DOI 10.36622/VSTU.2023.4.26.012
УДК 004.056.5

МЕТОДИКИ РЕГЛАМЕНТАЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АТАКУЕМЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Г.А. Остапенко, А.П. Васильченко

Рассматривается защита корпоративных информационных ресурсов и сетей от многообразия кибератак. Акцентируется внимание на методиках построения риск-ландшафта и частных регламентов (реагирования на несанкционированные вторжения, ликвидации их негативных последствий) обеспечения информационной безопасности защищаемых автоматизированных систем. В этом контексте предлагаются научно-методические решения для построения риск-ландшафта рассматриваемых разновидностей атак и вышеупомянутой регламентации в отношении сочетаний вектор атаки-уязвимость. Излагаются принципиальные моменты функционального и структурного согласования элементов создаваемых регламентов в плане их сквозной горизонтали, обеспечивающей взаимно однозначное соответствие злоумышленных действий и мер ликвидации их негативных последствий. Инструментарий противодействия целому классу кибератак определяется как совокупность сформированных частных регламентов.

Ключевые слова: защита, ресурсы, сети, системы, регламент, риск, атака, уязвимость.

Введение

Актуальность организационно-правовой защиты корпоративных информационных ресурсов и сетей не вызывает сомнений [1]. Однако регламентация этой деятельности на основе современных нормативных документов [2-4] требует углубленной конкретизации в части противодействия многообразию кибератак [2]. Речь идет, в первую очередь, о регламентах реагирования на несанкционированные внешние вторжения и ликвидации их негативных последствий [1]. Научно-методические рекомендации построения вышеуказанных документов должны обеспечивать основы эксплуатации и проектирования объектов защиты в контексте конкретики противодействия злоумышленным действиям атакующего субъекта. Отправным моментом в данном случае выступает сценарная последовательность деструктивных информационных систем. При этом, эффективность создаваемой системы защиты во многом будет зависеть от степени детализации формируемых регламентов и от взаимно однозначного соответствия, описываемых в них злоумышленных действий, мер ликвидации этих последствий. Именно этому посвящена настоящая работа, предлагающая научно-методические рекомендации построения регламентов организационно-правовой защиты информационных ресурсов и сетей корпоративного назначения.

Основные научно-методические рекомендации

Использование нормативных возможностей ресурса [1] CAPEC позволяет сформировать дерево проектной деятельности, изображенное на рис. 1, где исследователь от заданного вектора кибератаки (VA) имеет возможность перейти к рассмотрению используемых ею ошибок программного обеспечения (CWE) к соответствующим им уязвимостям (CVE) по стандарту NIST [2]. Такая формализация позволит обозреть все множество сочетаний вектор-уязвимостей исследуемого объекта и в результате построить его риск-ландшафт, обобщенно представленный на рис. 2, как результат расчета значений функции $Risk(VA, CVE)$ для соответствующих VA и CVE. Здесь [3] уместно воспользоваться возможностями калькулятор CVSS [5] в исчислении следующих метрик:

1) временная метрика (Temporal metrics), учитывающая реакцию производителя уязвимого продукта, зависящая от:

- возможности использования (Exploitability);
- уровня исправления (Remediation Level);
- доверия к отчету (Report confidence);

2) метрика воздействия (Impact Metrics), основанная на оценке воздействия на конфиденциальность, целостность и доступность атакованной информации;

3) метрика возможности использования (Exploitability Metrics), зависящая от:
- вектора класса атаки (Attack Vector);
- сложности атаки (Attack Complexity);
- необходимому для реализации уровню привилегий (Privileges Required);
- отсутствию или наличию взаимодействия с пользователем (User Interaction).

Вышеперечисленные метрики нельзя считать всеобъемлющими, однако они могут оказаться неплохим подспорьем для нахождения значений ущерба V и вероятности его наступления $P(V)$, определяющих величину рассчитываемого риска произведением

$$V * P(V) = Risk(V).$$

Видимо, здесь придется оперировать вероятностями совместных событий, а именно вероятностью реализации атаки P_{VA} и вероятностью использования уязвимости P_{CVE}, которые, как и ущерб, могут быть исчислены с помощью калькулятора. Отсюда риск будет равен

$$Risk(V) = [P_{AB} * P_{CVE}] * V$$

и его значения удастся отразить в ландшафте (рис. 2).

Предложенный формат позволит формировать проектную деятельность обеспечения кибербезопасности и открывает возможности аналитики по:
- выявлению наиболее опасных векторов атак и используемых ими уязвимостей;
- регулирование рисков реализации сочетаний вектор-уязвимость в конкретных проектных ситуациях;
- разработке регламентов борьбы с каждым таким сочетанием в виде таблицы с соответствующими графами (последовательность злоумышленных действий, меры реагирования на злоумышленные действия атакующего субъекта, последствия злоумышленных действий, меры ликвидации последствий злоумышленных действий), составление которой проиллюстрировано на рис. 3.

Рис. 1. Дерево проектной деятельности

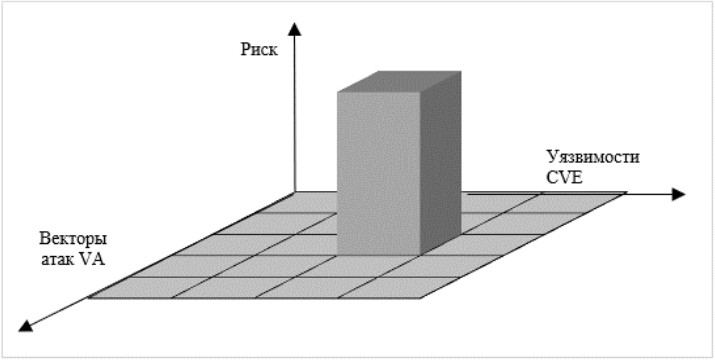

Рис. 2. Риск-ландшафт проектной деятельности

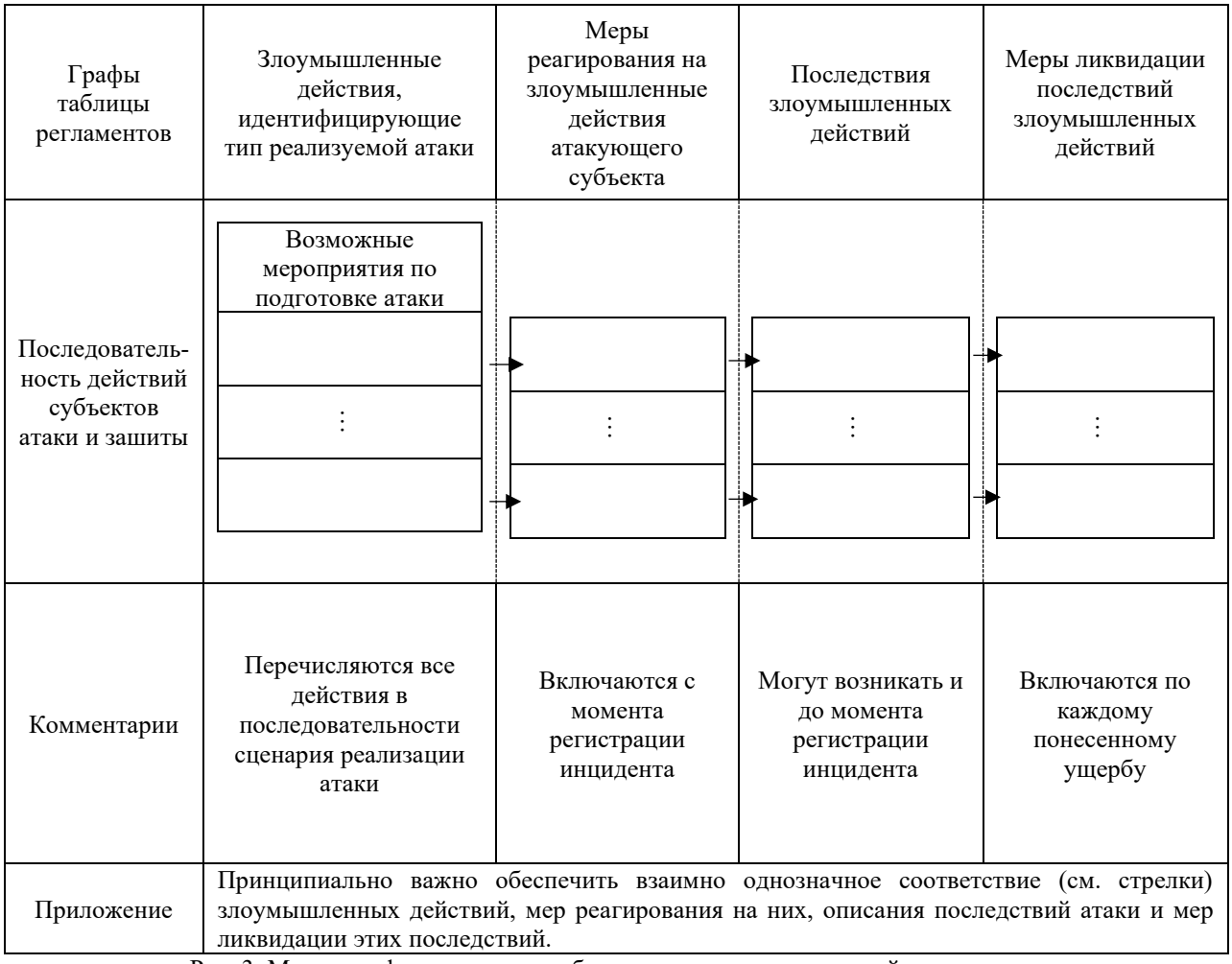

Рис. 3. Методика формирования таблиц регламентов противодействия атакам

Представленная на рис. 3 методика базируется на принципиальных моментах следующего содержания:

- всякая атака имеет свой сценарий, представляющий собой последовательность деструктивных (по отношению к атакуемому объекту) операций злоумышленника, которые защищающаяся сторона обязана отслеживать. Зачастую саму атаку предваряют некоторые подготовительные мероприятия субъекта атаки, которые обнаружить зачастую не представляется возможным;

- с момента регистрации и классификации атаки защитники объекта должны поступательно (в строгом с соответствующими действиями по сценарию злоумышленника) внедрять меры противодействия атаке. При этом к радикальным средствам (отключение от сети Интернет и т. п.) следует прибегать лишь в исключительных случаях, ибо тогда полностью нарушается работа корпоративной сети. Кроме того, частое использование банальных мер (фильтрация и т. п.) по поводу и, тем более, без повода свидетельствует о невысокой квалификации проектировщика, снижающей эффективность сетевого противоборства, которая будет на необходимом уровне только в случае глубокого понимания сущности операций злоумышленника и адекватного на них реагирования по каждой позиции сценария атаки;

- в свою очередь описание ожидаемых негативных последствий (ущербов) атаки также должно быть осуществлено по каждому действию злоумышленника. При этом, здесь следует отразить не какие-либо процессы, а проанализировать результаты атаки в виде наносимых объекту ущербов;

- не следует путать меры противодействия злоумышленным действиям и меры ликвидации их последствий. Первые используются по ходу реализации атаки для каждой позиции сценария атаки, а вторые

внедряются в отношении всякого понесенного ущерба. Эффективность защиты будет существенно повышена, если наряду с ликвидацией последствий злоумышленных действий проектировщик сможет предложить меры, исключающие возможность или хотя бы снижающие вероятность успеха подобных атак в будущем;

- важнейшим условием настоящей регламентации следует считать сквозную горизонталь (рис. 3), обеспечивающую взаимно однозначное соответствие злоумышленных действий, мер реагирования на них, последствий злоумышленных действий и мер ликвидации их негативных последствий. Только при выполнении этого условия может быть построена структурно и функционально сбалансированная система защиты, обладающая необходимой эффективностью противодействия разноплановым кибератакам;

- наконец, предложенные регламенты, табулированные в таблице (рис. 3), должны быть составлены для каждого сочетания вектор-уязвимость рассматриваемого класса (вида) кибератак. При этом, не следует путать ошибку программного обеспечения объекта (CWE) с используемой уязвимостью, которая именно нужна для регламентации, и которая лежит в основе определения величин ущерба и вероятностей их наступления (CVSS);

- совокупность частных регламентов для всевозможных сочетаний вектор-уязвимость сформирует инструментарий противодействия целом классу кибератак.

Особенности привлечения средств искусственного интеллекта к обеспечению кибербезопасности защищаемых автоматизированных систем

Объективной реальность сегодня является стремление к автоматизации интеллектуальной деятельности. В том числе это необходимо при проектировании и/или эксплуатации средств обеспечения информационной безопасности. В нашем случае к этому побуждает высокая размерность множества атак, уязвимостей и регламентов, оперативно обозреть которые и установить причинно-следственные связи между их элементами уже не представляется вручную возможным [1]. В этом контексте на рис. 4 предлагается обобщенная структурно-функциональная схема нейросетевой реализации организационно-правовой защиты атакуемых информационных систем и сетей.

Первичной в этой схеме является стадия регистрации инцидентов, где предусмотрены выявление аномалий в работе системы с признаками вторжений, а также – идентификация выявленного инцидента в сущностях атак и уязвимостей, многообразие которых отражено [2-4] в соответствующих базах данных и знаний (векторов и сценариев, тактик и техник, ошибок и уязвимостей ПО). В данном случае «опыт – сын ошибок трудных» при обеспечении кибербезопасности, аккумулированный на открытых платформах незаменим в практической деятельности специалиста по защите информации и является актуальным подспорьем в ходе информационного противоборства, в том числе и с использованием искусственных нейросетей.

Вторая стадия предусматривает [1] реагирование на идентифицированный инцидент безопасности. Здесь актуальны поиск адекватных частных регламентов и оперативное исполнение отобранного варианта противодействия в порядке ответных действий на операции, реализуемые злоумышленником. Основой в этом реагировании выступают базы данных и знаний частных регламентов, созданные администрацией защищаемой системы для многообразия сочетаний вектор атаки – уязвимость [1].

Третья стадия ориентирована [1] на ликвидацию последствий атаки и коррекцию политики, регламентов и инструкций обеспечения информационной безопасности системы. Прежде всего речь идет о поиске регламентов, адекватного нанесенному атакой ущербу, и приведение (по этому регламенту) системы в состояние штатной работы. При этом важным вопросом выступает анализ негативных последствий инцидента для последующего укрепления защиты системы на основе модернизации ее политики, регламентов и инструкций, несовершенство которых было выявлено в ходе информационного противоборства.

Все вышеперечисленные стадии входят в зону подготовки запросов и их пополнения с помощью нейросети. В свою очередь вышеперечисленные базы данных и знаний образуют зону машинного обучения.

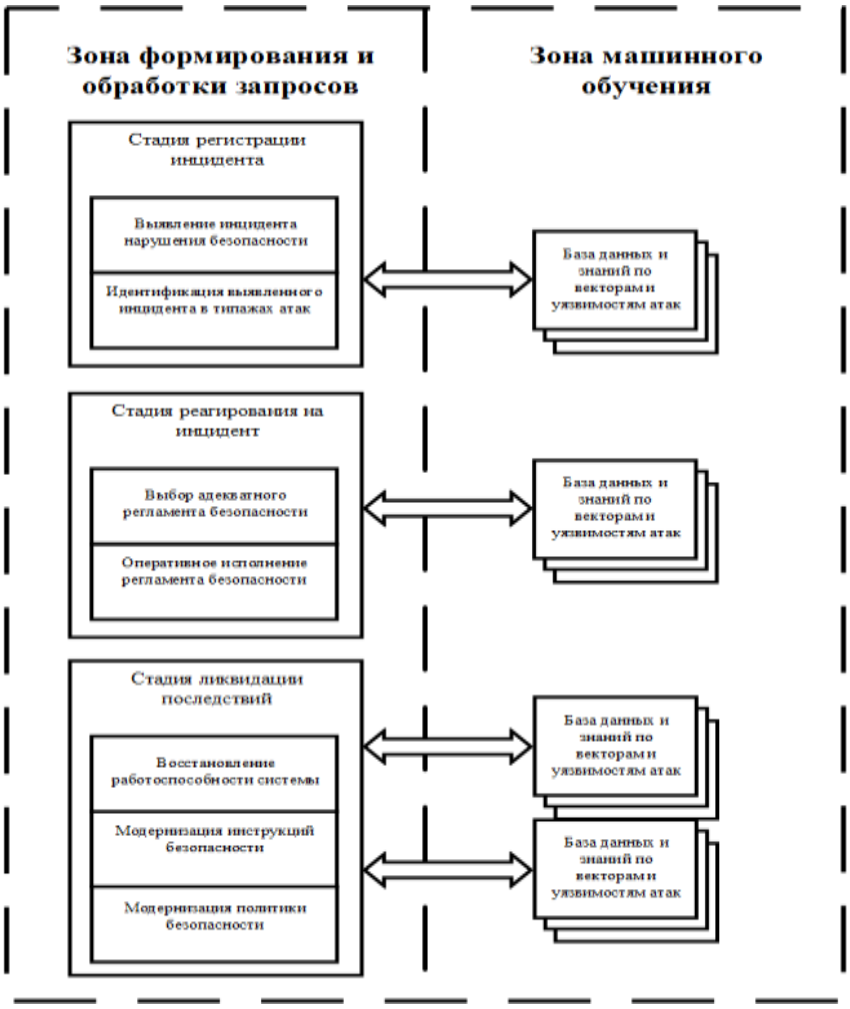

Рис. 4. Обобщенная структурно-функциональная схема нейросетевой реализации защиты атакуемой автоматизированной системы

Заключение

Фактически, в работе предлагаются некоторые шаблоны для построения регламентов реагирования на злоумышленные действия атакующего субъекта и ликвидации последствий этих действий. При этом обсуждаются принципиальные моменты такого построения в контексте обеспечения сквозного взаимно однозначного соответствия реализации злоумышленником операций, мер реагирования на них, описания негативных последствий. Схемы такой формализации, представленные в работе, открывают новые возможности учета специфики рассматриваемых атак, функционального и структурного согласования элементов системы защиты от них. Руководствуясь предлагаемым формализмом лица, принимающие решения ЛПР при эксплуатации и проектировании защищенных автоматизированных систем, способны существенно повысить степень обеспечения информационной безопасности объекта защиты.

В качестве перспективы развития результатов настоящей работы уместно отметить необходимость автоматизации выработки интеллектуальных подсказок ЛПР и поиск во множестве предлагаемых частных регламентов рациональных (в момент регистрации инцидента) технических

решений защиты от реализуемой злоумышленником кибератаки. Здесь предлагается целесообразным использование искусственных нейросетей, эффективно применяемых ныне в сфере обеспечения информационной безопасности.

Список литературы

1. Организационно-правовая защита сетей / Г. А. Остапенко, Д. В. Щербакова, А. О. Калашников и др.; Под ред. Акад. РАН Д. А. Новикова. Сер. Теория сетевых воин. Вып. 8. М.: Горячая линия – Телеком, 2023. 226 с.

2. The Common Attack Pattern Enumeration and Classification (CAPEC). URL: https://capec.mitre.org/ (дата обращения: 5.11.2023).

3. NIST Information Technology Laboratory National Vulnerability Database – URL: https://nvd.nist.gov/vuln (дата обращения: 5.11.2023).

4. MITRE ATT&CK– URL: https://attack.mitre.org/matrices/enterprise/ ((дата обращения: 5.11.2023).)

5. NIST Common Vulnerability Scoring System Calculator. URL: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (дата обращения: 5.11.2023).

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

Поступила в редакцию 07.11.2023

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, профессор, проректор по цифровизации Финансового университета при Правительстве Российской Федерации, e-mail: ostg@mail.ru.

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

METHODS FOR REGULATING INFORMATION SECURITY OF ATTACKED AUTOMATED SYSTEMS

G.A. Ostapenko, A.P. Vasilchenko

The protection of corporate information resources and networks from a variety of cyber attacks is considered. Attention is focused on methods for constructing a risk landscape and private regulations (responding to unauthorized intrusions, eliminating their negative consequences) to ensure the information security of protected automated systems. In this context, scientific and methodological solutions are proposed for constructing a risk landscape for the types of attacks under consideration and the above-mentioned regulation regarding attack vector-vulnerability combinations. The fundamental points of functional and structural coordination of the elements of the created regulations are outlined in terms of their end-to-end horizontal, ensuring a one-to-one correspondence between malicious actions and measures to eliminate their negative consequences. The tools for countering a whole class of cyber attacks are defined as a set of developed private regulations.

Keywords: protection, resources, networks, systems, regulations, risk, attack, vulnerability.

Submitted 07.11.2023

Information about the authors

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

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