DOI 10.36622/1682-7813.2024.27.1.001
УДК 004.056

АВТОМАТИЗИРОВАННЫЙ БАНК ЗНАНИЙ И КАЛЬКУЛЯТОР РИСКОВ РЕАЛИЗАЦИИ КИБЕРАТАК И УЯЗВИМОСТЕЙ (ЧАСТЬ I)

Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, Д.С. Нестеров, А.С. Дубов, В.А. Старцев

В статье рассмотрены вопросы повышения защищенности атакуемых автоматизированных информационных и телекоммуникационных систем за счет разработки и применения методического, алгоритмического и программного обеспечения автоматизации риск-анализа и регламентации противодействия кибератакам. Решена научно-техническая задача создания инструментария, интегрирующего пространство данных, техник и мер противодействия кибератакам, включая целеполагание, риск-анализ и формирование знаний о регламентации борьбы с компьютерными инцидентами. Сформирован банк знаний кибератак и уязвимостей в виде агрегированных регламентов различных стадий противодействия вторжениям, включая текущее реагирование и ликвидацию последствий в отношении зарегистрированных инцидентов. Пользователь может в диалоговом режиме получить из банка практические рекомендации по борьбе с многообразием сценариев атак и брешей, используемых злоумышленниками.

Ключевые слова: система, безопасность, риск, ущерб, вероятность, регламент, база знаний и данных.

Введение

Излишне упоминать о стремительном росте количества компьютерных вторжений в автоматизированные информационные системы (АИС) и телекоммуникационные сети (ТКС), акцентирующем внимание исследователей киберпространства на нарушениях его безопасности [1], в основе которых лежат сочетания векторов (сценариев) реализации атак и уязвимостей АИС и ТКС, используемых злоумышленниками [2-7]. В этом контексте научно-техническому персоналу, защищающему АИС и ТКС, сейчас приходится иметь дело с сотнями известных злоумышленных сценариев и тысячами выявленных уязвимостей, порождающими десятки тысяч их сочетаний, каждое из которых имеет свою специфику реагирования средств и органов защиты. Очевидная мультиразмерность вышеуказанной проблемной ситуации обуславливает необходимость автоматизации агрегирования данных и знаний о киберинцидентах, а также выработки на их основе адекватных проектных решений по методологии и технике противоборства с ними, наиболее свежие попытки формализации которых представлены в работах [8-16].

Объект исследования, представленного в настоящей статье, − проектное пространство регистрируемых инцидентов, атакуемых АИС и ТКС, включающее базы данных и знаний о компьютерных атаках и уязвимостях различного профиля.

Предметом исследования являются оценка рисков возникновения киберинцидентов, формирование мер реагирования на них и ликвидация их последствий в условиях реализации компьютерных атак и уязвимостей АИС и ТКС.

Цель исследования состоит в повышении защищенности атакуемых АИС и ТКС за счет разработки и применения методического, алгоритмического и программного обеспечения автоматизации риск-анализа и регламентации противодействия кибератакам.

Научно-техническая задача настоящей работы заключается в создании автоматизированного инструментария для управления защищенностью АИС и ТКС посредством риск-калькуляции и регламентации реагирования на инциденты,

создаваемые успешной реализацией кибератак.

Исследование аналогов [8-16] позволяет констатировать наличие следующих недостатков в инструментах современного анализа рисков:

- некорректное объединение ущербов различных по своей сущности нарушений конфиденциальности, целостности и доступности информации,
- для конкретной защищаемой системы отсутствие в оценках возможности учета ценности информации,
- ошибочное неразделение авторами калькуляций факторов частичной и полной утраты работоспособности атакуемой системы, которые требуют принципиально различные показатели в оценке возможных ущербов,
- необоснованное алгебраическое перемножение значений множества метрик,
- введение, видимо, эмпирически полученных констант в виде коэффициентов и слагаемых, которые очевидно должны меняться по ходу развития арсенала кибер-вторжений и по мере совершенствования подсистем защиты от них,
- некорректное введение аналогий с теорией вероятности в отношении совместного и раздельного учета факторов нарушения качеств доступности, целостности и конфиденциальности информации.

Кроме того, необходимо отметить, что мультиразмерность множества обрабатываемых сведений требует автоматизации процесса как на стадии формирования, так и при актуализации создаваемого информационного базиса; структурной, терминологической, методической и др. разобщенности ресурсов CAPEC, NIST, MITRE ATT&CK, БДУ, CISA KEV (предлагающих меры, тактики, техники и калькуляцию в отношении ожидаемых инцидентов кибербезопасности) затрудняют противодействие атакам

Представленные выше недостатки обуславливают необходимость решения следующих задач:

- разработка методического, алгебраического и программного обеспечения оценки рисков успешной реализации кибератак, предусматривающего (с использованием данных полей CVSS) среднестатистическое раздельное измерение ущербов нарушения целостности, доступности и конфиденциальности информации доя различных CAPEC-векторов и актуальных уязвимостей (CISE KEV), включая адаптацию метрик риска к специфике защищаемой системы (в многообразии наличиствующих в ней уязвимостей, ее защищенных объектов, стоимости информационных ресурсов атакуемых компонентов),
- триединство методического, алгоритмического и программного обеспечения, создание автоматизированного инструментария агрегирования знаний и данных, относящихся к парам вектор атак-уязвимость АИС и ТКС, имея ввиду предоставление пользователю возможности автоматического получения возможности автоматического получения регламентов противодействия в отношении всяких пар, поименованных в ресурсах CAPEC и CISA KEV.

Результаты решения перечисленных задач видятся в разработке:

- калькулятора риска, обеспечивающего автоматизированный расчет ущербов и вероятностей их наступления для различных нарушений качеств информации и работоспособности АИС и ТКС в результате реализации всевозможных компьютерных атак и с использованием ими зарегистрированных уязвимостей, а также – способствующий построению риск-ландшафтов для исследуемых сочетаний векторов кибератак и программных ошибок;
- банка знаний об инцидентах компьютерных вторжений в АИС и ТКС, которые автоматизировано агрегированы в специально разработанном формате регламентов различных стадий противодействия кибератакам (реагирование и ликвидации последствий в отношении зарегистрированных инцидентов);
- иллюстрирующих сформированный банк знаний примеров формирования риск-ландшафтов и регламентов организационно-правового противодействия актуальным атакам на инфраструктурные сервисы, контроллеры домена корпоративных сетей, а также веб-приложений, демонстрирующих

возможности практического применения созданного инструментария.

1 Методическое обеспечение баз данных и знаний о компьютерных атаках и уязвимостях различного профиля атак

Значимость задачи совершенствования организационного-правового обеспечения информационной безопасности растет с каждым днем. Об этом свидетельствует растущее количество кибератак на информационные системы и необходимость в формализации знаний о таковых.

Создание баз данных уязвимостей с различными типами атак обусловлено необходимостью эффективного управления рисками в области информационной безопасности. Эти базы данных и ресурсы служат важным инструментом для специалистов по кибер-безопасности, позволяя им быстро и эффективно оценивать и приоритизировать уязвимости на основе их серьезности и потенциальной опасности. Поэтому для формализации многообразия угроз требуется рассмотрение наиболее часто используемых ресурсов, которые максимально полно охватывают многообразие кибератак и предоставляют актуальную информацию.

Очевидно, что основой для защиты информационных систем выступает риск-анализ определенных событий, который показывает необходимость применения того или иного решения. Значимость данного факта подталкивает исследователя рассматривать информацию, предоставляемую базами знаний о кибератаках в качестве инструмента для оценки рисков.

К сожалению, на данный момент не существует идеального всеохватывающего инструмента, который позволит с разных сторон отразить все аспекты деструктивного воздействия на информационные системы. Поэтому базы знаний должны иметь смысловое пересечение описания угроз информационной безопасности (ИБ) между собой.

Исходя из описанных проблем, возникают особые требования для задачи формализации многообразия баз знаний:

1) актуальность: База знаний должна быть актуальной, чтобы отражать текущие тенденции и развитие кибербезопасности.

2) полнота: База знаний должна охватывать все возможные типы уязвимостей и атак, чтобы предоставить полный обзор потенциальных угроз.

3) совместимость: Базы знаний должны рассматривать различные аспекты угроз и при этом иметь пересечения между собой.

4) ориентированность: Информация, предоставляемая ресурсом, должна выступать в качестве поддержки для риск-анализа.

1.1 Исследование базы знаний CAPEC

CAPEC (Common Attack Pattern Enumeration and Classification) − это словарь широко распространенных и хорошо известных атакующих методик и шаблонов поведения, которые могут использоваться злоумышленниками для эксплуатации общих типов ошибок в программном обеспечении (CWE). Он представляет собой структурированный набор информации, который предоставляет общую терминологию для описания и обсуждения атак, их вредоносные последствия, типичные методы защиты и связанные с ними уязвимости. CAPEC помогает специалистам информационной безопасности (ИБ-специалистам) понимать атаки и связанные с ними угрозы на более глубоком уровне, что важно для разработки эффективных мер безопасности и стратегий защиты. На данный момент база знаний CAPEC включает в себя описание 559 шаблонов атак [2].

ИБ-специалисты, такие как пентестеры, разработчики и специалисты по сетям, используют CAPEC в своей работе для:

1) идентификации и анализа потенциильных атак, которые могут быть использованы против систем и приложений,

2) планирования тестов на проникновение и оценки уязвимостей, предоставляя общий язык для обсуждения и документирования атак,

3) разработки защитных мер, в отношении атакующих методик и разработки стратегий, чтобы предотвратить или смягчить их воздействие.

CAPEC использует иерархический подход для классификации типов атак, который позволяет организовать атаки на разных уровнях абстракции и сложности. Эта структура помогает понять связи между различными атаками и упрощает поиск и анализ атакующих методов. Информация, содержащаяся для каждого шаблона атаки, включает в себя множество элементов, которые предоставляют подробное описание и контекст для атаки.

Актуальность использования базы знаний CAPEZ

База знаний CAPEC регулярно обновляется специалистами по информационной безопасности. В ходе обновлений редактируются уже существующие шаблоны атак, реже добавляются новые экземпляры. Об этом свидетельствует предоставленная авторами ресурса страница последних обновлений.

Полнота предоставляемой информации

Несмотря на свою обширность (на момент написания работы содержит 593 шаблонов атак), CAPEC не всегда предоставляет информацию о взаимосвязи между различными атаками, уязвимостями и техниками, используемыми злоумышленниками. Важным негативным аспектом является то, что CAPEC не предоставляет информацию о способах защиты от этих атак. Для получения такой информации обычно требуется использование других ресурсов, таких как базы данных уязвимостей или руководства по безопасности.

В целом, несмотря на свою полезность, CAPEC не может заменить полноценную систему управления угрозами и рисками, которая включает в себя не только сбор и анализ информации, но и планирование и реализацию мер по снижению риска.

Совместимость с другими информационными ресурсами

Ресурс предоставляет исследователю информацию об ошибках программного обеспечения CWE применительно почти ко всем шаблонам атак. Поэтому также необходимо рассматривать CWE как звено в формализации информации о многообразии кибератак.

Также в описании некоторых шаблонов атак CAPEC явно указаны взаимосвязи с тактиками и техниками из MITRE ATT&CK, но процент (177 из 593 CAPEC – 29 %) содержания таких записей очень мал.

Содержание данных для риск-анализа угроз

Информационная база предоставляет данные о вероятности успеха атак и серьезности их последствий в виде качественной оценки. Эти значения можно использовать для риск-аналитики.

Обзор предоставляемой ресурсом информации

Каждый шаблон атаки в CAPEC, согласно приведенной схеме, указанной на ресурсе с базой знаний может содержать следующую информацию (табл. 1).

Таблица 1

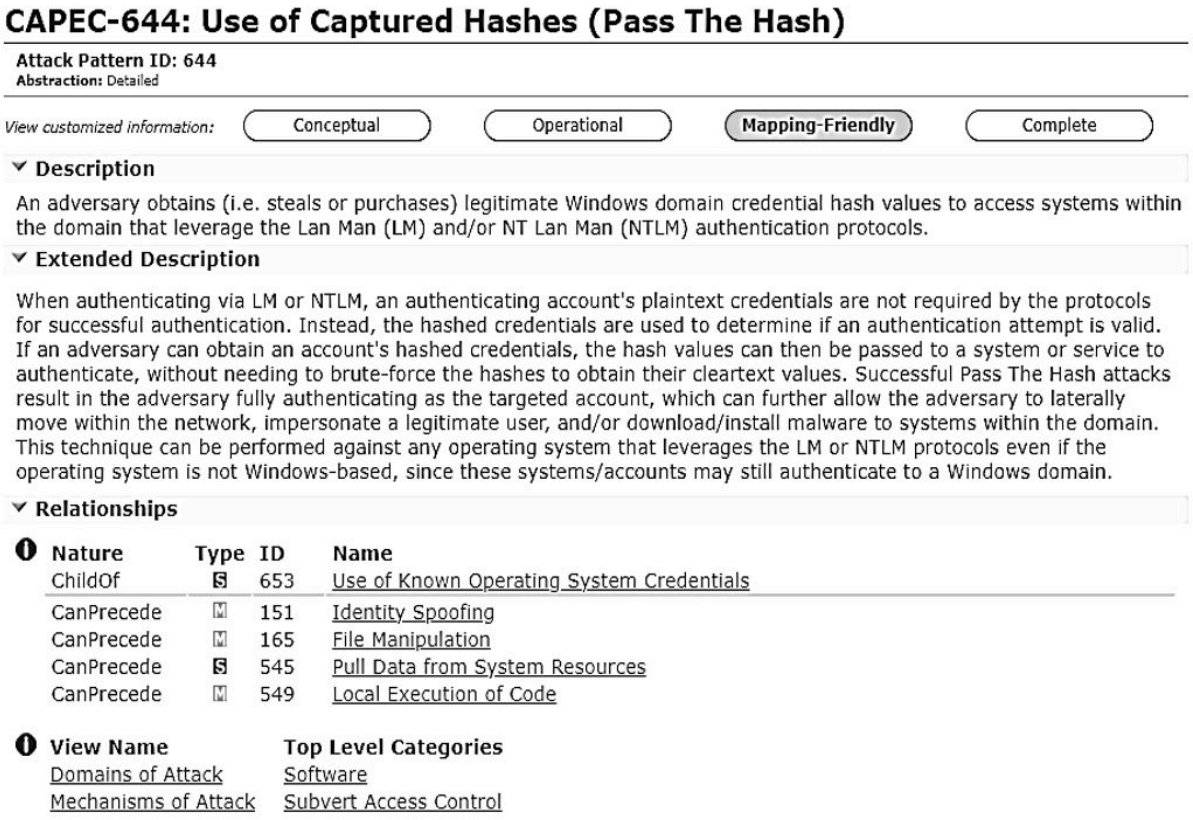
Наименования и краткое описание полей шаблона атаки CAPEC

Наименование поля	Краткое описание поля
ID и имя	Уникальный идентификатор и название шаблона атаки.
Описание	Подробное описание атаки, включая последовательность действий атакующего.
Сводка	Краткое описание атаки, включая цель атаки и последовательность шагов.
Поток выполнения атаки	Перечень шагов, обычно выполняемых атакующим при осуществлении атаки.

Продолжение табл. 1

Наименование поля	Краткое описание поля
Альтернативные термины	Другие термины, используемые для идентификации шаблона атаки.
Целевая атакуемая поверхность	Характеристики мест, с которыми атакующий взаимодействует в целевой системе.
Предпосылки атаки	Условия, которые должны существовать для успеха атаки.
Типичная серьезность	Отражает типичную серьезность атаки по шкале от очень низкой до очень высокой.
Типичная вероятность эксплуатации	Вероятность успеха атаки с объяснениями и предположениями.
Методы атаки	Перечень определенных векторов, идентифицирующих механизмы, используемые в атаке.
Примеры - инстанции	Конкретные примеры или демонстрационные экземпляры атаки.
Требуемые навыки или знания атакующего	Уровень навыков или знаний, необходимых для осуществления атаки.
Требуемые ресурсы	Ресурсы (вычислительные мощности, IP-адреса, инструменты и т.д.), необходимые атакующему для эффективного выполнения атаки.
Техники зондирования	Методы, используемые для исследования потенциальной цели для определения уязвимости.
Индикаторы - предупреждения об атаке	Активности, события, условия или поведение, которые могут указывать на то, что атака неминуема, в процессе или уже произошла.
Техники обфускации	Методы, используемые для маскировки факта атаки.
Мотивация и последствия атаки	Желаемые технические результаты, которые могут быть достигнуты с помощью этого шаблона атаки.
Векторы внедрения, полезная нагрузка, зона активации, воздействие активации полезной нагрузки	Детали механизма и формат атаки на основе ввода данных.
Связанные уязвимости и атаки	Специфические уязвимости или другие атаки, которые связаны с данным шаблоном атаки.
Ключевые слова	Текстовые строки, используемые для маркировки и поиска данных в каталоге CAPEC.
Ссылки	Ссылки на внешнюю документацию, которая была использована для разработки определения атаки или может быть полезной для дальнейшего изучения.

Пример шаблона атаки. Давайте посмотрим на запись CAPEC для известного шаблона атаки – «Использование захваченных хэшей (Pass The Hash)» – и проанализируем, как различные свойства полезны для понимания шаблонов атак в целом (рис. 1).



CAPEC-644: Use of Captured Hashes (Pass The Hash)

Attack Pattern ID: 644
Abstraction: Detailed

View customized information: Conceptual | Operational | **Mapping-Friendly** | Complete

Description

An adversary obtains (i.e. steals or purchases) legitimate Windows domain credential hash values to access systems within the domain that leverage the Lan Man (LM) and/or NT Lan Man (NTLM) authentication protocols.

Extended Description

When authenticating via LM or NTLM, an authenticating account's plaintext credentials are not required by the protocols for successful authentication. Instead, the hashed credentials are used to determine if an authentication attempt is valid. If an adversary can obtain an account's hashed credentials, the hash values can then be passed to a system or service to authenticate, without needing to brute-force the hashes to obtain their cleartext values. Successful Pass The Hash attacks result in the adversary fully authenticating as the targeted account, which can further allow the adversary to laterally move within the network, impersonate a legitimate user, and/or download/install malware to systems within the domain. This technique can be performed against any operating system that leverages the LM or NTLM protocols even if the operating system is not Windows-based, since these systems/accounts may still authenticate to a Windows domain.

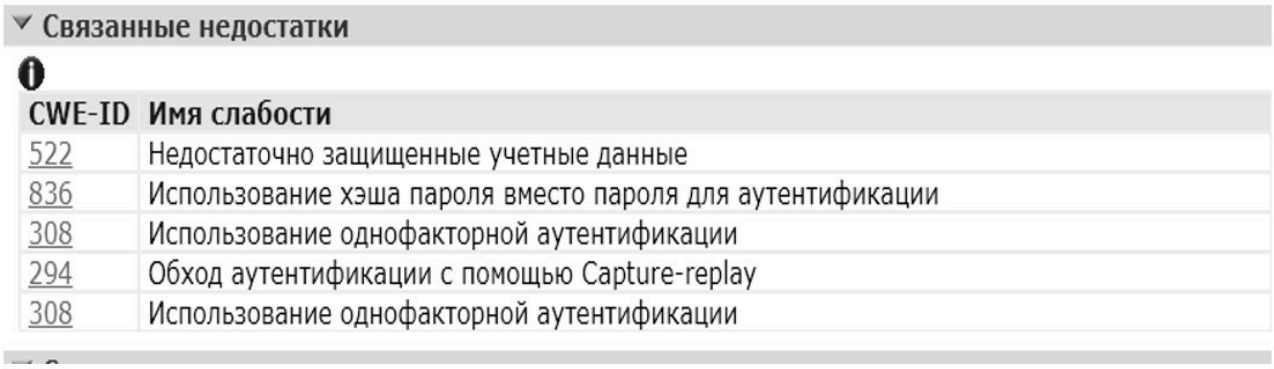
Relationships

Nature	Type	ID	Name
ChildOf	S	653	Use of Known Operating System Credentials
CanPrecede	M	151	Identity Spoofing
CanPrecede	M	165	File Manipulation
CanPrecede	S	545	Pull Data from System Resources
CanPrecede	M	549	Local Execution of Code

View Name	Top Level Categories
Domains of Attack	Software
Mechanisms of Attack	Subvert Access Control

Рис. 1. Пример записи шаблона атаки на сайте CAPEC

Каждый из образцов атак имеет свой числовой идентификатор. В нашем примере это CAPEC-644. Номер не содержит никакой специальной информации и выдается образцам атак по мере внесения в базу знаний. У каждой записи CAPEC имеется заголовок и описание. Описание представляет собой краткое изложение того, о чем идет речь в шаблоне атаки. Почти у каждой записи CAPEC имеется поле с связанными с ним CWE (недостатков ПО). Пример приведен на рис. 2.



Связанные недостатки

CWE-ID	Имя слабости
522	Недостаточно защищенные учетные данные
836	Использование хэша пароля вместо пароля для аутентификации
308	Использование однофакторной аутентификации
294	Обход аутентификации с помощью Capture-replay
308	Использование однофакторной аутентификации

Рис. 2. Пример поля со приведенными типами ошибок CWE на сайте CAPEC

Стоит обратить внимание, что сопоставление между записями CAPEC и недостатками CWE не обязательно является отношением один к одному. Шаблон атаки может потребовать использования всех перечисленных слабых мест, подмножества или только одного.

Далее имеется поле «Сценарий выполнения (Execution Flow)» дает инструкции о том, как выполнить атаку (рис. 3).

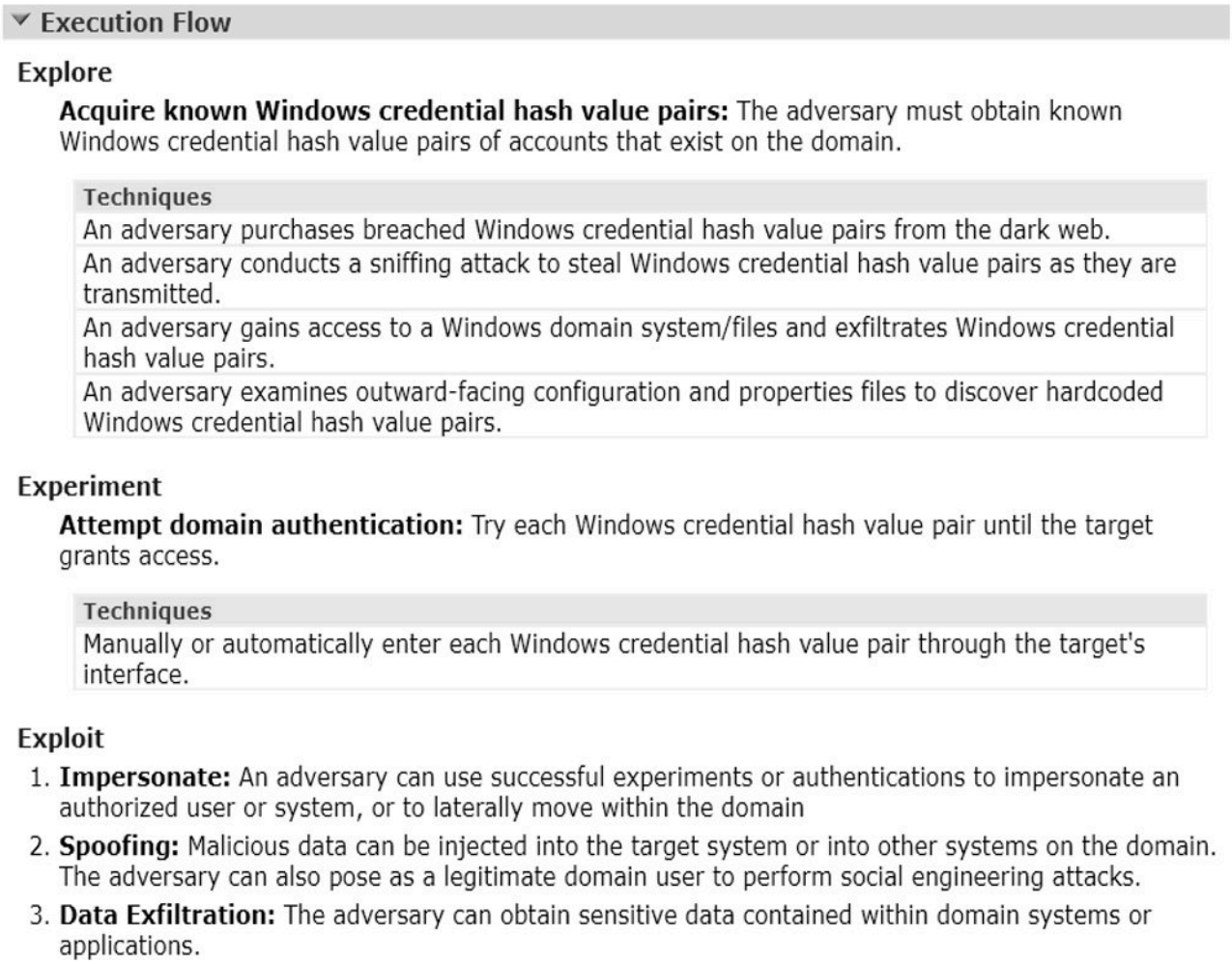


Рис. 3. Пример поля «Сценарий выполнения» на сайте CAPEC

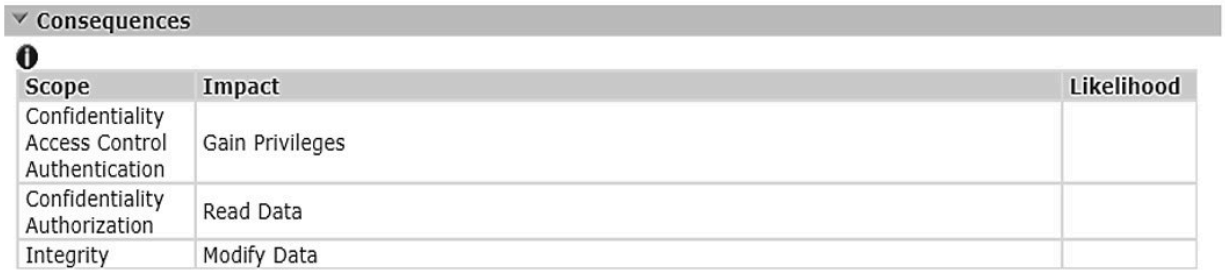
Потоки выполнения обычно состоят из трех фаз:

1) исследование: на этом этапе описываются различные способы поиска потенциальной цели для атаки. Все три этапа иногда включают более одного шага. Каждый шаг предлагает различные методы выполнения этого шага,

2) эксперимент: после того, как цель найдена, методы экспериментальной фазы потока выполнения предлагают различные способы определения того, содержит ли эта цель уязвимость, которую хочет использовать эта запись CAPEC,

3) эксплойт: предлагаемые методы проведения фактической атаки.

Последствия успешной атаки с использованием этого паттерна перечислены в разделе «Последствия». Пример приведен на рис. 4.



Consequences

Scope	Impact	Likelihood
Confidentiality Access Control Authentication	Gain Privileges	
Confidentiality Authorization	Read Data	
Integrity	Modify Data	

Рис. 4. Пример поля «Последствия» на сайте CAPEC

Также в некоторых шаблонах (преобладает меньшинство) имеется поле «Сопоставление таксономии», которое приводит исследователя к технике из матрицы MITRE ATT&CK (рис. 5).

Taxonomy Mappings

Relevant to the ATT&CK taxonomy mapping

Entry ID	Entry Name
1550.002	Use Alternate Authentication Material:Pass The Hash

Рис. 5. Пример поля «Taxonomy Mappings»

Поле «Тип ошибки CWE» предоставляет исследователю информацию о ошибках программного обеспечения, которые могут привести к созданию уязвимости в разрабатываемом программном обеспечении. Поэтому также необходимо рассматривать CWE как звено в формализации информации о многообразии кибератак.

1.2 Исследование базы знаний CWE

Common Weakness Enumeration (CWE) — поддерживаемая и развиваемая сообществом система классификации недостатков безопасности. CWE выступает в качестве общего языка, позволяющего описывать (а как следствие — предотвращать) недостатки безопасности в программном и аппаратном обеспечении. Под недостатками безопасности понимаются сбои и ошибки при реализации программного или аппаратного обеспечения, в проектировании, архитектуре и т.д., которые могут сделать конечный продукт уязвимым к различного рода атакам. Основная цель CWE — предотвращать возникновение уязвимостей за счёт обучения специалистов способам избегания наиболее распространённых ошибок. То есть в конечном итоге CWE позволяет избегать уязвимости, которым подвержено программное и аппаратное обеспечение.

Актуальность использования базы знаний CWE

CWE активно поддерживается и обновляется сообществом, включая представителей ведущих производителей операционных систем, коммерческих инструментов информационной безопасности, академических кругов, государственных агентств и исследовательских институтов. Обновление происходит ежегодно и включают в себя:

- добавление новых слабостей, которые были обнаружены или стали актуальными с момента последнего обновления;
- обновление существующих записей CWE с учетом новых данных, улучшений в описаниях;

CWE используется в качестве общего стандарта для идентификации, смягчения и предотвращения уязвимостей.

Полнота предоставляемой информации

CWE содержит подробные описания слабостей, включая режимы внедрения, потенциальные меры по устранению и типичные последствия эксплуатации уязвимостей. В базе знаний на данный момент содержится 959 типов ошибок программного обеспечения.

CWE предоставляет демонстрационные примеры кода и наблюдаемые примеры, которые иллюстрируют проблемы в реальных продуктах.

Совместимость с другими информационными ресурсами

CWE обеспечивает внешние отображения содержимого на связанные ресурсы, такие как база данных уязвимостей NVD NIST и MITRE CAPEC. Таким образом появляется возможность связать описанные в базе знаний CAPEC шаблоны атак и уязвимости CVE базы данных NVD NIST [5].

Содержание данных для риск-анализа угроз

Использование информации, предоставляемой базой данных CWE, во всем ее многообразии не позволяет применить ее для риск-аналитики угроз информационной безопасности приложений, ввиду ее основного назначения - обучения специалистов способам избегания наиболее распространённых ошибок программного обеспечения.

Обзор предоставляемой ресурсом информации

Каждый тип ошибки программного обеспечения CWE, согласно приведенной схеме, указанной на ресурсе с базой знаний может содержать следующую информацию (табл. 2).

Таблица 2

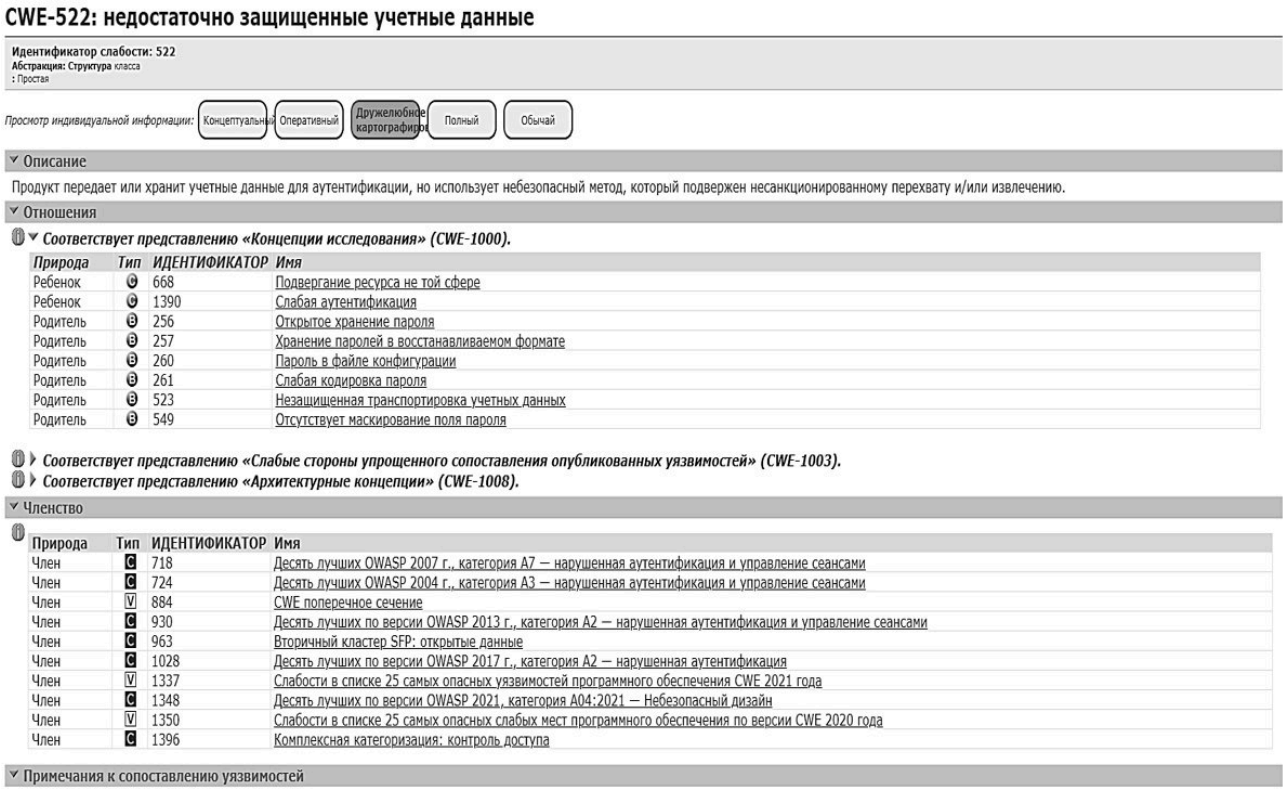
Наименование и краткое описание полей типа ошибки CWE

Название поля	Описание
CWE-ID	Уникальный числовой идентификатор, присвоенный каждой слабости в базе данных CWE.
Name	Официальное название слабости, как оно представлено в CWE.
Weakness Abstraction	Уровень абстракции слабости, указывающий на её общность или специфичность.
Status	Текущее состояние слабости, например, "Активный", "Устаревший" или "Черновик".
Description	Краткое описание слабости, включая её природу и потенциальные последствия.
Extended Description	Расширенное описание слабости с дополнительными деталями
Related Weaknesses	Список связанных слабостей, которые могут быть связаны или использоваться вместе.
Weakness Ordinalities	Категоризация слабости по её порядковому номеру или типу.
Applicable Platforms	Платформы, на которых слабость может проявляться
Background Details	Информация о фоне, которая может помочь в понимании слабости.
Alternate Terms	Другие термины или названия, которые могут использоваться для обозначения слабости.
Modes Of Introduction	Способы, которыми слабость может быть введена в систему или программное обеспечение.
Exploitation Factors	Факторы, которые могут способствовать эксплуатации слабости, выраженные числовым значением
Likelihood of Exploit	Вероятность эксплуатации слабости, выраженная числовым значением.
Common Consequences	Общие последствия, которые могут возникнуть в результате эксплуатации слабости.

Продолжение табл. 2

Название поля	Описание
Detection Methods	Методы обнаружения слабости.
Potential Mitigations	Потенциальные меры предосторожности или методы, которые могут быть применены для устранения или смягчения слабости.
Observed Examples	Примеры, в которых наблюдалась данная слабость.
Functional Areas	Функциональные области системы или программного обеспечения, которые могут быть затронуты слабостью
Affected Resources	Ресурсы, которые могут быть затронуты слабостью.
Taxonomy Mappings	Ссылки на другие классификации или таксономии, где слабость также может быть найдена.
Related Attack Patterns	Список связанных шаблонов атак, которые могут быть связаны или использоваться вместе со слабостью.
Notes	Дополнительные заметки, комментарии или уточнения относительно слабости.

Рассмотрим пример ошибки CWE из выбранного ранее образца атаки CAPEC, а именно CWE-522 (рис. 6).



CWE-522: недостаточно защищенные учетные данные

Идентификатор слабости: 522
Абстракция: Структура класса
: Простая

Просмотр индивидуальной информации: Концептуальный | Оперативный | Дружелюбное картографирование | Полный | Обычай

▾ Описание

Продукт передает или хранит учетные данные для аутентификации, но использует небезопасный метод, который подвержен несанкционированному перехвату и/или извлечению.

▾ Отношения

Соответствует представлению «Концепции исследования» (CWE-1000).

Природа	Тип	ИДЕНТИФИКАТОР	Имя
Ребенок	B	668	Подвергание ресурса не той сфере
Ребенок	B	1390	Слабая аутентификация
Родитель	B	256	Открытое хранение пароля
Родитель	B	257	Хранение паролей в восстанавливаемом формате
Родитель	B	260	Пароль в файле конфигурации
Родитель	B	261	Слабая кодировка пароля
Родитель	B	523	Незащищенная транспортировка учетных данных
Родитель	B	549	Отсутствует маскирование поля пароля

Соответствует представлению «Слабые стороны упрощенного сопоставления опубликованных уязвимостей» (CWE-1003).
Соответствует представлению «Архитектурные концепции» (CWE-1008).

▾ Членство

Природа	Тип	ИДЕНТИФИКАТОР	Имя
Член	C	718	Десять лучших OWASP 2007 г., категория A7 – нарушенная аутентификация и управление сеансами
Член	C	724	Десять лучших OWASP 2004 г., категория A3 – нарушенная аутентификация и управление сеансами
Член	V	884	CWE поперечное сечение
Член	C	930	Десять лучших по версии OWASP 2013 г., категория A2 – нарушенная аутентификация и управление сеансами
Член	C	963	Вторичный кластер SFP: открытые данные
Член	C	1028	Десять лучших по версии OWASP 2017 г., категория A2 – нарушенная аутентификация
Член	V	1337	Слабости в списке 25 самых опасных уязвимостей программного обеспечения CWE 2021 года
Член	C	1348	Десять лучших по версии OWASP 2021, категория A04:2021 – Небезопасный дизайн
Член	V	1350	Слабости в списке 25 самых опасных слабых мест программного обеспечения по версии CWE 2020 года
Член	C	1396	Комплексная категоризация: контроль доступа

▾ Примечания к сопоставлению уязвимостей

Рис. 6. Пример карточки типа ошибки CWE

Как и в рассмотренном ранее CAPEC-644 имеется поле описания и названия. Номер CWE также не несет никакой информативности. Наиболее интересующее нас поле для изучения – поле «Связанные шаблоны атак (Related Attack Patterns)» (рис. 7).

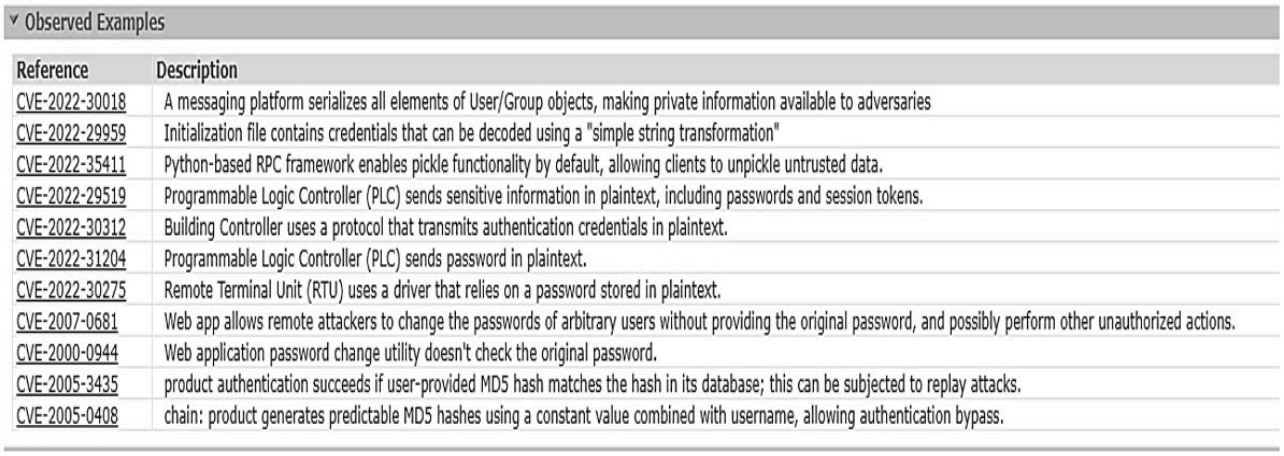
Related Attack Patterns

CAPEC-ID	Attack Pattern Name
CAPEC-102	Session Sidejacking
CAPEC-474	Signature Spoofing by Key Theft
CAPEC-50	Password Recovery Exploitation
CAPEC-509	Kerberoasting
CAPEC-551	Modify Existing Service
CAPEC-555	Remote Services with Stolen Credentials
CAPEC-560	Use of Known Domain Credentials
CAPEC-561	Windows Admin Shares with Stolen Credentials
CAPEC-600	Credential Stuffing
CAPEC-644	Use of Captured Hashes (Pass The Hash)
CAPEC-645	Use of Captured Tickets (Pass The Ticket)
CAPEC-652	Use of Known Kerberos Credentials
CAPEC-653	Use of Known Operating System Credentials

Рис. 7. Пример поля «Связанные шаблоны атак» для типа ошибки CWE

На рис. 7 представлена информация о том, в каких образцах атак содержится рассматриваемый тип ошибки CWE. Рассматриваемый ранее CAPEC-644 здесь также присутствует.

Одним из ключевых также является поле «Observed Examples», содержащее все уязвимости CVE, в который используется данный тип ошибки CWE (рис. 8).



Observed Examples

Reference	Description
CVE-2022-30018	A messaging platform serializes all elements of User/Group objects, making private information available to adversaries
CVE-2022-29959	Initialization file contains credentials that can be decoded using a "simple string transformation"
CVE-2022-35411	Python-based RPC framework enables pickle functionality by default, allowing clients to unpickle untrusted data.
CVE-2022-29519	Programmable Logic Controller (PLC) sends sensitive information in plaintext, including passwords and session tokens.
CVE-2022-30312	Building Controller uses a protocol that transmits authentication credentials in plaintext.
CVE-2022-31204	Programmable Logic Controller (PLC) sends password in plaintext.
CVE-2022-30275	Remote Terminal Unit (RTU) uses a driver that relies on a password stored in plaintext.
CVE-2007-0681	Web app allows remote attackers to change the passwords of arbitrary users without providing the original password, and possibly perform other unauthorized actions.
CVE-2000-0944	Web application password change utility doesn't check the original password.
CVE-2005-3435	product authentication succeeds if user-provided MD5 hash matches the hash in its database; this can be subjected to replay attacks.
CVE-2005-0408	chain: product generates predictable MD5 hashes using a constant value combined with username, allowing authentication bypass.

Рис. 8. Пример поля «Связанные шаблоны атак» для типа ошибки CWE

Очевидная взаимосвязь между шаблонами атаки CAPEC и типам ошибки CWE приводит исследователя к еще одной взаимосвязи – уязвимостям CVE.

1.3 Исследование базы знаний CVE

Common Vulnerabilities and Exposures (CVE) – список известных уязвимостей и дефектов безопасности. Цель CVE – выявлять, описывать и каталогизировать информацию о публично раскрытых уязвимостях. Список создавался для унификации именования и регистрации обнаруженных дефектов безопасности. CVE позволяет специалистам по безопасности, инструментам обнаружения уязвимостей и базам данных уязвимостей получать и обмениваться информацией о конкретных дефектах. Благодаря этому они могут быть уверены, что имеется ввиду одна и та же проблема.

MITRE Corporation – американская некоммерческая организация, которая занимается исследованиями в области

системной инженерии. Она поддерживает различные проекты, связанные с безопасностью, включая CVE и CWE.

CVE – это система, которая предоставляет стандартизированные идентификаторы для уязвимостей в программном обеспечении и аппаратном обеспечении. CWE – это система, которая классифицирует различные типы уязвимостей.

Актуальность использования базы знаний CVE

База знаний CVE играет ключевую роль в индустрии информационной безопасности, предоставляя стандартизированный список уязвимостей. Перечень уязвимостей активно поддерживается корпорацией MITRE и финансируется Отделением национальной безопасности США, пополняется и обновляется ежедневно [4].

Полнота предоставляемой информации

База CVE обеспечивает описание уязвимостей, назначение уникального идентификатора и ссылки на дополнительную информацию. На данный момент на информационном ресурсе размещено 222,637 уязвимостей, но стоит отметить, что не все уязвимости, зарегистрированные в CVE, остаются активными. Производители программного обеспечения регулярно выпускают патчи и обновления для исправления уязвимостей, после чего они перестают быть актуальными для эксплуатации.

Совместимость с другими информационными ресурсами

CVE тесно связана с другими ресурсами, такими как NVD, которая предоставляет анализ каждой уязвимости, опубликованной в списке CVE, и может включать оценки CVSS и информацию CWE. Такая интеграция обогащает базу CVE, делая её более полезной для анализа угроз и управления рисками. Таким образом появляется возможность отследить смысловую последовательность «шаблон атаки CAPEC – тип ошибки программного обеспечения CWE – уязвимость CVE».

Содержание данных для риск-анализа угроз

База CVE предоставляет основную информацию для оценки рисков, связанных с уязвимостями, включая идентификаторы CVE и описания уязвимостей. Для получения более подробной информации пользователи могут обратиться к NVD, которая предоставляет оценки CVSS, включающие в себя метрики эксплуатации и воздействия уязвимостей. Эти данные могут быть использованы для качественной и количественной оценки угроз, что важно для планирования мер по оценке и регулированию рисков, а также управления угрозами.

Обзор предоставляемой ресурсом информации

Рассмотрим карточку уязвимости CVE-2022-23067 в качестве примера для определения информационно ценных полей (рис. 9).

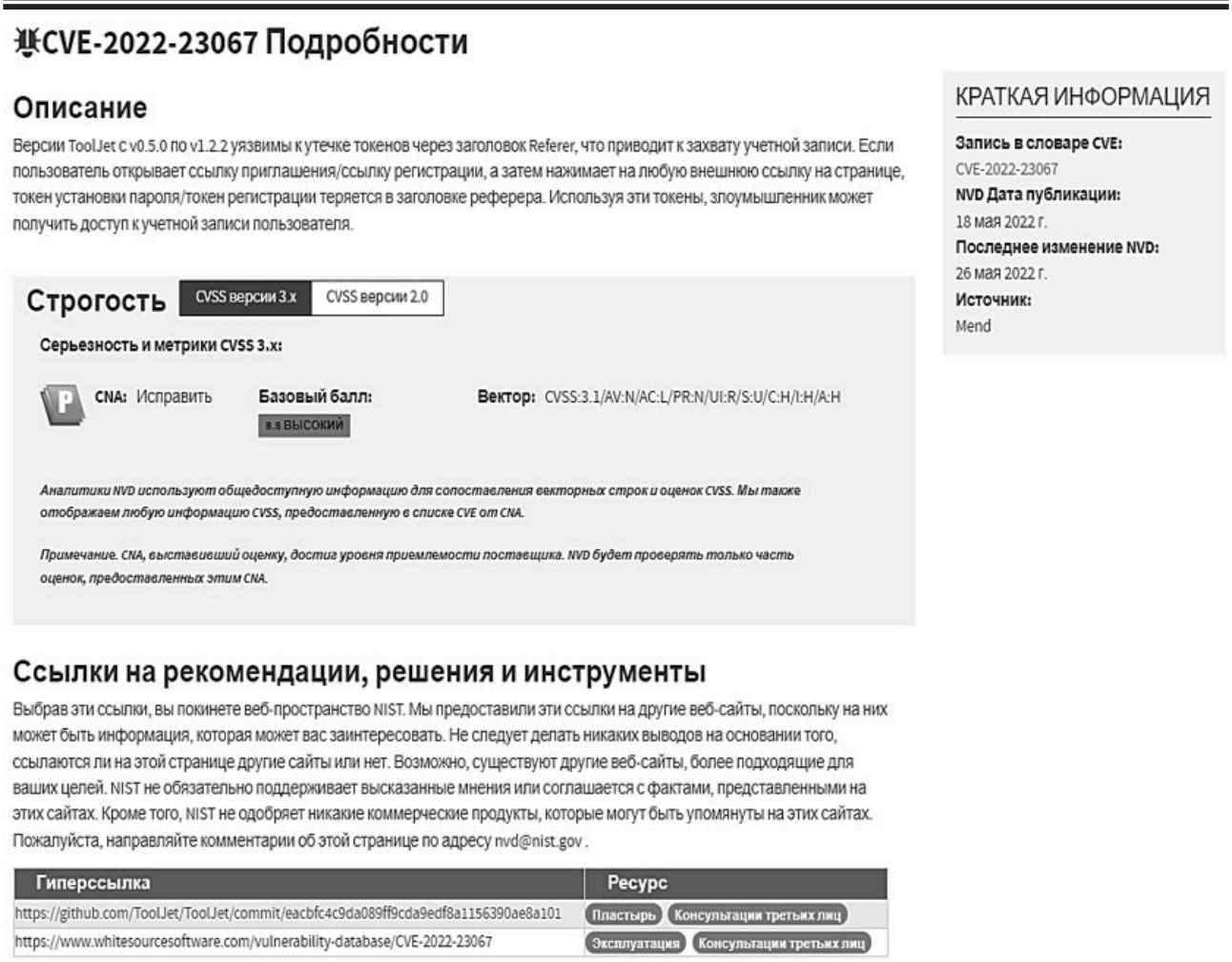


Рис. 9. Пример карточки CVE на сайте nvd.nist

Для каждой уязвимости CVE обязательными полями для заполнения являются описание, оценка ее критичности, рассчитывающая на основе калькулятора CVSS, ссылки на рекомендации по ее устранению и перечисление типов ошибок CWE используемых при ее реализации. В свою очередь метрики оценки критичности являются важной информацией, позволяющей использовать их для риск-анализа (рис. 10).

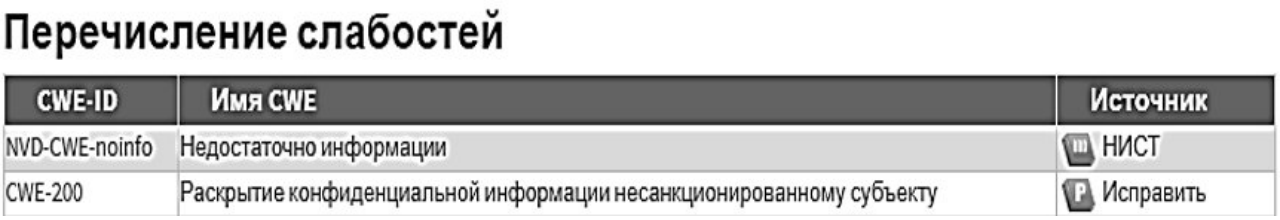


Рис. 10. Пример поля «Перечисление слабостей» для уязвимости CVE

Информационный ресурс CVE NIST также предоставляет данные о используемых типах ошибки программного обеспечения CWE.

Проблема использования базы знаний состоит в том, что при всем ее многообразии уязвимостей большинство являются либо неактуальными из-за отсутствия подтверждения их эксплуатации, либо из-за практического отсутствия использования уязвимого устаревшего программного, программно-аппаратного обеспечения. Поэтому обратимся с следующему ресурсу, основанному на использовании базы знаний CVE NIST.

1.4 Исследование базы знаний CISA KEV

CISA KEV (Known Exploited Vulnerabilities) Catalog является источником информации, поддерживаемым Агентством кибербезопасности и инфраструктурной безопасности США (CISA), который содержит перечень уязвимостей, которые были активно эксплуатированы злоумышленниками. Этот каталог предназначен для использования организациями с целью приоритизации устранения уязвимостей, чтобы снизить вероятность компрометации известными угрозами [7].

Актуальность использования базы знаний CISA KEV

Актуальность базы данных CISA KEV заключается в том, что она содержит информацию об уязвимостях, которые были использованы в реальных атаках, и является авторитетным источником для сетевых защитников и сообщества кибербезопасности. База регулярно обновляется для отражения новых эксплуатируемых уязвимостей, что делает ее актуальной для организаций, стремящихся управлять уязвимостями и соответствовать активности угроз. Все федеральные гражданские исполнительные органы США (FCEB) обязаны устранять уязвимости, перечисленные в каталоге KEV, в установленные сроки в соответствии с Директивой по оперативным действиям (BOD) 22-01, что подчеркивает важность базы данных для государственных организаций.

Полнота предоставляемой информации

Каталог KEV предоставляет информацию, включая идентификаторы CVE, данные о производителе, продукте, дате добавления уязвимости в список и предписанном сроке устранения. Для каждой уязвимости предоставляется руководство по устранению, что позволяет организациям предпринимать четкие действия для защиты своих систем.

Совместимость с другими информационными ресурсами

CISA KEV представляет собой каталог активно эксплуатируемых уязвимостей CVE, поэтому совместимость с другими информационными ресурсами аналогична NVD NIST CVE.

Содержание данных для риск-анализа угроз

Информация, описывающая уязвимости информационного ресурса CISA KEV, аналогична информации CVE NIST. Она также включает описание метрик для подсчета оценки критичности CVSS.

Обзор предоставляемой ресурсом информации

На главной странице ресурса предоставляется каталог известных эксплуатируемых уязвимостей. На данный момент в нем содержится 1069 уязвимостей. Список уязвимостей постоянно меняется исходя из наличия доказательств их эксплуатации (рис. 11).

При нажатии на идентификатор уязвимости исследователь перенаправляется на страницу уязвимости ранее рассмотренного ресурса NVD NIST CVE.

Ценностью CISA KEV, в отличии от CVE NIST является тот факт, что приведенные здесь уязвимости, которые были замечены в инцидентах информационной безопасности. Поэтому при построении сочетаний вектор атаки – уязвимость уместно использовать данный ресурс, вместо CVE NIST.

На данном этапе имеет смысл сформировать дерево проектной деятельности, представленного на рис. 12:

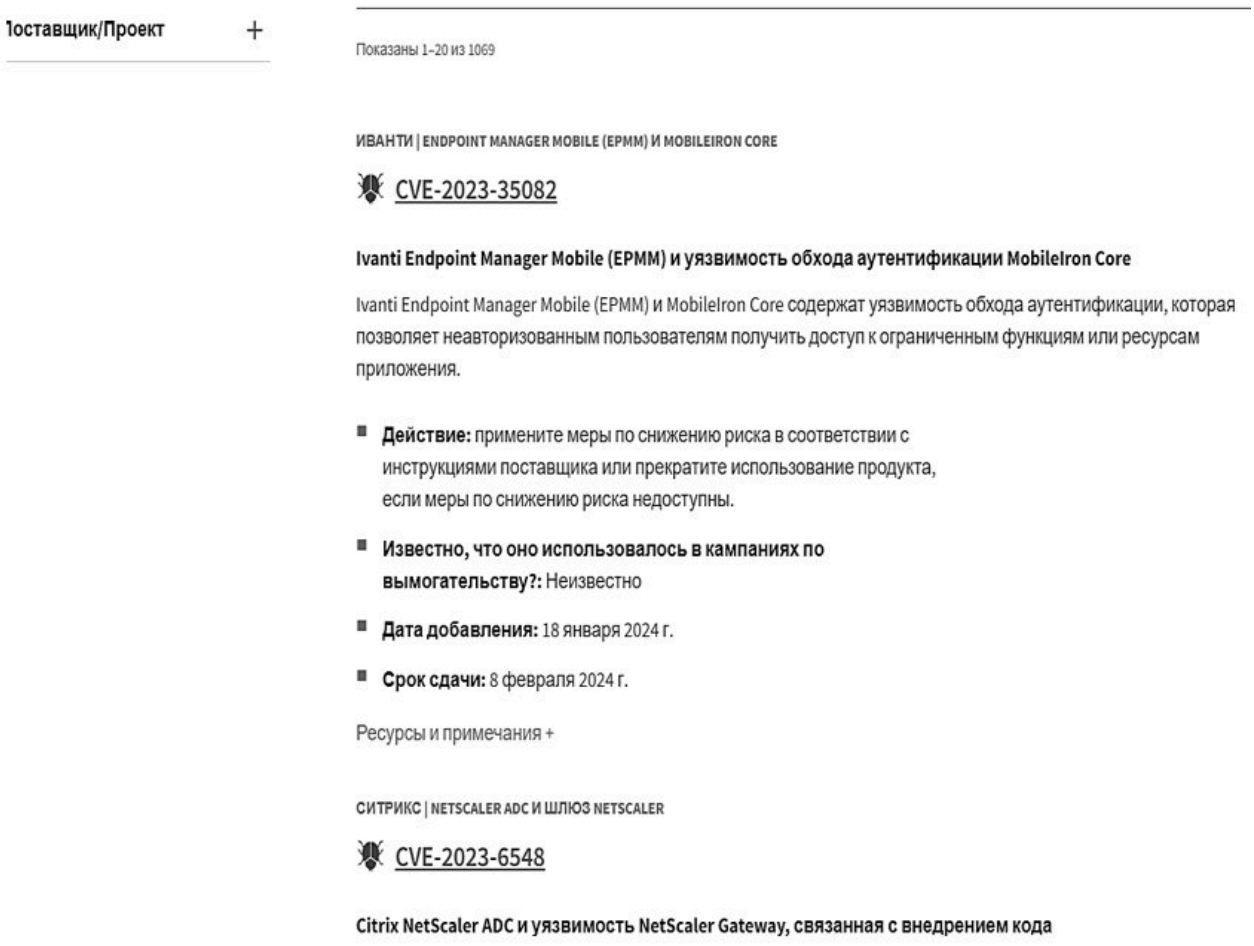


Рис. 11. Главная страница каталога KEV

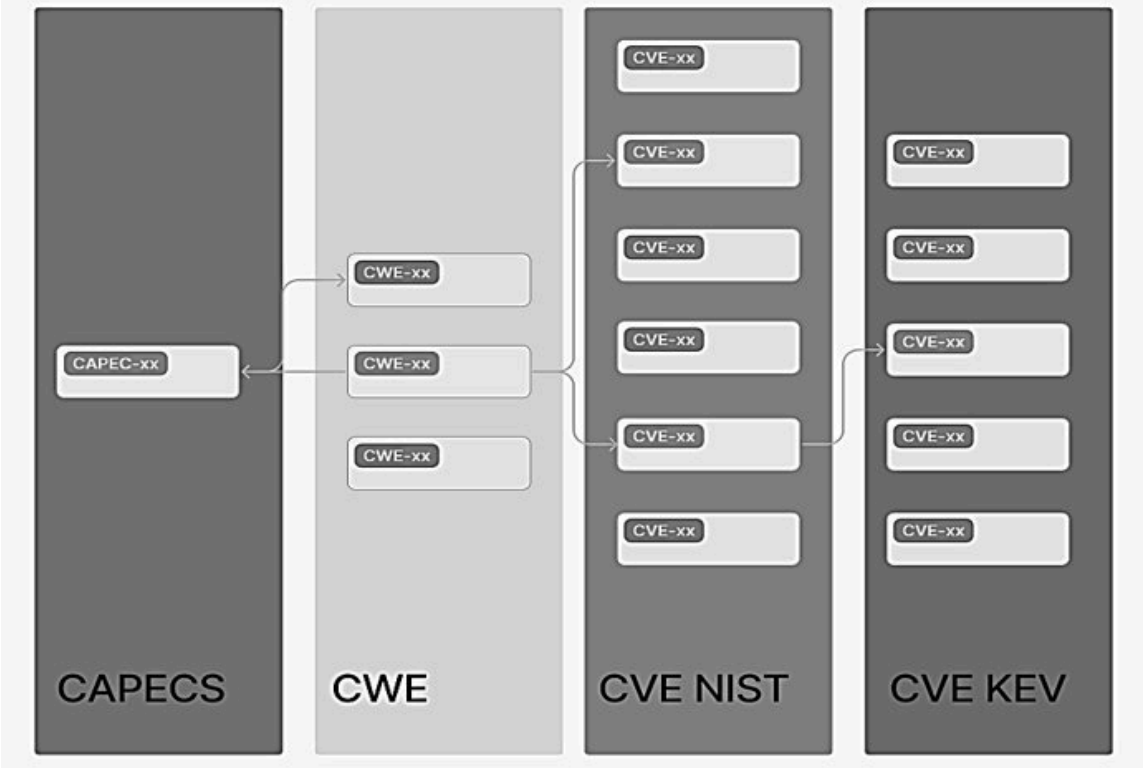


Рис. 12. Дерево проектной деятельности

Данное дерево позволяет рассмотреть для множества шаблонов атак CAPEC, соответствующие им типы ошибок CWE, которые могут быть проэксплуатированы в уязвимостях CVE и выделить те уязвимости CVE KEV, факт успешной эксплуатации которых подтвержден.

Методическое обеспечение калькуляции риска

Сущность предлагаемого подхода вытекает из определения безопасности как состояния системы, мерилом которого выступает риск – показатель возможности наступления ущерба. При этом, мерой риска выступает произведение величины ущерба на значение вероятности ее наступления. В данной формулировке четко просматривается прямая причинно-следственная связь между ущербом и возможностью (измеренную вероятностью) ею наступления. В свою очередь данная вероятность (в нашем случае) описывается произведением (совместное событие) вероятности успешной реализации вектора кибератаки и вероятности использования соответствующем ему уязвимости (здесь кроется вышеупомянутая причинно-следственная связь с ущербом, возникающим в рассматриваемой уязвимости под воздействием избранного вектора атаки).

Именно в этом контексте целесообразно оценивать опасность возникающих в киберпространстве вредоносных пар: сценарий (вектор) атаки-уязвимость защищаемой системы. В этом ракурсе рассмотрим безопасность атакуемых АИС и ТКС через «его величество» риск.

Анализ системы оценки критичности уязвимостей

Для оценки критичности уязвимостей в базе знаний NIST [5] предусмотрено использование калькулятора CVSS.

Существует две версии калькулятора оценки критичности уязвимости:

1) CVSS версии 2.0;

2) CVSS версии 3.0.

Метрики, учитывающие реакцию производителя уязвимого продукта, которые применяются с момента обнаружения уязвимости и до момента ее поправления:

1) эксплуатационные возможности (E), показывающие текущее состояние способов эксплуатации уязвимости,

2) поправочный показатель (RL), который является корректирующим числом, позволяющим смягчить временную оценку по мере того, как становятся доступны направления уязвимости,

3) показатель уверенности (RC) позволяет измерить уровень уверенности в существовании уязвимости и достоверности ее технических данных.

Необходимо понимать, что информация о уязвимостях представлена с помощью экспертных оценок, которые, как известно, страдают существенной субъективностью. Усугубляется ситуация тем, что не каждый производитель готов откровенно делится подобными данными

Метрики уязвимости, учитывающие **конкретные требования безопасности к защищаемой системе**, в которой наличествует уязвимый продукт:

1) сопутствующий ущербный потенциал (CDP) учитывает потенциальный ущерб для компании от данной уязвимости,

2) распределение мишеней (TO) оценивает долю уязвимых компонент системы,

3) воздействие элементов модификации учитывают корректирующие числа конфиденциальности (CR), целостности (IR) и доступности (AR), позволяющие изменить метрики и конечную оценку под конкретные требования безопасности конкретного окружения уязвимости.

Здесь речь идет о специфике защищаемой системы в контексте ущербов, возможных в рассматриваемой уязвимости. Однако формализация поиска перечисленных в данном разделе параметров весьма непроста, что существенно затрудняет калькуляцию особенно при наличии множества уязвимостей.

Если говорить об аналитических выражениях расчетов по второй версии калькулятора CVSS, то они таковы:

$$E = 20 * AV * AC * Au;$$
$$Impact = 10{,}41 * [1 - (1 - C) * (1 - I) * (1 - A)];$$

$$f\,(Impact) = \begin{cases} 0, \text{ при } Impact = 0 \\ 1{,}176 \text{ в других случаях} \end{cases};$$

Базовая мера (БМ) = округление до первого десятичного разряда для $[0{,}6Impact + (0{,}4E) - 1{,}5] * f(Impact)$;

Временная мера (ВМ) = округление до первого десятичного разряда для $[\text{БМ} * E * RL * RC]$;

Мера воздействия (МВ) $= \min\,[10; 10.41 * (1 - (1 - C * CR) * (1 - I * IR) * (1 - A * AR))]$;

Мера уязвимости (МУ) = округление до первого десятичного разряда для $[\text{МВ} + (10 - \text{МВ}) * CDP * TD]$, и вызывают множество вопросов.

Исходя из данных аналитических выражений можно сделать следующие выводы:

1. Видимо, почерпнутая из теории вероятности форма

$$[(1 - (1 - C) * (1 - I) * (1 - A)] = \\ = C + I + A - CI - IA - CA + CIA$$

приводит нас к знакопеременному ряду всевозможных одиночных, попарных и тройного сочетания нарушений конфиденциальности, целостности и доступности, что совершенно непонятно с точки зрения риск-анализа, ибо требует приведения их единой размерности ущерба (несмотря на их не несовместимую сущность, что подтверждено выше).

2. Требуют также своего обоснования формы поголовного перемножения параметров в рамках выделенных метрик.

3. Численные значения коэффициентов и слагаемых, видимо вытекают из «опыта – сына ошибок трудных». При этом, нет никакой уверенности, что не одна из них.

Таким образом, несмотря на масштабность полей данных различных сочетаний вектор-уязвимость, предоставленных авторами калькулятора, его версия 2.0 методически неприемлема для оценки рисков киберинцидентов. Поэтому, необходим поиск других форм представления и обработки параметров процессов нарушения информационной безопасности.

Исходя из этого очевидно, что для подсчета риска для пар «вектор атаки – уязвимость» необходимо разработать собственную калькуляцию с использованием предоставляемой нам информации о уязвимостях.

Методическое обеспечение оценки рисков сочетаний пар «вектор атаки – уязвимость».

Построение риск ландшафта сопровождается процедурой расчета риска каждой из пар «вектор атаки – уязвимость».

Используя общую формулу расчета риска

$$Risk = P \times U,$$

применительно к кибератакам, формула будет выглядеть следующим образом:

$$Risk_{AiYj} = P_{AiYj} \times U_{AiYj}, \qquad (1)$$

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

P_{AiYj}– вероятность успешности сочетания *i*-го вектора атаки *A* и *j*-ой уязвимости *Y*;

U_{AiYj} – ущерб от сочетания *i*-го вектора атаки *A* и *j*-ой уязвимости *Y*.

Так как мы рассматриваем $Risk_{AiYj}$ для сочетания *i*-го вектора атаки *A* с используемой *j*-ой уязвимостью *Y*, то уместно предположить, что вероятность успешности *i*-го вектора атаки *A* и вероятность успешности *j*-ой уязвимости *Y* являются совместными событиями, поэтому:

$$P_{AiYj} = P_{Ai} \times P_{Yj}, \qquad (2)$$

где P_{Ai} – вероятность успешности эксплуатации *i*-ой атаки *A*;

P_{Yj} – вероятность успешности *j*-ой уязвимости *Y*;

Верно утверждать о том, что в случае успешной кибератаки, ущерб U_{AiYj} от сочетания *i*-го вектора атаки *A* с используемой *j*-ой уязвимостью *Y*, будет зависеть только от ущерба, нанесенного в случае успешной эксплуатации *j*-той уязвимости *Y*.

Исходя из вышеописанного, уместно сделать следующее преобразование:

$$U_{AiYj} = U_{Yj}, \quad (3)$$

где U_{Yj} – ущерб в случае успешной эксплуатации *j*-ой уязвимости *Y*.

Выразить P_{Ai} вероятность успешности *i*-ой атаки *A* мы можем, воспользовавшись данными из базы знаний ресурса CAPEC. Так как для определения сценария атаки (вектора атаки) мы используем образцы (шаблоны) атак, описанные в CAPEC, то уместно было бы использовать для определения вероятности ее (атаки) успешности данные из этого же источника. У каждого образца атаки в базе знаний CAPEC имеется поле – «Вероятность успешности атаки (Likelihood Of Attack)», представляющая ценность для использования ее значения в качестве переменных для подсчета $Risk_{AiYj}$.

Так как информация о P_{Ai} вероятности успешности *i*-ой атаки *A* описана в виде качественной оценки, то будет уместно в данном случае преобразовать качественные значения в количественные (табл. 3).

Таблица 3

Сопоставление качественных характеристик с количественными

Качественная оценка	Количественная оценка
Очень низкая (Very Low)	0,1
Низкая (Low)	0,3
Средняя (Medium)	0,5
Высокая (High)	0,7
Очень высокая (Very High)	0,9

В тоже время информационный ресурс NVD NIST приводит количественные показатели некоторых метрик, которые используются для подсчета оценки критичности уязвимости CVSS v2.0 и v3.0. Используем показатели значений CVSS, оказывающих влияние на вероятность успешной эксплуатации уязвимости CVE, а именно базовые метрики уязвимости, упоминающийся в предыдущем пункте главы.

При этом необходимо учитывать, что метрика CVSS v3.0 наиболее полно описывает данные показатели, нежели метрики CVSS v2.0, поэтому если уязвимость включает информацию в виде обеих версий метрик, то метрика третьей версии будет приоритетной в расчетах.

1. Метрики, использующееся для CVSS v2.0:

- вектор доступа (Access Vector) (AV);
- сложность доступа (Access Complexity) (AC);
- аутентификационный параметр (Authentication) (Au).

2. Метрики, использующееся для CVSS v3.0:

- вектор атаки (Attack Vector) (AV);
- сложность эксплуатации уязвимости (Attack Complexity) (*AC*);
- требуемый уровень привилегий (Privileges Required) *(PR)*;
- необходимость взаимодействия с пользователем (User Interaction) *(UI)*.

Данные метрики представлены в качественных значениях, в связи с чем появляется необходимость преобразования этих значений в количественные.

Приведем сопоставления для метрик CVSS v2.0.

Вектор доступа (Access Vector) (AV) показывает, каким путем уязвимость может быть внедрена (табл. 4).

Таблица 4

«Сопоставление метрик Access Vector»

Качественное значение метрики	Количественное значение метрики
Локальный (L)	0,5
Соседняя сеть (A)	0,7
Сетевой (N)	0,9

Сложность доступа (Access Complexity) (AC) показывает, насколько легко или сложно использовать данную уязвимость (табл. 5).

Таблица 5

«Сопоставление метрик Access Complexity»

Качественное значение метрики	Количественное значение метрики
High (Высокая сложность)	0,5
Medium (Средняя сложность)	0,7
Low (Низкая сложность)	0,9

Аутентификационный параметр (Authentication) (Au), оценивающий количество аутентификаций, которые атакующий должен произвести прежде, чем воспользоваться уязвимостью (табл. 6).

Таблица 6

«Сопоставление метрик Authentication»

Качественное значение метрики	Количественное значение метрики
Множественный (M)	0,5
Одиночный (S)	0,7
Отсутствует (N)	0,9

Приведем сопоставления для метрик CVSS v3.0.

Вектор атаки (Attack Vector) *(AV)* – Степень удаленности потенциального атакующего от уязвимого объекта (табл. 7).

Таблица 7

«Сопоставление метрик Attack Vector»

Качественное значение метрики	Количественное значение метрики
Локальный (L)	0,5
Соседняя сеть (A)	0,7
Сетевой (N)	0,9
Физический (P)	0,3

Сложность эксплуатации уязвимости (Attack Complexity) (*AC*) – качественная оценка сложности проведения атаки представлена в табл. 8.

Таблица 8

«Сопоставление метрик Attack Complexity»

Качественное значение метрики	Количественное значение метрики
High (Высокая сложность);	0,3
Low (Низкая сложность).	0,8

Требуемый уровень привилегий (Privileges Required) *(PR)* показывает, требуется ли аутентификация для проведения атаки, и если требуется, то какая именно (табл. 9 и 10).

Таблица 9

«Сопоставление метрик Privileges Required»

Качественное значение метрики	Количественное значение метрики
High (Высокий уровень привилегий);	0,3
Low (Низкий уровень привилегий).	0,5
None (Не требуется)	0,8

Необходимость взаимодействия с пользователем (User Interaction) *(UI):*

Таблица 10

«Сопоставление метрик User Interaction»

Качественное значение метрики	Количественное значение метрики
Требуется	0,3
Не требуется	0,8

Отсюда вероятность успешного использования *j*-ой уязвимости *Y* посредством *i*-ой атаки *A* для CVSS v2.0 имеет вид:

$$P_{AiYj\,2.0} = P_{Ai}\prod_{m=1}^{3} P_{Yj}(m), \quad (4)$$

где $P_{Yj}(m)$ для m=1(1)3 – определяется из вышеперечисленных показателей метрик CVSS v2.0;

P_{Ai} – как вероятность успеха i-ой атаки определяется по шкале {0; 0,1; 0,3; 0,5; 0,7; 0,9} исходя из предоставленных CAPEC информации о вероятности успешности атаки *A*.

Для CVSS v3.0 вероятность успешного использования j-ой уязвимости *Y* посредством i-ой атаки *A:*

$$P_{AiYj\,3.0} = P_{Ai}\prod_{m=1}^{4} P_{Yj}(m), \quad (5)$$

где $P_{Yj}(m)$ для m=1(1)4 – определяется из вышеперечисленных показателей метрик CVSS v2.0;

P_{Ai} – как вероятность успеха i-ой атаки определяется по шкале {0; 0,1; 0,3; 0,5; 0,7; 0,9} исходя из предоставленных CAPEC информации о вероятности успешности атаки *A*.

В свою очередь, ущербы оцениваются по шкале {0; 0,2; 0,5} раздельно для каждого вида (конфиденциальность, целостность, доступность) $\overline{U_к}$, $\overline{U_ц}$, $\overline{U_д}$. Видимо, их можно интерпретировать как доли утраченного информационного ресурса (соответствующего качества). Алгебраическое суммирование данных

ущербов некорректно (о чем уже упоминалось ранее) ввиду различия их сущностей.

Сведение оценок ущербности к некоторой единой размерности возможно через измерение ценности информации. Зная удельную (относительную к общей ценности информационных ресурсов системы) ценность поврежденной информации $\overline{C_{\text{к}}}$, $\overline{C_{\text{ц}}}$, $\overline{C_{\text{д}}}$, представляется возможным оценить нормированные риски:

$$\begin{aligned}\overline{Risk_{\text{к}}} &= P_{AY}\,\overline{U_{\text{к}}}\,\overline{C_{\text{к}}};\\ \overline{Risk_{\text{ц}}} &= P_{AY}\,\overline{U_{\text{ц}}}\,\overline{C_{\text{ц}}};\\ \overline{Risk_{\text{д}}} &= P_{AY}\,\overline{U_{\text{д}}}\,\overline{C_{\text{д}}}.\end{aligned} \tag{6}$$

Особым вопросом выступает рискоценка при использовании сразу нескольких k уязвимостей. В этом случае для (4) имеет место следующая форма:

$$\begin{aligned}\overline{Risk_{\text{кz}}} &= \sum_{s=1}^{k}\overline{Risk_{\text{кs}}};\\ \overline{Risk_{\text{цz}}} &= \sum_{s=1}^{k}\overline{Risk_{\text{цs}}};\\ \overline{Risk_{\text{дz}}} &= \sum_{s=1}^{k}\overline{Risk_{\text{дs}}}.\end{aligned} \tag{7}$$

Такое алгебраическое суммирование допустимо при отсутствии корреляции между рассматриваемыми уязвимостями. Иначе потребуется соответствующие правки.

Резюмируя данный раздел риск-анализа, уместно заметить, что вышеуказанные выражения работают в пространстве конкретных защищаемых АИС и ТКС, ибо сопряжены с ценностными оценками ресурса систем, что возможно при конкретном знании ее особенностей собственником и/или системным администратором.

Если же необходима обобщенно-абстрактная рискоценка (для класса, вида и типа векторов атаки), то следует воспользоваться выражением (7):

$$\begin{aligned}\overline{Risk_{\text{к}}} &= P_{AY}\,\overline{U_{\text{к}}};\\ \overline{Risk_{\text{ц}}} &= P_{AY}\,\overline{U_{\text{ц}}};\\ \overline{Risk_{\text{д}}} &= P_{AY}\,\overline{U_{\text{д}}}.\end{aligned} \tag{8}$$

Все изложенное выше относится к частичной утрате работоспособности защищаемой системы, так как повреждаются некоторые доли информационного ресурса, не останавливающие функционирование АИС и ТКС. В случае, когда необходимо для оценки ущерба оперировать уже временем простоя [1,8-10]. Тогда выражение риска примет следующий вид:

$$Risk = P_{AY}(\Delta t)\ \overline{C_{\text{п}}}, \tag{9}$$

где Δt – среднестатистическое значение простоя системы в результате успеха i-го вектора атаки;

$\overline{C_{\text{п}}}$ – стоимость единицы времени простоя атакуемой системы, известная ее собственнику.

По предложенным в настоящей работе аналитическим выражения (5)-(8) с использованием полей статданных и экспертных оценок [5,6] представляется возможным построение риск-ландшафтов [1,8-10] на плоскость реализуемых векторов атаки и используемых ими уязвимостей. При этом, имеется возможность построения ландшафта не только для данных, абстрагированных от конкретной защищаемой системы (4)-(6), но и с учетом особенностей ее ресурсов (5)-(8). Практический интерес представляет также сочетание ландшафта по отдельному виду вектора атаки, где можно сконцентрировать внимание на ликвидации (защите) наиболее

опасных уязвимостей. Его можно легко построить с помощью предложенного инструментария (5)-(8).

В целом, ландшафт является наглядным подспорьем для управления кибер-рисками.

Заключение

Пожалуй, впервые удалось столь глубоко и масштабно рассмотреть довольно актуальную научно-техническую задачу создания инструментария, интегрирующего пестрое и мало согласованное пространство данных, техник и мер противодействия кибератакам, включая целеполагание, риск-анализ и формирование знаний о регламентации борьбы с компьютерными инцидентами.

Разумеется, не все удалось учесть и точно сформулировать в настоящем исследовании, требует своей доработки и программный продукт. Однако сам факт обращения к столь масштабной проблематике и получения заслуживающих внимания теоретических и практических результатов ее хотя бы частичного разрешения достоин позитивной оценки научно-технической общественности, для которой далее предлагаются развернутые характеристики достижений настоящей работы.

Новизна полученных результатов просматривается в том, что:

- предложенный калькулятор риска обеспечивает комплексный подход к оценке ущербов и вероятностей их наступления, в отличие от аналогов учитывающий различные сущность нарушения качеств информации, частичную либо полную утрату работоспособности и особенности защищаемой системы;

- впервые автоматизировано сформирован банк знаний, в диалоговом режиме предлагающий пользователю регламенты реагирования на компьютерные инциденты и ликвидации их последствий для существующего многообразия кибератак и уязвимостей, используемых ими.

Практическая ценность достигнутых результатов состоит в том, что:

- построенный калькулятор рисков открывает перспективу формирования риск-ландшафтов защищаемых АИС и ТКС во всем многообразии известных векторов атак и уязвимостей при адекватном пользовании их показателей в отношении различных нарушений работоспособности и с учетом специфики атакуемого объекта;

- в широком множестве АИС и ТКС различного назначения (при соответствующей адаптации к специфике заданного объекта) созданный банк знаний позволит весьма оперативно выдавать регламенты для борьбы с конкретными вариантами кибервторжений, что в дальнейшем даст возможность незамедлительно организовать эффективную защиту объекта;

- примеры автоматизированной регламентации борьбы с кибервторжениями, приведенные в работе, могут быть с успехом использованы при противодействии кибератакам на корпоративные сети и веб-приложения.

Теоретическая значимость результатов работы представляется существенной в следующих аспекта:

- аналитика риск-анализа, реализованная в предложенном в работе калькуляторе, объективно имеет потенциал к совершенствованию и реально может быть развита, особенно в плане учета множества одновременно используемых уязвимостей и расширения учитываемых показателей защищаемой системы;

- в контексте современной практики применения искусственного интеллекта созданный банк знаний имеет перспективу своего теоретического развития в плане реализации машинного обучения и внедрения нейросетевых технологий для противодействия компьютерным атакам.

Список литературы

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

2. The Common Attack Pattern Enumeration and Classification (CAPEC). URL: https://capec.mitre.org/ (дата обращения 25.12.2023).

3. NIST Information Technology Laboratory National Vulnerability Database –

URL: https://nvd.nist.gov/vuln (дата обращения 25.12.2023)/

4. MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения 25.12.2023).

5. NIST Common Vulnerability Scoring System Calculator. URL: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (дата обращения 25.12.2023).

6. База данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat (дата обращения 25.12.2023).

7. Каталог известных эксплуатируемых уязвимостей (CISA KEV). URL: https://www.cisa.gov/known-vulnerabilities-catalog (дата обращения 25.12.2023).

8. Остапенко Г.А. Совершенствование организационно-правового обеспечения информационной безопасности предприятия: формирование риск-ландшафта сетевых атак / Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.Ю. Пекло // Информация и безопасность. 2023. Т. 26. Вып. 2. С. 203-210.

9. Пекло А.Ю. Атаки типа «сетевая разведка»: риск-ландшафт и частная политика информационной безопасности предприятия / А.Ю. Пекло, Г.А. Остапенко, Д.В. Щербакова, А.А. Остапенко // Информация и безопасность. 2023. Т. 26. Вып. 2. С. 235-246.

10. Хромых С.А. Сетевые атаки на уровне приложений: риск-ландшафт и частная политика информационной безопасности предприятия / С.А. Хромых, Г.А. Остапенко, Д.В. Щербакова, А.А. Остапенко // Информация и безопасность. 2023. Т. 26. Вып. 2. С. 261-276.

11. Остапенко Г.А. Организационно-правовая защита от сетевых атак: методики формирования частных политик, регламентов и инструкций обеспечения безопасности организации (часть I) / Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.С. Кривошеин // Информация и безопасность. 2023. Т. 26. Вып. 3. С. 329-340.

12. Остапенко Г.А. Организационно-правовая защита от сетевых атак: методики формирования частных политик, регламентов и инструкций обеспечения безопасности организации (часть II) / Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.Г. Краснобородкин // Информация и безопасность. 2023. Т. 26. Вып. 3. С. 329-340.

13. Остапенко Г.А. Организационно-правовая защита от сетевых атак: методики формирования частных политик, регламентов и инструкций обеспечения безопасности организации (часть III) / Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.Г. Краснобородкин // Информация и безопасность. 2023. Т. 26. Вып. 3. С. 341-358.

14. Остапенко А.Г. Проектная деятельность: научно-методическое развитие в направлении внедрения средств искусственного интеллекта для обеспечения организационно-правовой защиты корпоративных сетей / А.Г. Остапенко, Д.В. Щербакова, А.А. Остапенко, Д.А. Нархов // Информация и безопасность. 2023. Т. 26. Вып. 3. С. 447-454.

15. Остапенко Г.А. Нейросетевые задачи и компетенции проектной деятельности по созданию защищённых автоматизированных информационных систем / Г.А. Остапенко, А.П. Васильченко // Информация и безопасность. 2023. Т. 26. Вып. 4. С. 579-586.

16. Остапенко Г.А. Методики регламентации обеспечения информационной безопасности атакуемых автоматизированных систем / Г.А. Остапенко, А.П. Васильченко // Информация и безопасность. 2023. Т. 26. Вып.4. С. 597-602.

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

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 07.01.2024

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@uandex.ru

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

Нестеров Дмитрий Сергеевич – студент, Воронежский государственный технический университет, e-mail: NesterovWork@yandex.ru

Дубов Андрей Сергеевич – студент, Воронежский государственный технический университет, e-mail: whodatandrey@gmail.com

Старцев Валерий Александрович – студент, Воронежский государственный технический университет, e-mail: startsev@keeneye.pro

AUTOMATED KNOWLEDGE BANK AND CYBER ATTACK RISK AND VULNERABILITY CALCULATOR (PART I)

G.A. Ostapenko, A.P. Vasilchenko, A.A. Ostapenko, D.S. Nesterov, A.S. Dubov, V.A. Startsev

The article discusses the issues of increasing the security of attacked automated information and telecommunication systems through the development and application of methodological, algorithmic and software for automating risk analysis and regulating counteraction to cyber attacks. The scientific and technical problem of creating tools that integrate the space of data, techniques and measures to counter cyber attacks, including goal setting, risk analysis and the formation of knowledge about the regulation of combating computer incidents has been solved. A knowledge bank of cyber attacks and vulnerabilities has been formed in the form of aggregated regulations for various stages of countering intrusions, including ongoing response and liquidation of consequences in relation to registered incidents. The user can interactively receive practical recommendations from the bank on how to combat a variety of attack scenarios and gaps used by attackers.

Keywords: system, safety, risk, damage, probability, regulations, knowledge and data base.

Submitted 07.01.2024

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@uandex.ru

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

Dmitry S. Nesterov – student, Voronezh State Technical University, e-mail: NesterovWork@yandex.ru

Andrey S. Dubov – student, Voronezh State Technical University, e-mail: whodatandrey@gmail.com

Valery A. Startsev – student, Voronezh State Technical University, e-mail: startsev@keeneye.pro