DOI 10.36622/VSTU.2023.26.2.005
УДК 004.056

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

В работе рассматриваются особенности формирования риск-ландшафта как основа совершенствования организационно-правового обеспечения безопасности корпоративных сетей. В этой связи осуществлено соответствующее целеполагание и намечены основные направления исследования. Применительно к риск-анализу реализована матричная формализация отношений векторов атак и используемых ими уязвимостей для заданного вида сетевого воздействия на защищаемый объект. В результате предлагается риск-ландшафт, позволяющий выявить наиболее опасные сочетания вектор-уязвимость, для противодействия которым необходимо формировать соответствующее организационно-правовое обеспечение в виде частных политик безопасности, регламентов и инструкции по защите информации корпоративной сети от сетевых атак. Предложены аналитические выражения для оценки риска успешной реализации векторов атак через сетевые уязвимости.

Ключевые слова: корпоративная сеть, вектор атак, уязвимость, политика, регламент, инструкция.

Введение

Первоначально уместно определиться [1– 10] с основными терминами.

Кибератака – это любой наступательный маневр, направленный на компьютерные информационные системы, компьютерные сети, инфраструктуру или персональные компьютерные устройства.

Злоумышленник – это лицо или процесс, который пытается получить доступ к данным, функциям или другим ограниченным областям системы без авторизации, потенциально со злым умыслом.

Вектор атаки – последовательность действий или средство для получения неавторизированного доступа к защищаемой информационной системе.

Уязвимость – недостаток системы, используя который, можно намеренно нарушить её целостность и вызвать неправильную работу.

Компонент – составной элемент системы.

Политика информационной безопасности (организации) – формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

Частная политика информационной безопасности (организации) – документ, определяющий правила, требования и принципы, используемые применительно к отдельным областям информационной безопасности, видам и технологиям деятельности организации

Регламент информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

Инструкция информационной безопасности – это документ, который описывает конкретные шаги и последовательность действий при выполнении различных задач в рамках защиты информации.

На основании вышеупомянутого глоссария уместно реализовать следующее целеполагание.

Целеполагание исследования

Объект исследования: корпоративные вычислительные сети, подвергающиеся сетевым атакам различных типов.

Предметом исследования являются не программно-технические и иные решения, а именно нормативно-правовые предложения, оригинальные и ориентированные на защиту исключительно от заданного класса атак на корпоративные сети.

Цель исследования состоит в повышении защищенности корпоративных сетей за счёт создания (посредством риск-анализа) комплекса мер и средств организационно-правового направления, обеспечивающих снижение рисков успешности атак рассматриваемого типа.

С учетом осуществленного целеполагания представляется возможной формулировка следующих трех направлений исследования.

Принципиальным вопросом является сбор данных и знаний. За этим следует анализ материала для изучения причинно-следственных связей по следующим аспектам деструктивного воздействия и противодействия: объекты и сценарии атак, используемые уязвимости, средства и меры защиты, особенно на организационно-правовом уровне. Интернет статистика позволит здесь на основе риск-анализа выявить наиболее опасные сочетания вышеперечисленных аспектов, акцентировав внимание на них дальнейших исследованиях.

Необходимое и достаточное информационное обеспечение, полученное на первом этапе исследования, позволит отыскать взаимно однозначное соответствие между проанализированными аспектами заданного типа атак и брешами в организационно-правовых режимах традиционной конфигурации, сохраняющих популярность рассматриваемого класса атак в деструктивном воздействии на корпоративные сети. Выявленные в этом случае противоречия между динамично развивающимся арсеналом изучаемых атак и сложившейся в корпорациях нормативно-правовой защитой своих сетей обусловят направления её развития, прежде всего, в контексте противодействия именно этим атакам.

Венцом исследования станут, ориентированные исключительно на объект и предмет конкретной работы, предлагаемые организационно-правовые нормы для установления необходимого и достаточного режима в части формирования политик безопасности, регламентов защиты и инструкций пользования корпоративной сети, обеспечивающих для неё значительное снижение рисков успешности рассматриваемого класса атак. Разумеется, предложенное решение потребует обоснования его эффективности и интеграции с аналогичными результатами по другим типам атак.

Формализация риск-анализа

Пусть защищаемая система (сеть) состоит из множества её технологических компонент:

$$S = \{TC_1, \dots TC_k \dots TC_N\}, \qquad (1)$$

где TC_i – i-я технологическая компонента сети, $i = \overline{1, N}$,

N – количество компонент.

Такой подход существенно облегчает анализ систем, особенно сложных. В этом случае декомпозиция на технологические компоненты (далее – ТК) позволяет глубже вникнуть в существо процессов реализации атак и защиты.

В свою очередь, класс атак, реализуемых в отношении защищаемой системы, также может быть разложен на векторы (сценарии) атак:

$$\mathrm{A} = \{VA_1, \dots VA_i \dots VA_n\}, \qquad (2)$$

где VA_i – i-й сценарий атаки.

n – количество сценариев.

Аналогично для уязвимостей, используемых злоумышленниками, можно записать следующую последовательность:

$$V = \{VB_1, \dots VB_j \dots VB_m\}. \qquad (3)$$

где VB_i – i-я уязвимость сети.

m – количество уязвимостей.

Представленные выражения (1) – (3) открывают перспективу для формализации описания процесса информационного

противоборства, где, прежде всего, необходимо установить соответствие между элементами множеств A и V. Это представляется сделать с помощью матрицы смежности (рис. 1), которую можно транспонировать (на основе статистических данных реализуемых атак и используемых ими уязвимостей) в матрицу рисков (рис. 2). Отсюда для каждого отдельно взятого технологического компонента системы можно построить ландшафт опасности реализации в отношении него кибератак (рис. 3). В дальнейшем появляется возможность сконцентрировать внимание на наиболее опасных сочетаниях вектор атаки - уязвимость.

	VA_1	...	VA_i	...	VA_n
VB_1		...		...	
...	...	...	...	...	...
VB_j		...	1	...	
...	...	...	...	...	...
VB_m		...		...	

Рис. 1. Матрица смежности векторов атак и уязвимостей

	VA_1	...	VA_i	...	VA_n
VB_1		...		...	
...	...	...	...	...	...
VB_j		...	$Risk_{ij}$	...	
...	...	...	...	...	...
VB_m		...		...	

Рис. 2. Матрица рисков реализации атак через уязвимости

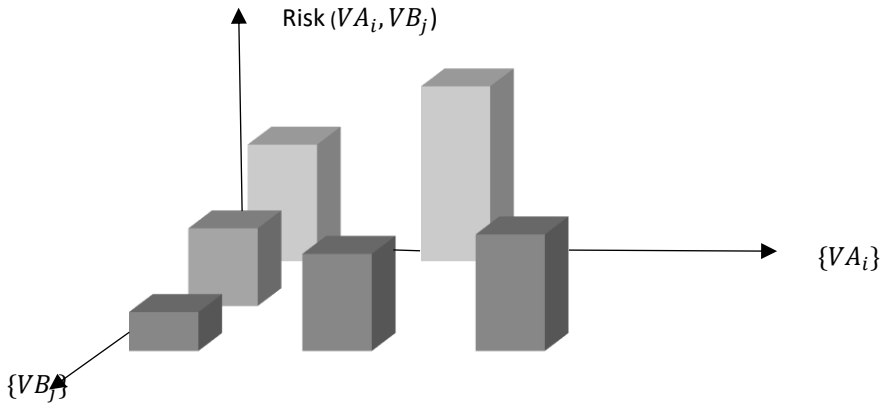

Рис. 3. Risk-ландшафт реализации кибератак на технологический компонент защищаемой системы

Способы оценки рисков могут быть различными: от статистических до экспертных. Однако величина риска всегда связана с ожидаемым ущербом. К примеру, для беспроводных сетей, компонентами которых выступают приемно-передающие устройства и канал связи, ущерб зачастую связан с утраченными (под воздействием угроз) цифровыми отсчетами и блоками информации (нарушение её целостности и доступности). С другой стороны, для этого нужно осуществлять оценки в единицу времени.

Применительно к кибератакам следует собрать (на соответствующих сайтах) данные о их частоте к ущербности (усреднено на единичную атаку рассматриваемого сценария). В результате можно рассчитывать риск для отдельно взятой компоненты системы.

Что же касается интегральной (для компонент в сумме) оценки рисков, то она должна учитывать значимости каждого из компонентов в системе, способы которой достаточно известны. Разумеется, регулирование рисков также обязано учитывать вышеупомянутую значимость.

Методическое обеспечение для построения риск-ландшафта

В методическом плане риск-оценка сетевой атаки типа S может быть осуществлен на основе следующего подхода.

Введем следующие обозначения:

VA_{si} - i-ый вектор сетевой атаки типа S;

VB_{sj} - j-ыя уязвимость, используема для реализации сетевой атаки типа S;

$Risk_{sij}$ - риск реализации атаки типа S посредством i-го вектора на j-ую уязвимость;

F_{sij} - частота успешного использования j-ой уязвимости при реализации атаки типа S посредством i-го вектора;

K_{sij} - уровень критичности уязвимости;

Δt_{si} - среднестатистическое значение простоя атакуемой сети в результате успеха атаки типа S посредством i-го вектора.

С учетом введенных обозначений вероятность реализации атаки типа S посредством i-го вектора на j-ую уязвимость может быть оценена выражением:

$$P_{sij} = \frac{F_{sij}}{\sum_j F_{sij}}. \quad (4)$$

В свою очередь, ущерб может быть оценен следующим образом:

$$U_{sij} = \frac{K_{sij}}{\sum_j K_{sij}} \times (\Delta t_{si}). \quad (5)$$

Тогда риск будет равен:

$$Risk_{sij} = P_{sij} \times U_{sij}\,. \quad (6)$$

Данные по F_{sij} и Δt_{si} предлагают источники [8, 9] При этом K_{sij} рассчитать достаточно затруднительно, так как основополагающими данными для его расчета являются сведения о составе и архитектуре информационных ресурсов организации, полученные по результатам их инвентаризации [10]. Поэтому подход (4) – (6) уместно несколько трансформировать. Здесь можно учесть тот факт, что успехи

атак через различные уязвимости обычно являются вероятностно несовместимыми событиями. Если принять подобное предположение за основу, то искомая вероятность будет равна:

$$P_{sij} = \sum_j F_{sij} \ , \qquad (7)$$

то есть сумме всех частот использования уязвимостей, соответствующих заданному типу атак S и рассматриваемому его вектору i.

В свою очередь, коэффициент, учитывающий долю j-ой уязвимости, можно также трансформировать:

$$U_{sij} = \frac{F_{sij}}{\sum_j F_{sij}} \times (\Delta t_{si}) \ . \qquad (8)$$

Заменив K_{sij} на F_{sij}. Тогда из (7) и (8) выражение риска примет следующий вид:

$$Risk_{sij} = (\sum_j F_{sij}) \times \frac{F_{sij}}{\sum_j F_{sij}} \times \times (\Delta t_{si}) = F_{sij} \times (\Delta t_{si}) \ . \qquad (9)$$

Разделив выражение (9) на максимальное значение Δt_{si} можно получить нормированный риск:

$$\overline{Risk_{sij}} = F_{sij} \times \frac{(\Delta t_{si})}{\max[\Delta t]} = = F_{sij} \times \overline{U_{sij}}. \qquad (10)$$

В результате (10) получается сопоставимые (по величинам риска) друг с другом ландшафты по типам и векторам рассматриваемых атак.

Далее следует действовать по схеме, представленной на рис. 4, где фактически требуется установить соответствие принимаемых защитных мер с действиями злоумышленников.

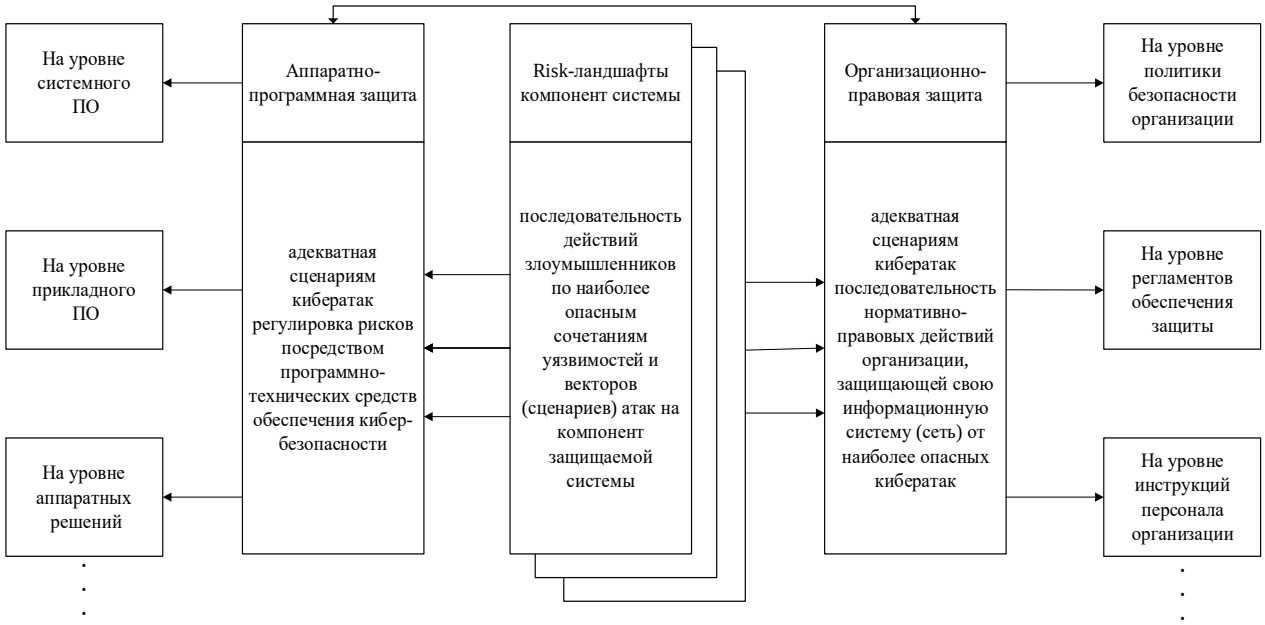

Рис. 4. Схема генерации практических решений по снижению рисков успешности кибератак на компоненты защищаемой информационной системы организации

Заключение

Перспективным направлением настоящего исследования является использование выявленной специфики формирования риск-ландшафта для развития организационно-правового обеспечения предприятия по противодействию сетевым атакам.

На основании приведенной ниже методики представляется возможным разработать частные политики, а также вытекающие из нее регламенты и инструкции сетевой безопасности предприятия, которые значительно могут снизить риски успешности рассматриваемого класса атак.

Структуру частной политики, регламентов и инструкций необходимо построить таким образом, чтобы в ней была выделена инвариантная часть, относящаяся ко всем возможным атакам на сеть и ресурсы предприятия, а также обозначены окна, учитывающие специфику защиты от заданного типа сетевых атак.

Примеры построения структуры частной политики, регламентов и инструкций представлены на рис. 5-7.

Инвариантная часть частной политики сетевой безопасности предприятия

Окна, учитывающие противодействие сетевым атакам заданного типа, включая меры защиты:

- от рассматриваемых векторов атаки;
- уязвимостей сети предприятия, используемых вышеупомянутыми векторами.

Рис. 5. Структура частной политики сетевой безопасности предприятия с учетом необходимости противодействия заданному типу атак

Инвариантная часть регламентов сетевой безопасности предприятия

Окна, определяющие порядок действия при борьбе с инцидентами безопасности, которые могут возникнуть в ходе реализации сетевых атак заданного типа на предприятии, включая в себя:

- обнаружение инцидентов безопасности;
- реагирование на инциденты безопасности;
- ликвидация последствий инцидентов безопасности.

Рис. 6. Структура регламентов сетевой безопасности предприятия с учетом действий, направленных на борьбу с инцидентами

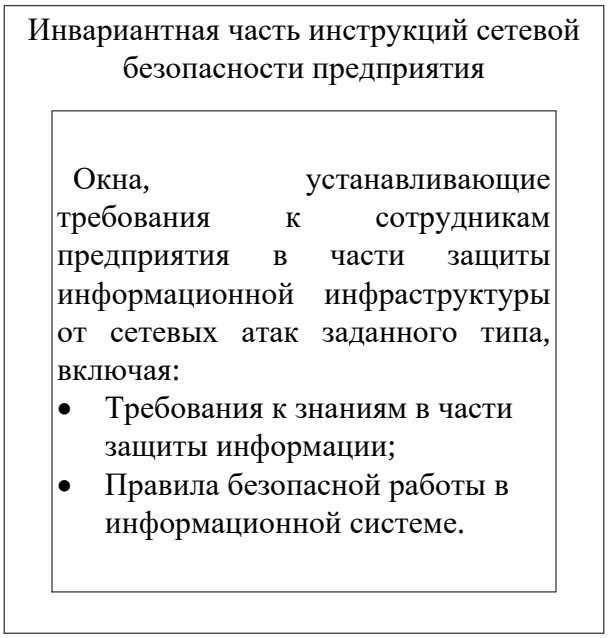

Рис. 7. Структура инструкции сетевой безопасности пользователей предприятия

Представленные примеры (рис. 5-6) наглядно демонстрируют способы совершенствования организационно-правового обеспечения [9] сетевой безопасности информационных ресурсов предприятия, которые могут быть практически полезны специалистам в области кибер-защиты.

Список литературы

1. Эпидемии в телекоммуникационных сетях / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Серия «Теория сетевых войн»; вып. 1).

2. Атакуемые взвешенные сети / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Серия «Теория сетевых войн»; вып. 2).

3. Социальные сети и деструктивный контент / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Серия «Теория сетевых войн»; вып. 3).

4. Социальные сети и риск-мониторинг / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2019. – 284 с. (Серия «Теория сетевых войн»; вып. 4).

5. Социальные сети и психологическая безопасность / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2020. – 284 с. (Серия «Теория сетевых войн»; вып. 5).

5. Сетео-информационная эпидемиология / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2021. – 284 с. (Серия «Теория сетевых войн»; вып. 6).

6. Картография защищаемого киберпространства / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2022. – 372 с. (Серия «Теория сетевых войн»; вып. 7).

7. Банк данных угроз безопасности информации URL: https://bdu.fstec.ru/threat (дата обращения 23.04.2023).

8. UNSW_NB15 URL: https://www.kaggle.com/datasets/ (дата обращения 23.04.2023).

9. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств (утв. Федеральной службой по техническому и экспортному контролю 28 октября 2022 г.).

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 12.05.23

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, проректор Финансового университета при Правительстве Российской Федерации, e-mail: alexanderostapenkoias@gmail.com

Щербакова Дарья Владимировна – соискатель, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Мирошниченко Татьяна Юрьевна – студентка, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

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

Пекло Арина Юрьевна – студентка, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

IMPROVING THE ORGANIZATIONAL AND LEGAL SUPPORT OF THE INFORMATION SECURITY OF THE ENTERPRISE: FORMING THE RISK LANDSCAPE OF NETWORK ATTACKS

G.A. Ostapenko, D.V. Shcherbakova, T.Yu. Miroshnichenko, A.A. Ostapenko, A.Yu. Peklo

The paper discusses the features of risk landscape formation as a basis for improving the organizational and legal security of corporate networks. In this regard, the appropriate goal-setting has been carried out and the main directions of research have been outlined. With regard to risk analysis, a matrix formalization of the ratios of attack vectors and the vulnerabilities used by them for a given type of network impact on the protected object is implemented. As a result, a risk landscape is proposed that makes it possible to identify the most dangerous vector-vulnerability combinations, to counter which it is necessary to form appropriate organizational and legal support in the form of private security policies, regulations and instructions for protecting corporate network information from network attacks. Analytical expressions are proposed to assess the risk of successful implementation of attack vectors through network vulnerabilities.

Keywords: corporate network, attack vector, vulnerability, policy, regulation, instruction.

Submitted 12.05.23

Information about the authors

Grigory A. Ostapenko – Dr. Sc. (Technical), Vice-Rector of the Financial University under the Government of the Russian Federation, e-mail: alexanderostapenkoias@gmail.com

Daria V. Shcherbakova - applicant, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Tatyana Yu. Miroshnichenko – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

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

Arina Yu. Peklo – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com