС и КИИ.

Объектом исследования были выбраны уязвимости 2021 года, обладающие достаточной полнотой информации, т.е. наличием: описания, типа ошибки Common Weakness Enumeration (CWE), вектора CVSS, ссылок на источники, перечня программного обеспечения. Количество уязвимостей, удовлетворяющих вышеприведенным критериям составило 14 027 штук (данные действительны на 20.05.2022).

В рамках решения первой задачи была разработана и описана модель данных, в соответствии с которой будет храниться информация для последующей обработки. Модель данных представлена на рис. 1.

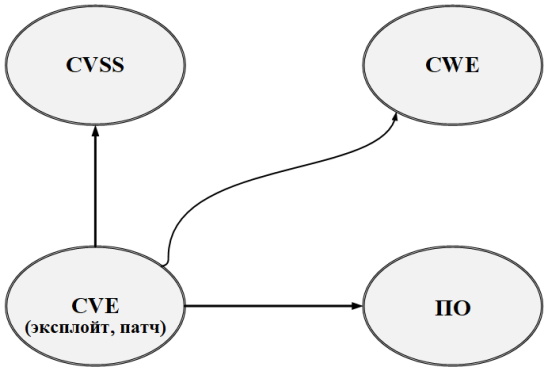

Рис. 1. Модель данных, использованная для построения информационной карты

Модель данных описывает сущности киберпространства (т.е. анализируемые объекты), которые связаны между собой в виде отношений. В табл. 1 приведено описание сущностей модели данных, а в табл. 2 – описание связей.

В настоящей работе граф является исходной формой для построения информационной карты [7,9]. Приведем порядок построения и основные характеристики графа.

Граф был уложен в двумерном пространстве с использованием «гравитационного» алгоритма ForceAtlas2 в программе для сетевого анализа и визуализации информации Gephi. Алгоритмы силовой укладки предполагают проведение расчетов сил «притяжения/отталкивания» для узлов, выступающих в роли «физических тел». Координаты узлов вычисляются таким образом, чтобы минимизировать интегральную оценку совокупности взаимосвязей всех пар узлов графа. При таком расположении графа наиболее связанные между собой узлы будут располагаться ближе друг к другу, чем менее связанные.

Таблица 1

Описание выделенных сущностей киберпространства

Сущность	Описание	Атрибуты	Примечание
CVE	Уникальные идентификаторы базы данных общеизвестных уязвимостей Common Vulnerabilities and Exposures (CVE)	Патч	Наличие исправления уязвимости.
		Эксплойт	Наличие эксплойта.
CVSS	Система оценки общих уязвимостей (Common Vulnerability Scoring System), открытый стандарт, используемый для расчета количественных оценок опасности уязвимостей в программных продуктах	-	Вектор CVSS в данной модели подразделяется на четыре категории по уровню опасности (низкий – от 0 до 3,9, средний – от 4,0 до 6,9, высокий – от 7,0 до 9,9 и критический – 10,0)
CWE	Система категорий для типов ошибок программного обеспечения CWE	-	-
ПО	Уязвимое программное обеспечение, которое категорировано согласно стандарту Common Platform Enumeration (CPE)	-	-

Таблица 2

Описание связей сущностей

Название связи	Сущность 1	Сущность 2	Описание	Тип связи
Base_Score_is	CVE	CVSS	Уязвимость относится к одному из 4-х уровней опасности	Одна к одной
Related_to	CVE	CWE	Уязвимость относится к одному из типов ошибок CWE	Одна ко многим
Vulnerable	CVE	ПО	Уязвимости подвержено ПО	Одна ко многим

По результатам укладки графа была осуществлена его автоматическая кластеризация с использованием Лейденского алгоритма и последующая ручная разметка с учётом выявленных топологических особенностей графа. Информационная карта взаимосвязей уязвимостей программного обеспечения, типов ошибок, классов программного обеспечения и уровней опасности (далее – информационная карта уязвимостей) представлена на рис. 2.

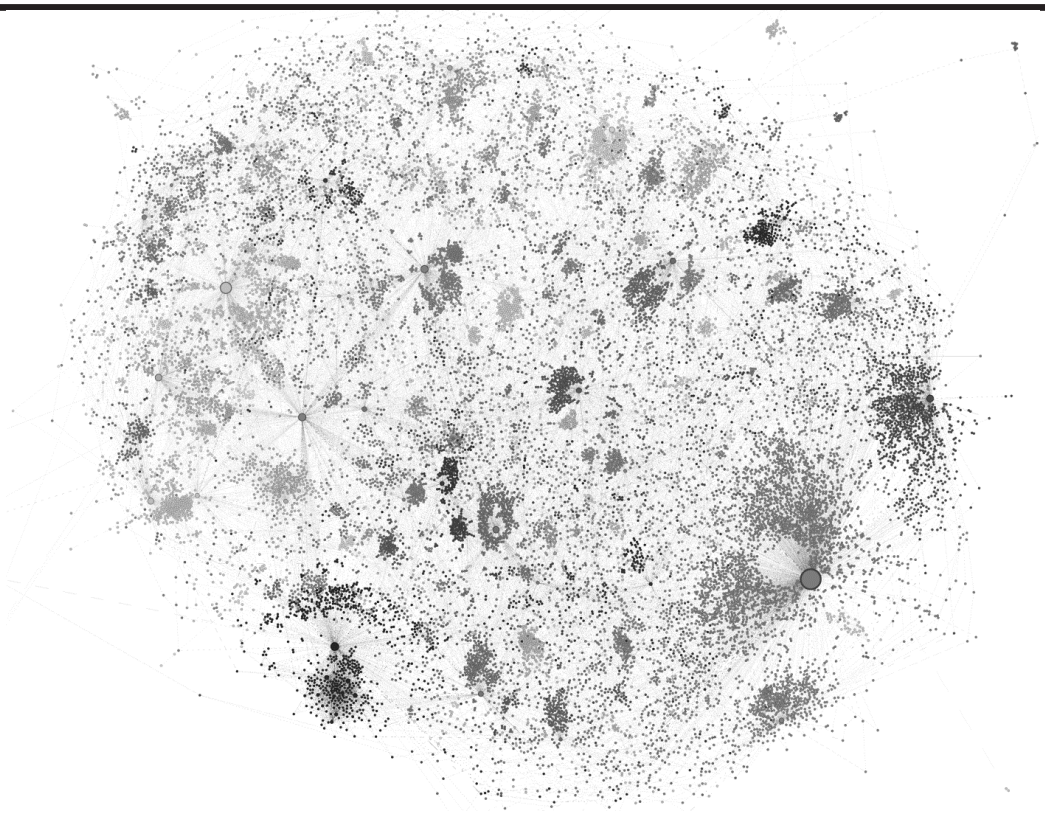

Рис. 2. Информационная карта ошибок уязвимостей, выявленных за 2021 год

Взаимозависимость кластеров программного обеспечения и типов ошибок CWE

Вторая решаемая задача – анализ построенной информационной карты. Карта была разделена на зоны в зависимости от того к какому способу эксплуатации относятся уязвимости (рис. 3).

Согласно принятой форме описания уязвимости в БДУ ФСТЭК России каждую уязвимость можно отнести к одному из двенадцати способов эксплуатации (способы были сформулированы путем обобщения шаблонов атак, взятых из международного стандарта CAPEC [1, 10]).

Сведения об уязвимостях, содержащиеся в базе данных NVD и в стандарте CAPEC не имеют прямой связи, однако определение такой связи возможно через типы ошибок CWE, что и проводится специалистами, занимающимися наполнением БДУ ФСТЭК России.

В процессе анализа информационной карты было выявлено, что рационально использовать только восемь способов эксплуатации, причем два из которых целесообразно объединить в один: «Нарушение *авторизации/ аутентификации*», а способы: «Анализ целевого объекта», «Злоупотребление функционалом», «Манипулирование сроками и состоянием», «Вероятностные методы», исходя из построенной карты не представляется возможным однозначно отнести к тому или иному кластеру на карте, что объясняется неоднородностью распределения обозначенных способов по типам ошибок и программному обеспечению.

Анализируя структуру графа, показанного на рис. 3, можно сделать следующие выводы:

1. На карте уязвимостей выделяются три больших зоны. Первая – это зона ошибок, связанных со способом эксплуатации «Нарушение авторизации/аутентификации», второй – «Манипулирование структурами данных», третий – «Инъекция».

2. Некоторые зоны не имеют общих границ, приведем их попарно: «Инъекция»/«Исчерпание ресурсов»; «Исчерпание ресурсов»/ «Несанкционированный сбор информации»; «Исчерпание ресурсов»/«Нарушение авторизации/аутентификации»;

«Несанкционированный сбор информации»/«Подмена при взаимодействии»; «Подмена при взаимодействии»/ «Манипулирование ресурсами». Программное обеспечение подверженное уязвимостям, эксплуатируемым одним способом очень редко подвержено уязвимостям эксплуатируемым вторым способом в вышеприведенных парах, что объясняется принципиальной разницей в приемах реализации этих способов. Например, исчерпание ресурсов возможно лишь при условии доступа к системе и возможности ее использования, а осуществление «Несанкционированного сбора информации» возможно из вне системы без доступа к ее внутренним ресурсам.

3. Наиболее слабо структурированным является зона «Манипулирование ресурсами», который имеет общие границы со всеми другими участками, из чего можно сделать вывод о том, что ПО, находящееся в этой зоне, атрибутируется к уязвимостям самого большого множества последствий эксплуатации уязвимостей, то есть этот способ является одним из многих, что позволяет сделать вывод о том, что уязвимости, связанные с этим способом имеют несколько векторов реализации атак, позволяющих считать их своего рода «швейцарскими ножами» для нарушителя.

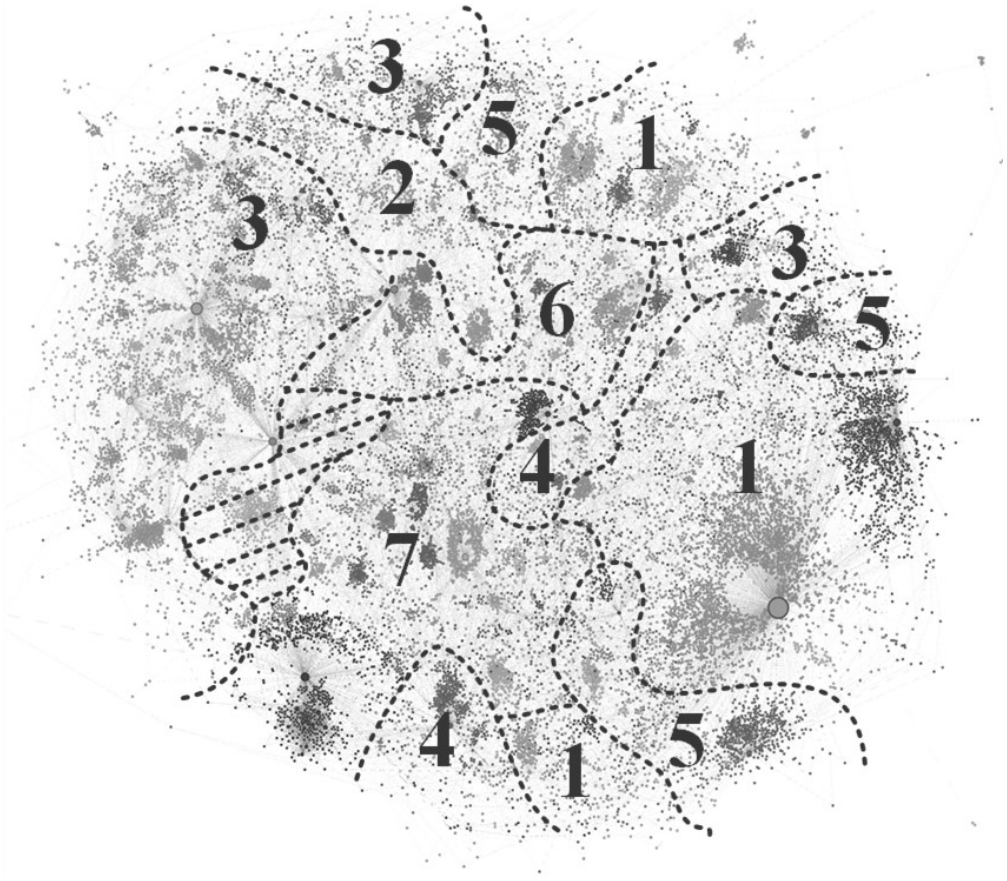

Рис. 3. Информационная карта уязвимостей за 2021 год, разделенная на области по Способу эксплуатации уязвимостей (1 – Инъекция; 2 – Исчерпание ресурсов; 3 – Манипулирование структурами данных; 4 – Несанкционированный сбор информации; 5 – Подмена при взаимодействии; 6 – Манипулирование ресурсами; 7 – Нарушение авторизации/аутентификации; Заштрихованная область – большой кластер продуктов Apple Inc., относящийся к различным способам)

Определим для каждой зоны основные типы ошибок CWE, которые формируют его основу (контур и площадь) (табл. 3).

Таблица 3

Типы ошибок CWE, формирующие зону

Способы эксплуатации уязвимостей	Формирующие CWE
Инъекция	CWE-79, CWE-89, CWE-611, CWE-74, CWE-77, CWE-798, CWE-78, CWE-94, CWE-88, CWE-74
Исчерпание ресурсов	CWE-400, CWE-401, CWE-404, CWE-617, CWE-835, CWE-775, CWE-674
Манипулирование структурами данных	CWE-120, CWE-121, CWE-787, CWE-190, CWE-125, CWE-502, CWE-415, CWE-476, CWE-788, CWE-122
Несанкционированный сбор информации	CWE-200, CWE-532, CWE-312, CWE-522, CWE-640
Подмена при взаимодействии	CWE-345, CWE-347, CWE-444, CWE-352, CWE-601, CWE-434
Манипулирование ресурсами	CWE-20, CWE-22, CWE-327, CWE-770
Нарушение авторизации/аутентификации	CWE-269, CWE-863, CWE-287, CWE-668, CWE-281, CWE-276

Далее рассмотрим кластеры, сформированные на основе принадлежности к определенному программному обеспечению.

Одним из таких скоплений является кластер, находящийся на краю карты уязвимостей, область номер 7 (рис. 4), он сформирован исключительно из операционных систем, выпускаемых компанией Microsoft. Узлы данного кластера в подавляющем большинстве находятся в зоне «Нарушение авторизации/аутентификации», и при масштабировании информационной карты, можно определить, что они связаны с узлом «CWE-269 Небезопасное управление привилегиями», из чего можно сделать вывод о том, что следует ожидать высокий уровень *корреляции* между программными продуктами Microsoft и ошибкой CWE-269 при приоритизации уязвимостей по ключевому слову «Microsoft» и типам ошибок CWE. То есть приоритет обработки устанавливаемый по CWE даст приближенно аналогичный результат, что и приоритет по продуктам Microsoft.

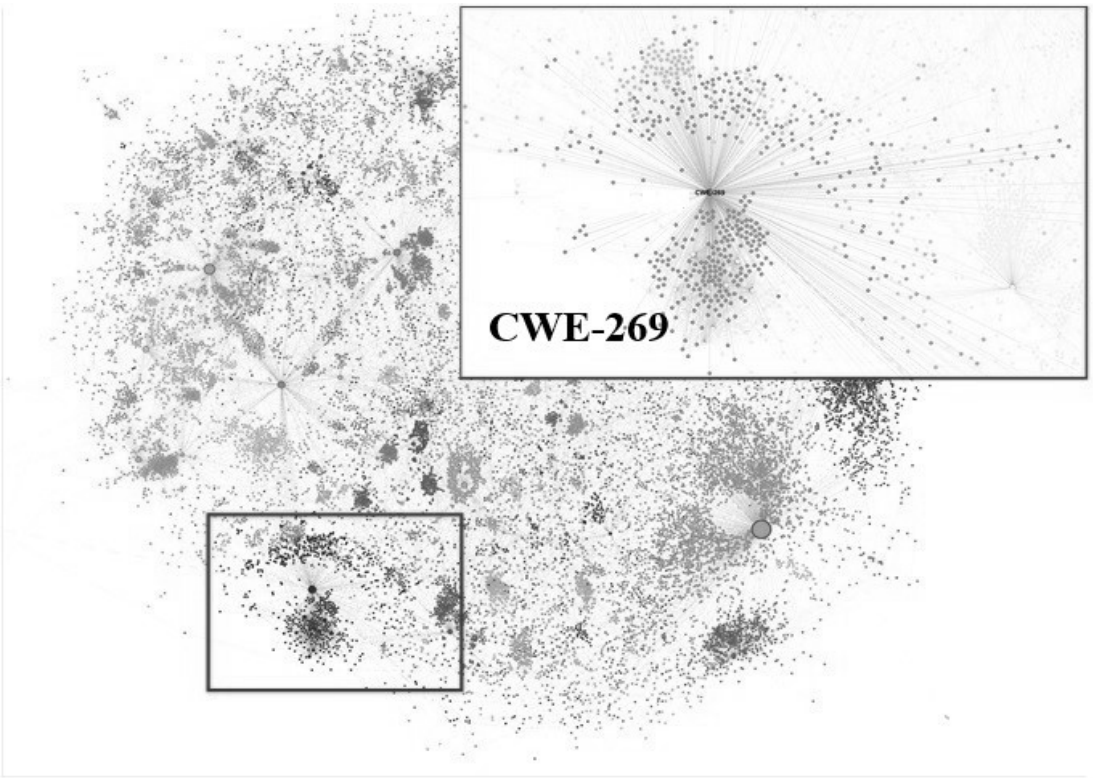

Рис. 4. Кластер «Windows»

Таким образом, повышая приоритет уязвимостей с ошибками CWE-269, необходимо учитывать, что большинство уязвимостей Microsoft получат высокий уровень опасности. Аналогично повышая приоритет программных продуктов Microsoft следует ожидать, что большинство самых опасных уязвимостей будут относиться к ошибке, а, следовательно, последствием их эксплуатации будет являться повышение привилегий нарушителя.

В табл. 4 приведены кластеры, сформированные на основе принадлежности к определенному ПО, и зоне информационной карты, в котором они находятся, а также дана их краткая характеристика.

Таблица 4

Кластеры программного обеспечения

Наименование ПО в кластере	Зона карты уязвимостей	Описание
Windows, Windows Server, Visual Studio Code, Microsoft Visual Studio	Нарушение авторизации/ аутентификации	Согласно методологии MITRE ATT&CK эксплуатация данных уязвимостей производится на этапе повышения привилегий. Также при анализе данных взятых из базы данных уязвимостей БДУ и сравнении их с данными NVD, можно сделать вывод о том, что американские специалисты акцентируют внимание именно на уязвимостях приводящих к повышению привилегий, не заполняя полностью паспорта уязвимостей с другими типами ошибок, приводящих к другим последствиям.
Google Chrome, WebKitGTK	Манипулирование структурами данных	Данные уязвимости связаны с ошибками использования памяти после освобождения, т.е., например, с использованием сохраненных cookie файлов. Также стоит учесть тот факт, что уязвимости, затрагивающие Google Chrome, могут относиться и к другим браузерам, которые были созданы на основе Chromium
TensorFlow, ImageMagick	Манипулирование структурами данных	Библиотека TensorFlow предназначена для классификации образов, ImageMagick консольный графический редактор. Так как эти программные продукты работают с изображениями, можно сделать вывод о том, что в них присутствуют одни и те же уязвимые программные компоненты.
Adobe Acrobat Document Cloud, Adobe Acrobat Reader Document Cloud, Adobe Acrobat 2020, Adobe Acrobat Reader 2020, Adobe Acrobat 2017, Adobe Acrobat Reader 2017	Манипулирование структурами данных	Уязвимости, затрагивающие программы просмотра и редактирования PDF-файлов производителя Adobe, согласно построенной карте уязвимостей, связаны с тремя типами ошибок: использование после освобождения, чтение за границами буфера, разыменование нулевого указателя. Согласно методологии MITRE ATT&CK эксплуатация данных уязвимостей производится на этапе внедрения и использования вредоносного кода. Внедрение часто происходит с помощью социальной инженерии, когда пользователю присылается вредоносный файл.
Mac OS, iOS, iPadOS, tvOS, watchOS, Iphone OS, OS X, Safari	Манипулирование структурами данных; Манипулирование ресурсами; Нарушение авторизации/ аутентификации	Уязвимости операционных систем и браузера Safari компании Apple Inc. Данный кластер находится на заштрихованной области (рис. 3) карты. Факт отсутствия строгого отнесения кластера к какой-либо зоне на карте указывает на то, что эксплуатация уязвимостей данного производителя приводит к максимально большому спектру возможных последствий.

Продолжение табл.4

Наименование ПО в кластере	Зона карты уязвимостей	Описание
Microsoft Office Web Apps, Microsoft SharePoint Server, Word, Office Web Apps Server, SharePoint Enterprise Server, Microsoft Office, Microsoft Office Online Server, Microsoft Office for Mac, 365 Apps for Enterprise, Excel	Манипулирование структурами данных	Уязвимости набора программ для работы с документами различных форматов от компании Microsoft. Данные уязвимости в большинстве случаев связаны с использованием пересылаемых специально сформированных вредоносных файлов.
Teamcenter Visualization, JT2Go	Манипулирование структурами данных	Уязвимости комплекса средств визуализации Teamcenter Visualization, JT2Go. Связанность двух данных продуктов объясняется использованием при их разработке одинаковых библиотек для обработки файлов
BIG-IP Local Traffic Manager, BIG-IP Application Acceleration Manager, BIG-IP Advanced Web Application Firewall, BIG-IP Advanced Firewall Manager, BIG-IP Analytics, BIG-IP Access Policy Manager, BIG-IP Application Security Manager, BIG-IP DDos Hybrid Defender, BIG-IP DNS, BIG-IP Fraud Protection Service, BIG-IP Global Traffic Manager, BIG-IP Link Controller, BIG-IP Policy Enforcement Manager, BIG-IP SSL Orchestrator	Манипулирование ресурсами	Уязвимости средств защиты приложений BIG-IP Application Security Manager, средств контроля доступа и удаленной аутентификации BIG-IP Access Policy Manager, системы балансировки интернет-трафика BIG-IP Link Controller, системы контроля и управления сетевым трафиком BIG-IP Policy Enforcement Manager, системы балансировки локального трафика BIG-IP Local Traffic Manager, DNS-сервера BIG-IP DNS, средства защиты веб-сервисов BIG-IP WebSafe, межсетевого экрана BIG-IP Advanced Firewall Manager, средств доставки приложений BIG-IP Application Acceleration Manager. Данные уязвимости в большинстве случаев связаны с недостатками разграничения доступа, что в свою очередь позволяет выполнять произвольные команды, изменять или удалять произвольные файлы.
IBM Engineering Insights, IBM Engineering Lifecycle Management, IBM Engineering Requirements Quality Assistant On-Premises, IBM Engineering Workflow Management, IBM Rational Engineering Lifecycle Manager, IBM Rational Team Concert, IBM Collaborative Lifecycle Management, IBM Engineering Test Management, IBM Rational Doors Next Generation, IBM Rational Quality Manager, IBM Removable Media Manager	Инъекция	Уязвимости программных продуктов IBM Corp. характеризуются тем, что кластерообразующий способ эксплуатации уязвимостей Инъекция позволяет нарушителю выполнять произвольный код, внедряя специально сформированный злонамеренный сценарий в код веб-приложения на серверной стороне сайта.
Atlassian Jira Server, Data Center	Инъекция	Уязвимости программного обеспечения для отслеживания ошибок Atlassian Jira Server и центра для обработки данных Data Center образуют кластер по причине того, что у этих продуктов один разработчик и при их написании использовались схожие модули, подверженные аналогичным ошибкам
EMUI, Magic UI	Манипулирование структурами данных; Манипулирование ресурсами	Уязвимости мобильных операционных систем EMUI, Magic UI, созданных на базе операционной системы Android, образуют кластер, связанный с проблемой «форков» (в силу того, что в ОС, основанной на базе оригинальной системы отсутствует ряд зависимостей, в «форках» возникают типичные ошибки)

Далее раскрасив карту основываясь на атрибутах patch и exploit сущности CVE (табл.1). Результат представлен на рис. 5, где A – это карта атрибута patch, B – карта атрибута exploit.

Как показано на рис. 5, основные области уязвимостей с отсутствием исправления (patch) совпадают с областями, в которых для уязвимостей в открытом доступе эксплойт (exploit) существует. Выделенные три области находятся в зонах карты, связанных со способами эксплуатации «Инъекция», «Манипулирование ресурсами», «Манипулирование структурами данных».

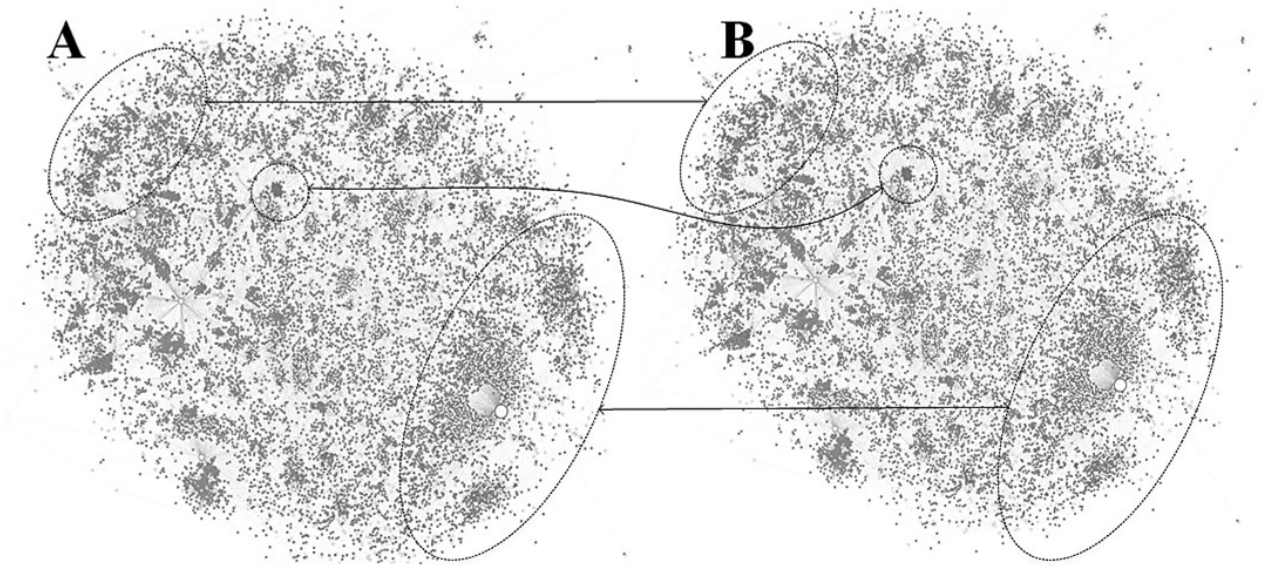

Рис. 5. Информационная карта атрибутов patch (A) и exploit (B)

Путем изменения масштаба карты было отмечено, что области *наличия эксплойта/отсутствия исправления* соответствуют кластерам CWE-79, CWE-89 в рамках зоны «Инъекция»; кластерам CWE-476 Разыменование указателя NULL, CWE-190 «Целочисленное переполнение или циклический сдвиг» – «Манипулирование структурами данных»; части кластера CWE-20 «Недостаточная проверка вводимых данных» – «Манипулирование ресурсами».

В качестве иллюстрации подробно остановимся на кластерах, находящихся в зоне «Инъекция», образуемых типами ошибок CWE-79 «Непринятие мер по защите структуры веб-страницы (или «Межсайтовая сценарная атака»)» и CWE-89 «Непринятие мер по защите структуры SQL-запроса (атаки типа «внедрение SQL»)».

Кластер, представленный на рис. 6 является крупнейшим по типу ошибок, связанных с уязвимостями веб-приложений, он образован CWE-79 «Непринятие мер по защите структуры веб-страницы (или «Межсайтовая сценарная атака»)». Отсутствие исправлений характерно для более чем 48 % уязвимостей. Количество эксплойтов среди уязвимостей, связанных с этим типом ошибки велико (52 % от общего количества). Числовые данные приведем в табл. 5,6.

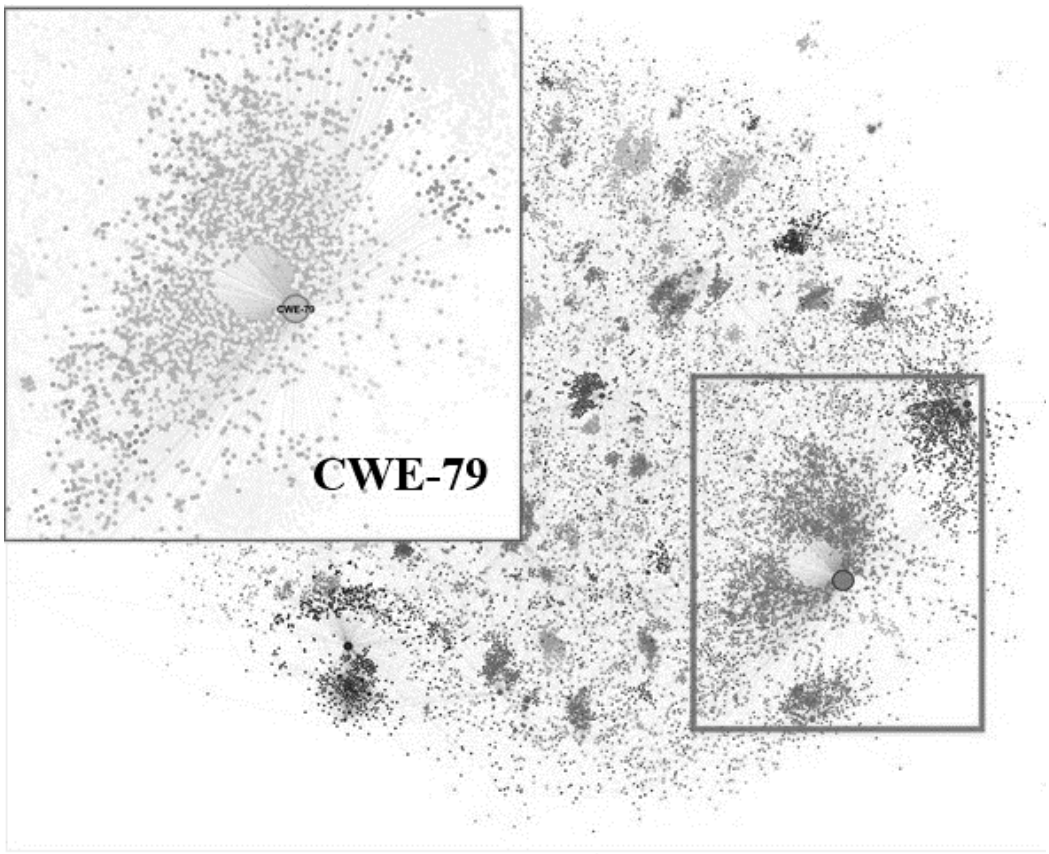

Рис. 6. Кластер, образованный типом ошибки

Таблица 5

Количество и процентное соотношение уязвимостей с эксплойтами и без по типу ошибки CWE-79

CWE-79	Количество, шт.	Процент, %
Всего записей	2154	100
С эксплойтами	1115	52
Без эксплойтов	1039	48

Таблица 6

Количество и процентное соотношение уязвимостей с опубликованными обновлениями (патчами) и без них по типу ошибки CWE-79

CWE-79	Количество, шт.	Процент, %
Всего записей	2154	100
Есть исправление	1129	52
Нет исправления	1025	48

Следующий кластер, представленный на рис. 7, сформированный типом ошибки CWE-89 «Непринятие мер по защите структуры запроса SQL (атаки типа внедрение SQL)» характеризуется наличием среди программных продуктов веб-приложений и СУБД.

Отсутствие исправлений характерно для более чем 63 % уязвимостей. Количество эксплойтов среди уязвимостей, связанных с этим типом ошибки велико (66 % от общего количества). Числовые данные приведем в табл. 7, 8.

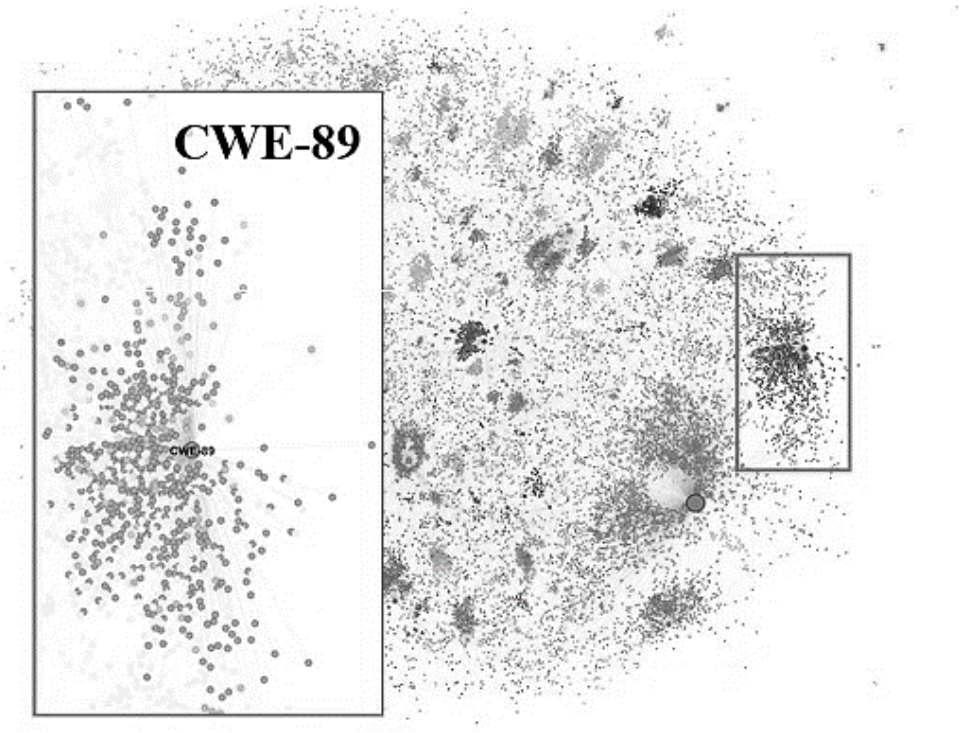

Рис. 7. Кластер, образованный типом ошибки

Таблица 7

Количество и процентное соотношение уязвимостей с эксплойтами и без по типу ошибки CWE-89

CWE-89	Количество, шт.	Процент, %
Всего записей	567	100
С эксплойтами	376	66
Без эксплойтов	191	34

Таблица 8

Количество и процентное соотношение уязвимостей с опубликованными обновлениями (патчами) и без них по типу ошибки CWE-89

CWE-89	Количество, шт.	Процент, %
Всего записей	567	100
Есть исправление	212	37
Нет исправления	355	63

Таким образом, при приоритизации уязвимостей следует обращать внимание на вышеприведенные ошибки CWE, при условии того, что в интегральном показателе расчета опасности учитываются факторы *наличия эксплойта/отсутствия исправления.*

Ранжирование кластеров CWE в рамках процесса приоритизации уязвимостей

Рассмотрим кластер (рис. 8), формируемый типом ошибки CWE-121 (Переполнение буфера в стеке). Объем кластера формируют 70 уязвимостей. Основная масса уязвимостей принадлежит к микропрограммному обеспечению и программному обеспечению сетевых программно-аппаратных средств.

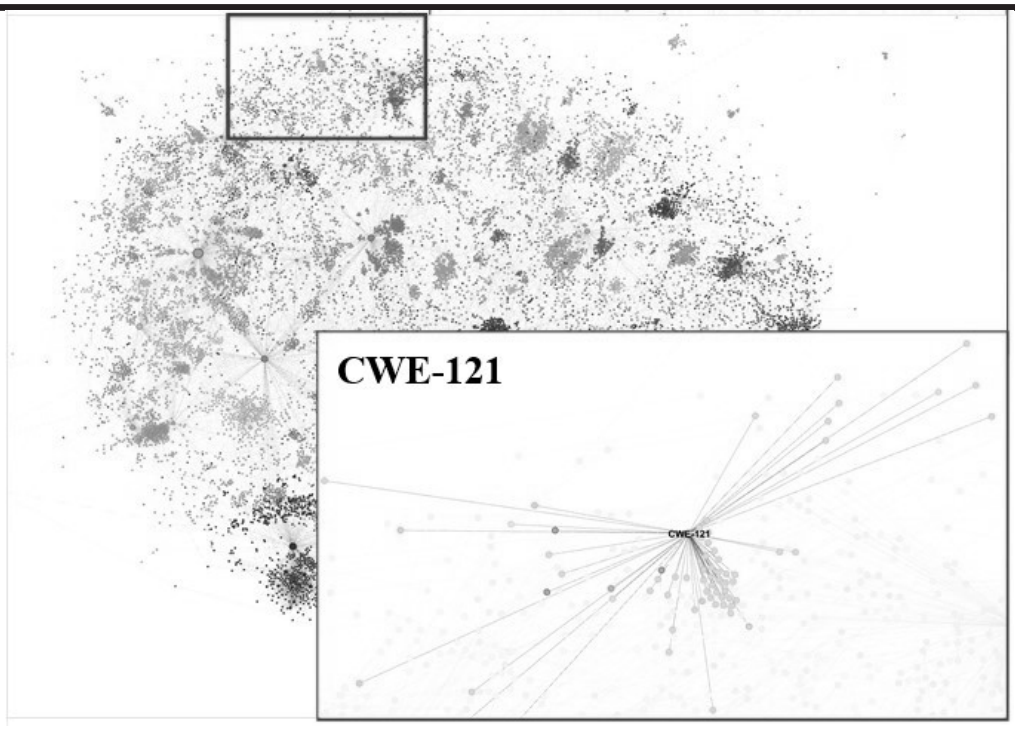

Рис. 8. Кластер CWE-121, формируемый типом ошибки CWE-121 (Переполнение буфера в стеке).

Ближайшие узлы CWE – это CWE-835 (Выполнение цикла с недоступным условием выхода (бесконечный цикл)), CWE-824 (Доступ неинициализированного указателя), CWE-120 (Копирование буфера без проверки размера входных данных (классическое переполнение буфера)) и CWE-252 (Непроверенное возвращаемое значение)

Данный кластер находится на краю карты уязвимостей, следовательно, ПО, попавшее в этот кластер, изолировано от уязвимостей с другим типом ошибок CWE (ни один луч от данного кластера не уходит в центр карты или к другим кластерам). На основании этого можно сделать вывод о том, что при приоритизации уязвимостей с помощью какого-либо интегрального показателя, включающего в качестве одного из элементов тип ошибки CWE, необходимо учитывать степень информативности той или иной CWE. Степень информативности определяет значимость ошибки CWE в контексте интегрального показателя и может быть оценена визуально на основании расположения связанных с ней уязвимостей.

Определим степень информативности каждого узла CWE. Для этого с помощью визуального анализа карты кластеризации (рис. 3), проранжируем ошибки CWE, разделив их на четыре категории по степени их вовлеченности в другие кластеры (табл.9).

Таблица 9

Ошибки по их степени информативности

Степень информативности	Наименование CWE	Количество уязвимостей в категории
Максимальная	CWE-915, CWE-305, CWE-36, CWE-61, CWE-759, CWE-425, CWE-316, CWE-93, CWE-662, CWE-1321, CWE-472, CWE-300, CWE-64, CWE-527, CWE-26, CWE-1188, CWE-763, CWE-704, CWE-823, CWE-548, CWE-259, CWE-916, CWE-565	127
Высокая	CWE-416, CWE-353, CWE-843, CWE-125, CWE-843, CWE-457, CWE-193, CWE-122, CWE-476, CWE-681, CWE-763, CWE-369, CWE-191, CWE-805, CWE-1284, CWE-170, CWE-824, CWE-121, CWE-823, CWE-73, CWE-399, CWE-489, CWE-123, CWE-121, CWE-1076, CWE-321, CWE-88, CWE-798, CWE-502, CWE-89, CWE-434, CWE-352, CWE-94, CWE-434, CWE-611, CWE-306	3692

Продолжение табл. 9

Степень информативности	Наименование CWE	Количество уязвимостей в категории
Средняя	CWE-74, CWE-79, CWE-190, CWE-119, CWE-835, CWE-120, CWE-347, CWE-444, CWE-345, CWE-77, CWE-78, CWE-347, CWE-522, CWE-347, CWE-862, CWE-200, CWE-427, CWE-276, CWE-319, CWE-327, CWE-203, CWE-401, CWE-755, CWE-404, CWE-617, CWE-732, CWE-918	5603
Низкая	CWE-20, CWE-400, CWE-287, CWE-863, CWE-287, CWE-22, CWE-668, CWE-787, CWE-532, CWE-269, CWE-770	4605

Обратимся к рейтингу наиболее популярных 25 ошибок CWE представленных на портале CWE MITRE [11], этим рейтингом пользуются многие специалисты в области информационной безопасности, скорректируем его с учетом построенной информационной карты. Для начала проанализируем в какие категории информативности попадают эти ошибки, для этого на основе табл. 9 построим диаграмму (рис. 9).

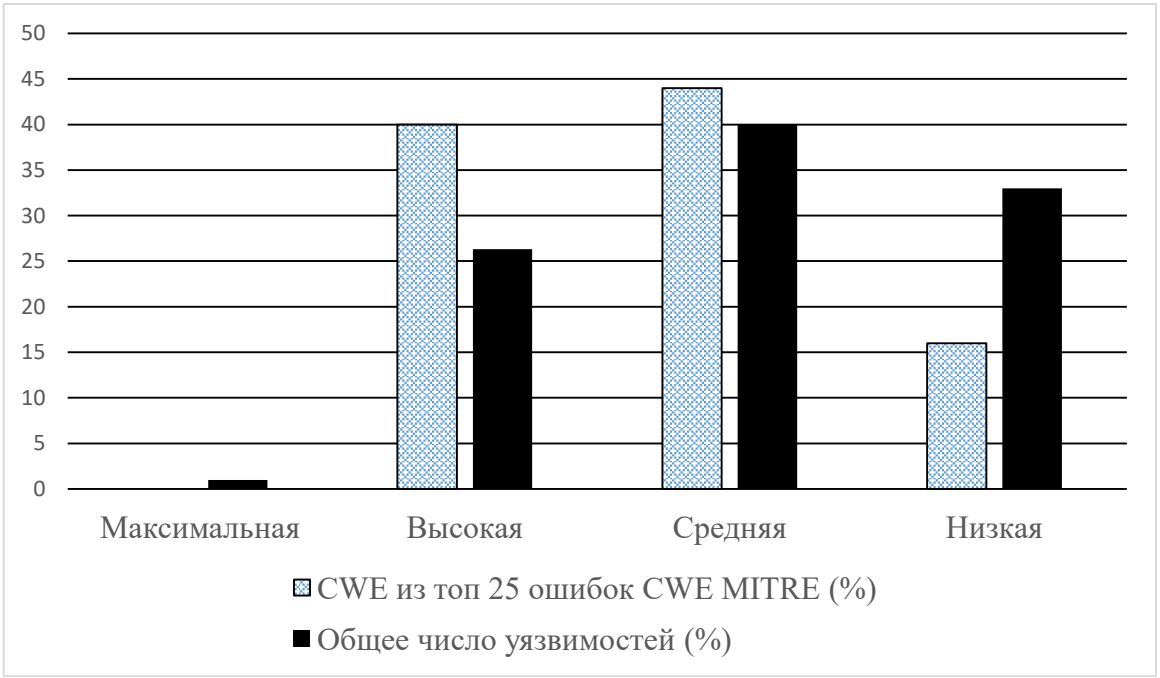

Рис. 9. Диаграмма распределения по ошибкам CWE MITRE по категориям информативности и общему количеству уязвимостей в этих категориях (в процентном соотношении)

Исходя из диаграммы видно, что большинство ошибок приходятся на среднюю и высокую группы информативности. Причем к средней группе информативности относится и максимальное число уязвимостей по отношению к другим группам.

На группу низкой информативности с четырьмя CWE приходится большее количество уязвимостей, чем на группы высокой информативности, это является косвенным подтверждением того, что визуальный анализ информационной карты для выявления таких групп был произведен верно.

Путем применения метода групповых экспертных оценок, а именно, метода Дельфи [12], определим соотношения между категориями CWE. Анализ с помощью данного метода проводится в несколько этапов, результаты обрабатываются статистическими методами. Экспертам предложено дать себе индивидуальную самооценку в баллах в диапазоне от 0 до 10. Далее предложено дать оценку для каждой категории от 0 до 10 (табл.10).

Таблица 10

Оценки, полученные с помощью метода Дельфи

Номер эксперта	Самооценка	Оценка для степени информативности			
		«Максимальная»	«Высокая»	«Средняя»	«Низкая»
1	10	10	7	5	3
2	10	10	8	6	4
3	9	10	8	5	3
4	5	10	7	4	3
5	7	10	8	6	4

Среднегрупповая самооценка равна 8.2.

Простая оценка: «Максимальная» - 10; «Высокая» - 7.6; «Средняя» - 5.2; «Низкая» - 3.4.

Средневзвешенная оценка: «Максимальная» - 10; «Высокая» - 7.63; «Средняя» - 5.29; «Низкая» - 3.41. Медиана: «Максимальная» - 10; «Высокая» - 8; «Средняя» - 5; «Низкая» - 3. Нижняя граница доверительной области: «Максимальная» - 10; «Высокая» - 7.25; «Средняя» - 4.5; «Низкая» - 3.25. Верхняя граница доверительной области: «Максимальная» - 10; «Высокая» - 7.75; «Средняя» - 5.5; «Низкая» - 3.75.

После второго тура были получены следующие результаты: Простая оценка: «Максимальная» - 10; «Высокая» - 7.5; «Средняя» - 5.5; «Низкая» - 3.5.

После полученных результатов ни один эксперт не выразил желание изменить свои оценки. Таким образом, после проведенных расчетов можно преобразовать топ 25 ошибок CWE MITRE в скорректированный согласно полученным результатам топ 25 (табл.11). При этом разделим полученную оценку для степени информативности на 10, чтобы пронормировать значения от 0 до 1. Нормированная оценка: «Максимальная» - 1; «Высокая» - 0.75; «Средняя» - 0.55; «Низкая» - 0.35.

Таблица 11

Сравнение «ошибок CWE MITRE» и скорректированного рейтинга

№	CWE MITRE	Рейтинг	CWE с учетом корректировки	Рейтинг (с учетом корректировки)
1	CWE-787	65.93	CWE-79	24.35
2	CWE-79	46.84	CWE-787	22.42
3	CWE-125	24.9	CWE-125	18.9
4	CWE-20	20.47	CWE-89	14.85
5	CWE-78	19.55	CWE-416	12.8
6	CWE-89	19.54	CWE-352	11
7	CWE-416	16.83	CWE-78	10.17
8	CWE-22	14.69	CWE-20	6.96
9	CWE-352	14.46	CWE-434	6.42
10	CWE-434	8.45	CWE-306	6.03
11	CWE-306	7.93	CWE-502	5.1
12	CWE-190	7.12	CWE-22	5.08
13	CWE-502	6.71	CWE-476	4.97
14	CWE-287	6.58	CWE-798	4.76
15	CWE-476	6.54	CWE-190	3.7
16	CWE-798	6.27	CWE-611	3.06
17	CWE-119	5.84	CWE-119	3.04
18	CWE-862	5.47	CWE-862	2.84
19	CWE-276	5.09	CWE-276	2.65
20	CWE-200	4.74	CWE-200	2.47
21	CWE-522	4.21	CWE-287	2.24
22	CWE-732	4.2	CWE-522	2.19
23	CWE-611	4.02	CWE-732	2.18
24	CWE-918	3.78	CWE-918	1.97
25	CWE-77	3.58	CWE-77	1.86

Заключение

В данной статье был предложен алгоритм построения информационной карты уязвимостей, позволяющей систематизировать сведения о типах ошибок программного обеспечения.

Тип ошибки относится к наиболее важным параметрам, определяющим причину возникновения уязвимости. Вместе с классом ПО данные показатели определяют возможные последствия от её эксплуатации.

В ходе анализа информационной карты были определены зависимости между типами конкретными типами ошибок CWE и программными продуктами с учётом различных факторов (наличием эксплойта, патча и оценкой уровня опасности). Благодаря визуальному анализу и учёт данных факторов были определены приоритеты для наиболее распространённых кластерообразующих типов ошибок.

Данные приоритеты позволяют ранжировать уязвимости ПО. Разработанная информационная карта может быть использована в качестве инструмента, который позволяет исследователю наглядно представить всё множество уязвимостей. Среди этого множества могут быть выделены наиболее приоритетные области, учитывающие специфику конкретных защищаемых ИС.

Приоритетным направлением исследований является использование построенной информационной карты в качестве основы для визуализации рисков эксплуатации уязвимостей ПО, рассчитанных для конкретных ИС в соответствии с выбранной методологией.

Список литературы

1. Банк Данных Угроз безопасности информации ФСТЭК России // URL: https://bdu.fstec.ru/vul (дата обращения: 12.05.2022).

2. National Vulnerability Database // URL: https://nvd.nist.gov/vuln (дата обращения: 12.05.2022).

3. Сердечный А.Л. Технологии картографирования защищаемого киберпространства. / А.Л. Сердечный, М.А. Тарелкин, А.А. Ломов, Д.М. Коваленко. // Информация и безопасность. 2019. Т. 22. Вып. 3. С. 399-410.

4. Калашников А.О, Сердечный А.Л., Остапенко А.Г. Картографический подход в библиометрическом исследовании отечественных научных школ, сложившихся в области защиты информации и обеспечения информационной безопасности. // Информация и безопасность. 2019. Т. 22. Вып. 4. С. 455-484.

5. Сердечный А.Л. Карты источников, содержащих сведения об уязвимостях программного обеспечения. / А.Л. Сердечный, М.А. Тарелкин, А.А. Ломов, К.В. Симонов. // Информация и безопасность. 2019. Т. 22. Вып. 3. С. 411-422.

6. Сердечный А.Л. Картографический подход к описанию киберпространства в контексте обеспечения безопасности информации и информационной безопасности / А.Л. Сердечный, А.Г. Остапенко // Информация и безопасность. 2019. Т. 22. Вып. 3. С. 387-398.

7. Сердечный А.Л. Концептуальные основы картографии защищаемого киберпространства. Часть 1 / А.Л. Сердечный // Информация и безопасность. 2021. Т. 24. Вып. 3. С. 373-386.

8. Сердечный А.Л. Концептуальные основы картографии защищаемого киберпространства. Часть 2 / А.Л. Сердечный // Информация и безопасность. 2021. Т. 24. Вып. 3. С. 387-400.

9. Serdechnyi A.L., Goncharov A.A., Ostapenko A.G., Bataronov I.L. Mapping retrieval method for academic publications in the field of aerospace technology safety. IOP Conference Series Materials Science and Engineering 862 (2020) 052028

10. Common Attack Pattern Enumerations and Classifications // URL: https://capec.mitre.org/ (дата обращения: 12.05.2022).

11. CWE - 2021 CWE Top 25 Most Dangerous Software Weaknesses // URL: https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html (дата обращения: 12.05.2022).

12. The Delphi Method. Techniques and Applications / ed. H. Linstone & M. Turoff. Addison-Wesley Publishing Company, 1975. P. 212-216.

Воронежский государственный технический университет
Voronezh State Technical University

Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю
State Research Testing Institute for Problems of Technical Information Protection of the Federal Service for Technical and Export Control

Поступила в редакцию 30.05.2022

Информация об авторах

Гончаров Андрей Андреевич– аспирант, Воронежский государственный технический университет, e-mail: zzzsuprema@gmail.com

Тарелкин Михаил Александрович– старший научный сотрудник, Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, e-mail: zzzsuprema@gmail.com

Сердечный Алексей Леонидович – канд. техн. наук, старший преподаватель, Воронежский государственный технический университет, e-mail: alex-voronezh@mail.ru

SYSTEMATIZATION OF DATA ABOUT SOFTWARE WEAKNESSES USING AN INFORMATION MAP AND ASSESSMENT OF THEIR SIGNIFICANCE

A.A. Goncharov, M.A. Tarelkin, A.L. Serdechnyy

The article presents the results of the construction and analysis of an information map systematizing information about software weaknesses. The information contained in the vulnerability database National Vulnerability Database was considered as the source data. The information map made it possible to establish the relationship between the classes of software and the types of weaknesses characteristic of them. The systematization of information about software weaknesses in the form of an information map allows us to assess the role of the relevant factor in determining the priority of processing information about the relevant vulnerabilities, taking into account their level of danger. The result is the development of recommendations on prioritizing vulnerabilities in order to process them as a priority and apply protection measures to minimize damage from their exploitation. The information map of software weaknesses can be the basis for a visual display of the risks of exploiting software vulnerabilities

Keywords: information map, software vulnerability, type of software weakness, CWE.

Submitted 30.05.2022

Information about the authors

Andrey A. Goncharov – graduate student, Voronezh State Technical University, e-mail: zzzsuprema@gmail.com

Mihail A. Tarelkin – senior researcher, State Research Testing Institute for Problems of Technical Information Protection of the Federal Service for Technical and Export Control, e-mail: zzzsuprema@gmail.com

Alexey L. Serdechnyy – Cand. Sc. (Technical), Senior Lecturer, Voronezh State Technical University, e-mail: alex-voronezh@mail.ru