DOI 10.36622/1682-7813.2024.27.1.003
УДК 004.056.57

СЕТЕВЫЕ АТАКИ КОМПЬЮТЕРНЫМИ ВИРУСАМИ: РИСК-ЛАНДШАФТ

О.Е. Кобцев, А.И. Шеншин, В.М. Питолин,
Л.В. Паринова, В.Г. Юрасов, Д.С. Печкин

Данная научная статья посвящена исследованию сетевых атак, осуществляемых компьютерными вирусами на корпоративные сети, в частности – комплексному риск-анализу соответствующих сценариев атак. В ходе исследования были проанализированы различные сценарии атак и уязвимости, используемые для их реализации. Особое внимание уделено статистической оценке частоты и ущербности таких атак. На основе полученных результатов был построен риск-ландшафт, а также выявлены наиболее опасные сочетания сценариев (векторов) атак и уязвимостей. Полученный результат может служить основой для дальнейшей разработки как организационно-правовых, так и технических мер по защите корпоративных сетей от сетевых атак компьютерными вирусами.

Ключевые слова: корпоративная сеть, компьютерные вирусы, уязвимости, ущерб, риск-ландшафт.

Введение

Современные информационные технологии играют важную роль в бизнесе и обществе в целом, обеспечивая беспрецедентные возможности для обмена информацией и повышения производительности. Однако, вместе с возросшей зависимостью от сетевых ресурсов и передовых технологий, возникают и новые угрозы для информационной безопасности организаций. Особую тревогу вызывают сетевые атаки, осуществляемые с использованием компьютерных вирусов, которые могут нанести значительный ущерб корпоративным сетям [1].

Актуальность данной темы обусловлена растущим объемом и сложностью компьютерных вирусов и сетевых атак, которые представляют серьезную угрозу для информационной безопасности предприятий. В современном информационном обществе, где цифровые технологии играют ключевую роль в бизнес-процессах, недостаточная защищенность корпоративных сетей может привести к серьезным последствиям, включая утечку конфиденциальных данных, прерывание операций и потерю репутации.

В результате проведенного исследования, основанного на отчете Positive Technologies за 2022 год, в 70% компаний была выявлена высокая активность вредоносного программного обеспечения (ВПО) в корпоративных сетях [2]. В связи с этим, исследование атак компьютерными вирусами и построение соответствующего риск-ландшафта являются неотъемлемой частью стратегии информационной безопасности, требующей глубокого анализа и применения передовых подходов.

Результаты исследований в данной области имеют высокий потенциал теоретической и практической значимости в контексте повышения безопасности информационных систем организаций за счёт регулирования рисков сетевых атак компьютерными вирусами [3].

Поэтому настоящая работа посвящена исследованию сетевых атак компьютерными вирусами на корпоративные сети и предлагает методику риск-оценки, включающую построение детализированного риск-ландшафта вирусных атак, позволяющего оценить характеристики отдельных векторов атак, а также выявить наиболее опасные сочетания вида “вектор-уязвимость”.

Риск-ландшафт уязвимостей и векторов атак компьютерными вирусами

Различные источники предоставляют разнообразные классификации векторов атак компьютерными вирусами. При этом в целях обеспечения высокой актуальности и достоверности результатов риск-анализа, целесообразно уделить особое внимание

выбору достоверных и общепризнанных источников. В данном контексте, основываясь на открытой информации с ресурса capec.mitre.org [4], выделим пять уникальных сценариев атак, представленных в табл. 1.

Таблица 1

Векторы атак на приложения [4]

Атака	Векторы атаки	Описание
Атака с помощью стелс-вирусов (VA_1)	Проникновение в систему через сетевой периметр	Использование стелс-вируса для обхода сетевых механизмов безопасности и проникновения в корпоративную сеть через уязвимости в сетевом периметре.
	Обход механизмов обнаружения и защиты	Обход механизмов обнаружения, таких как антивирусные программы, межсетевые экраны и системы обнаружения вторжений.
	Получение повышенных привилегий	Нацеленность на получение повышенных привилегий для обхода ограничений безопасности.
	Развитие атаки на целевые системы и реализация недопустимых событий	Продолжение развития атаки на целевые системы с использованием внутренних механизмов распространения и инфицирования.
	Получение доступа к ключевым системам	Использование стелс-вируса для получения доступа к ключевым системам в корпоративной сети.
	Установка задней двери	Установка задней двери для получения удаленного доступа и контроля над зараженной машиной или корпоративной сетью.
Атака с использованием макровирусов (VA_2)	Введение вредоносных макросов	Внедрение вредоносных макросов в документы и использование макроязыка для запуска вредоносного кода.
	Использование социальной инженерии	Использование социальной инженерии для убеждения пользователей в активации макросов и запуске вредоносного кода.
	Распространение через документы и сеть	Распространение макровирусов через зараженные документы, электронную почту, файлообменные сервисы и внутренние сетевые ресурсы.
	Маскировка и обход защитных механизмов	Маскировка макровирусов под легитимные макросы и обход антивирусных программ и других защитных механизмов.
	Запуск вредоносного кода	Запуск вредоносного кода при активации макросов, внедренных в макровирусе.
	Использование обновлений и патчей	Поиск уязвимостей в системах, приложениях и операционных системах для эксплуатации через макровирусы.
Атака с помощью сетевого червя (VA_3)	Идентификация уязвимых хостов	Поиск хостов в корпоративной сети с известными уязвимостями и слабыми местами в безопасности с использованием сканеров уязвимостей или автоматизированных инструментов.

Продолжение табл. 1

Атака	Векторы атаки	Описание
	Эксплуатация уязвимостей	Использование уязвимостей в операционных системах, службах или приложениях на целевых хостах для получения несанкционированного доступа.
	Заражение хостов	Размещение червя на зараженных хостах и использование различных методов для распространения, включая слабые пароли, вредоносные вложения в электронных письмах или сетевые уязвимости.
	Автоматическое распространение	Автоматическое исследование сети червем, обнаружение других уязвимых хостов и попытка распространения без взаимодействия пользователя.
	Загрузка дополнительных компонентов	Загрузка дополнительных вредоносных компонентов на зараженные хосты для дальнейшей эксплуатации или вредоносных действий.
	Создание задней двери	Создание задней двери на зараженных хостах для получения удаленного доступа и управления системами в дальнейшем.
Атака вирус-ботнетом (VA_4)	Заражение устройств	Распространение вируса-ботнета через вредоносные вложения в электронных письмах, зараженные ссылки, загрузки или эксплуатацию уязвимостей.
	Маскировка и уклонение от обнаружения	Использование различных методов для маскировки активности и уклонения от обнаружения, включая шифрование команд и данных, изменение сетевого трафика.
	Распространение	Распространение вируса-ботнета на другие устройства внутри или вне корпоративной сети, используя эксплуатацию уязвимостей, сканирование сети и другие методы.
	Установка контрольного узла	Установка контрольного узла вирусом-ботнетом, который служит злоумышленнику для удаленного управления зараженными устройствами.
	Формирование ботнета	Превращение зараженных устройств в "боты", которые подчиняются командам и контролю злоумышленника.
	Команды и управление	Отправка команд ботнету через контрольный узел для выполнения различных задач, таких как DDoS-атаки, спам, кража данных и другие вредоносные действия.
Атака вирусом с функцией рекламного ПО (VA_5)	Внедрение вредоносного кода в рекламные баннеры	Внедрение вредоносного кода в рекламные баннеры на веб-сайтах в корпоративной сети. При загрузке баннера пользователь может быть заражен вредоносным кодом.

Окончание табл. 1

Атака	Векторы атаки	Описание
	Распространение через вредоносные рекламные элементы	Использование вредоносных рекламных баннеров или всплывающих окон для распространения вируса с функцией рекламного ПО.
	Использование эксплойтов и уязвимостей	Использование известных эксплойтов и уязвимостей в программном обеспечении, используемом в корпоративной сети, для внедрения вируса с функцией рекламного ПО.
	Маскировка под легитимное рекламное ПО	Маскировка вируса с функцией рекламного ПО под легитимное рекламное ПО или расширение браузера для избежания обнаружения.
	Нежелательное отображение рекламы	Навязчивое отображение рекламных материалов на компьютере пользователя в корпоративной сети.
	Кража данных	Сбор и передача конфиденциальной информации о пользователях, такой как персональные данные, приватные файлы или учетные данные.

В данном исследовании рассматриваются уязвимости и векторы атак, представленные в табл. 1 и 2. При выборе уязвимостей учитываются не только векторы атак (табл. 1), но также учитывается популярность этих уязвимостей на основе статистики БДУ ФСТЭК [5]. Информация о различных уязвимостях предоставлена ресурсом cwe.mitre.org [6].

Таблица 2

Уязвимости приложений [6]

Атака	Название уязвимости	Код CWE
Атака с помощью стелс-вирусов	Уязвимость недостаточного контроля доступа к данным	CWE-284
	Уязвимость выполнения кода с повышенными привилегиями	CWE-274
	Уязвимость обхода авторизации и аутентификации	CWE-287
	Уязвимость повышения привилегий	CWE-269
	Утечка конфиденциальной информации	CWE-200
	Недостаточное контролируемое разделение между сферами доверия	CWE-284
Атака с использованием макровирусов	Исполнение вредоносного кода	CWE-94
	Классическое переполнение буфера	CWE-120
	Исполнение нежелательного кода	CWE-94
	Классическое переполнение буфера	CWE-128
	Неправильный доступ к индексируемому ресурсу	CWE-118
	Утечка конфиденциальной информации	CWE-200
Атака с помощью сетевого червя	Внедрение вредоносного кода	CWE-506
	Неконтролируемое потребление ресурсов	CWE-400
	Неправильная проверка на предмет отзыва сертификата	CWE-299
	Неправильная проверка сертификата при несоответствии хоста	CWE-297

Продолжение табл. 2

Атака	Название уязвимости	Код CWE
	Неправильная нейтрализация данных	CWE-643
	Неправильное ограничение ссылки на внешнюю сущность XML	CWE-611
Атака вирус-ботнетом	Обход авторизации с помощью управляемого пользователем ключа	CWE-566
	Неправильное ограничение ссылок на рекурсивные объекты в DTDS	CWE-776
	Неправильный доступ к индексируемому ресурсу	CWE-118
	Использование смещения указателя вне диапазона	CWE-823
	Неправильное ограничение операций в пределах буфера памяти	CWE-119
	Недостаточная проверка подлинности данных	CWE-345
Атака вирусом с функцией рекламного ПО	Использование строки формата, контролируемой извне	CWE-134
	Модификация внешней переменной PHP	CWE-473
	Внедрение вредоносного кода	CWE-506
	Строка неконтролируемого формата	CWE-134
	Зависимость от одного фактора при принятии решений о безопасности	CWE-654
	Обнаружение/передача личной информации без авторизации	CWE-359

Используя информацию из базы данных БДУ ФСТЭК, на рис. 1 показано количество упоминаний уязвимостей из табл. 2. Эти данные отражают информацию за 2022 год, когда общее число упоминаний уязвимостей составило 7532 [5].

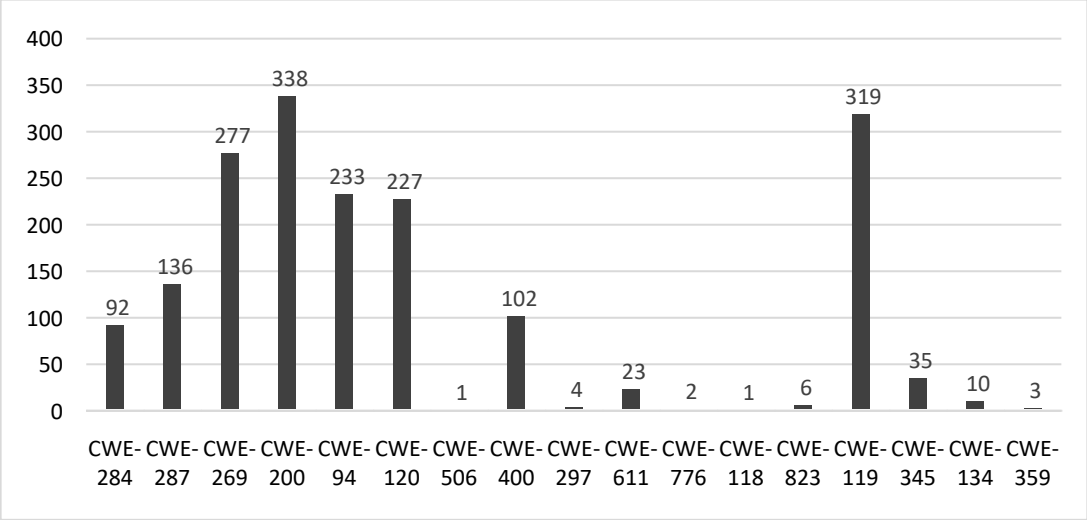

Рис. 1. Число упоминаний уязвимостей в 2022 году [5]

На основании графика на рис. 1 можно сделать вывод, что самыми опасными уязвимостями являются те, что связаны утечкой конфиденциальной информации, буфером памяти и повышением привилегий.

Риск рассчитаем по формуле:

$$\overline{Risk_{sij}} = F_{sij} \times \overline{U_{sij}}, \qquad (1)$$

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

$\overline{U_{sij}}$ – ущерб от реализации атаки типа S посредством i-го вектора.

Частота успешного использования уязвимости находится, как отношение числа упоминания данной уязвимости к общему

количеству упоминаний всех уязвимостей за исследуемый период.

Ущерб от реализации атаки рассчитаем в нормированном виде:

$$\overline{U_{sij}} = \frac{(\Delta t_{si})}{\max\,[\Delta t]}, \quad (2)$$

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

max $[\Delta t]$ – максимальное значение Δt_{si}.

Представим данные рис. 1 в виде табл. 3:

Таблица 3

Число упоминаний уязвимостей за 2022 год [5]

Уязвимость	Количество упоминаний
CWE-284	92
CWE-274	0
CWE-287	136
CWE-269	277
CWE-200	338
CWE-94	233
CWE-120	227
CWE-128	0
CWE-506	1
CWE-400	102
CWE-299	0
CWE-297	4
CWE-643	0
CWE-611	23
CWE-566	0
CWE-776	2
CWE-118	1
CWE-823	6
CWE-119	319
CWE-345	35
CWE-134	10
CWE-473	0
CWE-654	0
CWE-359	3
Общее число упоминаний уязвимостей	7532

В рамках данного исследования, мы представим информацию, полученную из DataSet "UNSW-NB15" [7], в виде табл. 4, отражающей временные значения простоя.

Таблица 4

Среднестатистическое время простоя для каждого вектора атаки [7]

Вектор атаки	Δt_{si}	$\max[\Delta t]$
VA_1	0,42	8
VA_2	1,89	25
VA_3	3,05	60
VA_4	1,41	4
VA_5	1,58	24

Исключив маловероятно используемые уязвимости из табл. 3, рассчитаем F_{sij} и $\overline{U_{sij}}$, с использованием данных табл. 3 и 4, а также формулы (2). Затем занесем полученные значения в табл. 5 и 6:

Таблица 5

Значения F_{sij} для уязвимостей

Уязвимость	F_{sij}
CWE-284	0,0122
CWE-287	0,0181
CWE-269	0,0368
CWE-200	0,0449
CWE-94	0,0309
CWE-120	0,0301
CWE-506	0,0001
CWE-400	0,0135
CWE-297	0,0005
CWE-611	0,0031
CWE-776	0,0003
CWE-118	0,0001
CWE-823	0,0008
CWE-119	0,0424
CWE-345	0,0046
CWE-134	0,0013
CWE-359	0,0004

Таблица 6

Значения $\overline{U_{sij}}$ для векторов атак

Вектор атаки	$\overline{U_{sij}}$
VA_1	0,053
VA_2	0,076
VA_3	0,051
VA_4	0,353
VA_5	0,066

Для создания матрицы рисков и риск-ландшафта необходимо разработать матрицу смежности для векторов атак и уязвимостей компьютерными вирусами. При создании матрицы смежности учитываются данные уязвимости атаки и их последствия, которые были получены из источника cwe.mitre.org [6].

Таблица 7

Матрица смежности векторов атак и уязвимостей

Уязвимость	VA_1	VA_2	VA_3	VA_4	VA_5
CWE-284	1	1	1	1	0
CWE-287	1	1	1	1	1
CWE-269	1	1	1	1	0
CWE-200	1	1	1	1	0
CWE-94	1	1	0	1	1
CWE-120	1	1	0	1	1
CWE-506	1	1	1	0	1
CWE-400	0	0	1	0	0

Продолжение табл. 7

Уязвимость	VA_1	VA_2	VA_3	VA_4	VA_5
CWE-297	0	1	1	1	1
CWE-611	1	0	1	0	0
CWE-776	1	0	0	1	0
CWE-118	0	0	0	1	0
CWE-823	0	0	0	1	0
CWE-119	1	0	0	1	1
CWE-345	0	0	0	1	1
CWE-134	0	0	0	0	1
CWE-359	1	0	0	0	1

На основе информации, представленной в табл. 5 и 6, с учетом данных из табл. 7, построим матрицу рисков, связанных с реализацией атак через уязвимости. Для этого мы воспользуемся формулой (1).

Таблица 8

Матрица рисков реализации атак через уязвимости

Уязвимость	VA_1	VA_2	VA_3	VA_4	VA_5
CWE-284	0,00065	0,00093	0,00062	0,00431	0
CWE-287	0,00096	0,00096	0,00092	0,00639	0,00119
CWE-269	0,00196	0,00279	0,00188	0,01299	0
CWE-200	0,00238	0,00341	0,00154	0,01585	0
CWE-94	0,00164	0,00235	0	0,01091	0,00204
CWE-120	0,00159	0,00229	0	0,01063	0,00199
CWE-506	0,00001	0,00001	0,00001	0	0,00001
CWE-400	0	0	0,00069	0	0
CWE-297	0	0,00004	0,00003	0,00018	0,00003
CWE-611	0,00016	0	0,00016	0	0
CWE-776	0,00002	0	0	0,00011	0
CWE-118	0	0	0	0,00004	0
CWE-823	0	0	0	0,00028	0
CWE-119	0,00225	0	0	0,01497	0,00279
CWE-345	0	0	0	0,00162	0,0003
CWE-134	0	0	0	0	0,00009
CWE-359	0,00002	0	0	0	0,00003

С использованием информации, содержащейся в табл. 8, построим риск-ландшафт, который представит собой визуализацию рисков, связанных с реализацией атаки компьютерными вирусами (рис. 2).

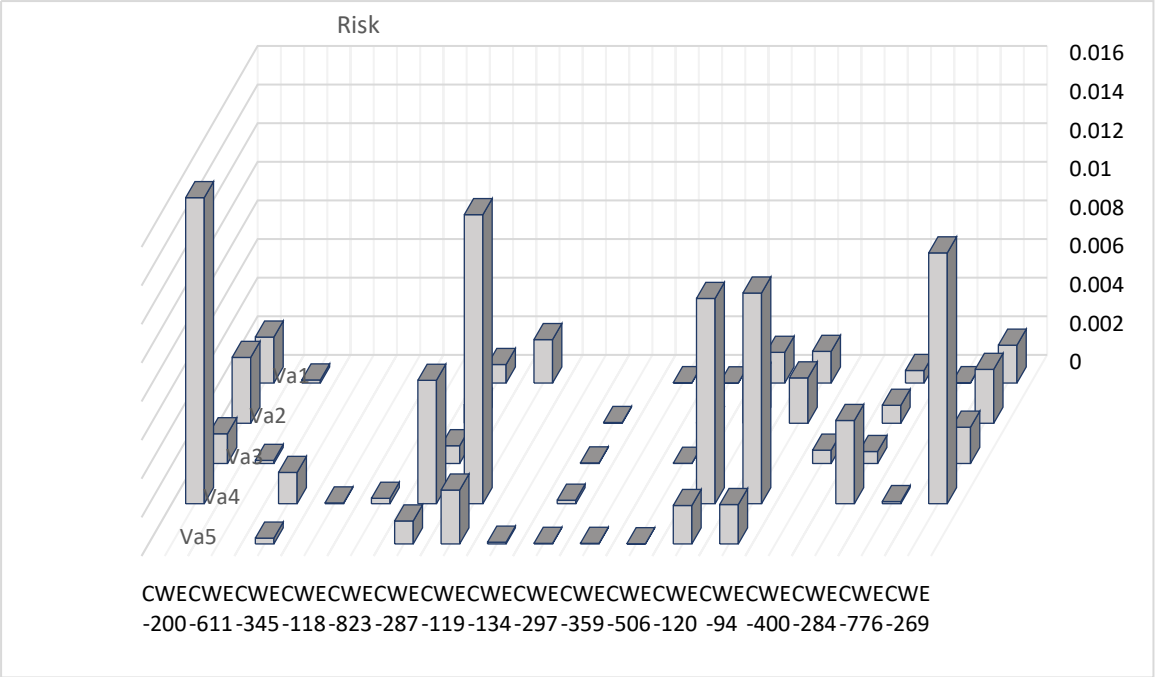

Рис. 2. Риск-ландшафт реализации атак компьютерными вирусами

Исходя из построенного риск-ландшафта уязвимостей и векторов для компьютерных выделим наиболее опасные сочетания вирусов.

Таблица 9

Опасные сочетания уязвимостей и векторов атаки

Идентификатор вектора атаки	Наименование вектора атаки	Уязвимость
Атака с помощью стелс-вирусов (VA_1)	Проникновение в систему через сетевой периметр	Неправильное ограничение операций в пределах буфера памяти (CWE-119)
		Классическое переполнение буфера (CWE-120)
		Исполнение вредоносного кода (CWE-94)
	Получение доступа к ключевым системам	Уязвимость обхода авторизации и аутентификации (CWE-287)
	Развитие атаки на целевые системы и реализация недопустимых событий	Уязвимость повышения привилегий (CWE-269)
	Обход механизмов обнаружения и защиты	Утечка конфиденциальной информации (CWE-200)
Атака с использованием макровирусов (VA_2)	Введение вредоносных макросов	Исполнение вредоносного кода (CWE-94)
		Уязвимость повышения привилегий (CWE-269)
	Использование социальной инженерии	Классическое переполнение буфера (CWE-120)
	Маскировка и обход защитных механизмов	Уязвимость обхода авторизации и аутентификации (CWE-287)

Продолжение табл. 9

Идентификатор вектора атаки	Наименование вектора атаки	Уязвимость
	Распространение через документы и сетевые ресурсы	Уязвимость недостаточного контроля доступа к данным (CWE-284)
	Использование обновлений и патчей	Утечка конфиденциальной информации (CWE-200)
Атака с помощью сетевого червя (VA_3)	Заражение хостов	Уязвимость повышения привилегий (CWE-269)
	Эксплуатация уязвимостей	Утечка конфиденциальной информации (CWE-200)
		Уязвимость обхода авторизации и аутентификации (CWE-287)
Атака вирус-ботнетом (VA_4)	Заражение устройств	Уязвимость повышения привилегий (CWE-269)
		Классическое переполнение буфера (CWE-120)
		Уязвимость обхода авторизации и аутентификации (CWE-287)
		Исполнение вредоносного кода (CWE-94)
	Формирование ботнета	Уязвимость недостаточного контроля доступа к данным (CWE-284)
	Маскировка и уклонение от обнаружения	Неправильное ограничение операций в пределах буфера памяти (CWE-119)
	Распространение	Недостаточная проверка подлинности данных (CWE-345)
		Утечка конфиденциальной информации (CWE-200)
Атака вирусом с функцией рекламного ПО (VA_5)	Внедрение вредоносного кода в рекламные баннеры	Уязвимость повышения привилегий (CWE-269)
	Маскировка под легитимное рекламное ПО	Уязвимость обхода авторизации и аутентификации (CWE-287)
	Кража данных	Утечка конфиденциальной информации (CWE-200)

В табл. 9 указаны уязвимости, которые представляют наибольшую опасность при атаке компьютерными вирусами на корпоративные сети.

Стоит отметить, что для дальнейшего практического применения не рекомендуется учитывать наименее опасные сочетания, так как их риски можно считать пренебрежимо малыми в контексте реальных сценариев.

Заключение

В ходе представленного исследования был проведен подробный риск-анализ сетевых атак компьютерными вирусами, включающий в себя построение соответствующего риск-ландшафта с учетом различных сценариев атак и уязвимостей, представляющих потенциальную угрозу для корпоративных сетей. Этот анализ позволил выявить наиболее опасные сочетания сценариев атак и уязвимостей, а также оценить степень риска и ущербности для организаций.

Полученный риск-ландшафт может являться основой для разработки соответствующих мер защиты

корпоративных сетей от сетевых атак компьютерными вирусами, как организационно-правовых, так и технических. Наиболее опасные сочетания сценариев атак и уязвимостей, выявленные в результате риск-анализа, представляют ценность в контексте приоритезации направлений дальнейших исследований и разработок в области обеспечения безопасности предприятий от сетевых атак компьютерными вирусами. В частности, представляется возможным разработать частные политику, регламенты и инструкции, представляющие собой формат, напрямую адаптированный для практического применения предприятиями и организациями [8,9].

Таким образом, проведенный риск-анализ и построение риск-ландшафта позволили достигнуть значимого результата в контексте исследования и оценки рисков сетевых атак компьютерными вирусами на корпоративные сети предприятий. Полученные результаты позволяют определить наиболее актуальные направления для дальнейшей разработки мер по регулированию соответствующих рисков, в частности – политики, регламентов и инструкций безопасности информации для эффективной защиты информационных систем организаций. Наиболее перспективным видится направление дальнейшей работы, включающее в себя разработку данных компонентов, позволяющих получить актуальные результаты, готовые к практическому использованию. С другой стороны, область применения полученных результатов может быть в будущем расширена за счёт исследований, специфически направленных на разработку мер защиты для противодействию выявленным наиболее опасным сочетаниям сценариев атак и уязвимостей. С учётом этого, полученные результаты, в совокупности с перспективами дальнейшей научно-исследовательской работы, позволят повысить защищённости корпоративных сетей от сетевых атак компьютерными вирусами.

Список литературы

1. Кибератаки. URL: https://www.tadviser.ru/index.php/Статья:Кибератаки (дата обращения 10.02.2024).

2. Обнаружение распространенных угроз ИБ в сетевом трафике. URL: https://www.ptsecurity.com/ru-ru/research/analytics/network-traffic-analysis-2022/ (дата обращения 10.02.2024)..

3. Вредоносное ПО в корпоративной сети: угрозы и способы обнаружения. URL: https://www.ptsecurity.com/ru-ru/research/analytics/malware-threats-and-detection-2023/ (дата обращения 10.02.2024)..

4. Common Attack Pattern Enumeration and Classification. URL: https://capec.mitre.org.

5. БДУ ФСТЭК России URL: https://bdu.fstec.ru/vul (дата обращения 10.02.2024)..

6. Common Weakness Enumeration. URL: https://cwe.mitre.org/index.html (дата обращения 10.02.2024)..

7. DataSet UNSW-NB15. URL: https://www.kaggle.com/datasets/alextamboli/unsw-nb15 (дата обращения 10.02.2024)..

8. Стандарты в области информационной безопасности. URL: https://www.altell.ru/legislation/standards/ (дата обращения 10.02.2024)..

9. ISO/IEC 27001. Системы менеджмента информационной безопасности. URL: https://www.iso.org/ru/standard/27001 (дата обращения 10.02.2024).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 14.02.2024

Информация об авторах

Кобцев Олег Евгеньевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Шеншин Александр Игоревич – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Питолин Владимир Михайлович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Паринова Лариса Владимировна – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Юрасов Владислав Георгиевич – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Печкин Дмитрий Сергеевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

NETWORK ATTACKS BY COMPUTER VIRUSES: RISK LANDSCAPE

O.E. Kobcev, A.I. Shenshin, V.M. Pitolin, L.V. Parinova, V.G. Yurasov, D.S. Pechkin

This scientific article is dedicated to the study of network attacks carried out by computer viruses on corporate networks, specifically focusing on a comprehensive risk analysis of corresponding attack scenarios. Various attack scenarios and vulnerabilities used for their implementation were analyzed during the research. Special attention was paid to the statistical assessment of the frequency and severity of such attacks. Based on the results obtained, a risk landscape was constructed, and the most dangerous combinations of attack scenarios (vectors) and vulnerabilities were identified. The obtained result can serve as a basis for further development of both organizational and legal, as well as technical measures to protect corporate networks from network attacks by computer viruses.

Keywords: corporate network, computer viruses, vulnerabilities, impact, risk landscape.

Submitted 14.02.2024

Information about the authors

Oleg E. Kobcev – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Alexander I. Shenshin – post-graduate, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Vladimir M. Pitolin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Larisa V. Parinova – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Vladislav G. Yurasov – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Dmitry S. Pechkin – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com