DOI 10.36622/1682-7813.2024.27.1.004
УДК 004.056.57

СЕТЕВЫЕ АТАКИ КОМПЬЮТЕРНЫМИ ВИРУСАМИ: ЧАСТНАЯ ПОЛИТИКА И РЕГЛАМЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О.Е. Кобцев, А.И. Шеншин, В.М. Питолин,
Л.В. Паринова, Ю.Г. Пастернак, Ю.В. Макаров

Данная научная статья посвящена исследованию сетевых атак, осуществляемых компьютерными вирусами на корпоративные сети, в частности – разработке комплекса мер по обеспечению информационной безопасности предприятия. В ходе исследования, на основе информации о сценариях (векторах) сетевых атак компьютерными вирусами, разработана частная политика и регламенты обеспечения информационной безопасности предприятия. Результаты исследования представляют собой значимый вклад в области обеспечения информационной безопасности предприятий, адаптированы для практического использования, а также могут служить основой для дальнейшей разработки мер по защите от сетевых атак компьютерными вирусами.

Ключевые слова: корпоративная сеть, компьютерные вирусы, уязвимости, частная политика, частные регламенты.

Введение

В настоящее время информационные технологии играют всё большую роль в повседневной деятельности, включая бизнес-процессы и частную жизнь в целом, расширяя возможности и повышая эффективность множества процессов. При этом вместе с преимуществами глобальной информатизации, возникают и новые угрозы для информационной безопасности, где особые ущербы несут сетевые атаки, осуществляемые с использованием компьютерных вирусов [1].

Актуальность данного направления исследований обусловлена растущими количеством и качеством (функциональности) компьютерных вирусов, которые представляют серьезную угрозу для информационной безопасности предприятий, в частности, для корпоративных сетей. Информационные технологии играют ключевую роль в бизнес-процессах коммерческих и государственных организаций, а недостаточная защищенность корпоративных сетей от атак может привести к серьезным последствиям, включая утечку конфиденциальных данных, отказ в обслуживании и подмену данных.

По данным 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 разработка соответствующих политик и регламентов являются неотъемлемой частью стратегии информационной безопасности.

Отсюда настоящая статья направлена на исследование сетевых атак компьютерными вирусами на корпоративные сети и предлагает разработку частных политик и регламентов безопасности информации, адаптированных для практического применения в рамках защиты информационных систем организаций.

Векторы сетевых атак компьютерными вирусами

В рамках разработки частной политики и регламентов информационной безопасности предприятия в контексте защиты от конкретного вида атак, необходимо проанализировать сценарии (векторы) соответствующей атаки. При этом необходимо придерживаться наиболее достоверных и проверенных источников. Основываясь на 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.
	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.

Продолжение табл. 1

Атака	Векторы атаки	Описание
	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.
	Распространение через вредоносные рекламные элементы	Использование вредоносных рекламных баннеров или всплывающих окон для распространения вируса с функцией рекламного ПО.
	Использование эксплойтов и уязвимостей	Использование 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 векторы атак, представленные в табл. 1. Они будут использоваться в качестве исходных данных в части механизмов реализации угрозы для формирования частной политики и регламентов информационной безопасности предприятия.

Частная политика и регламенты безопасности предприятия

Информационная безопасность является ключевым аспектом современного цифрового мира, где данные и информационные системы играют важную роль. Обеспечение безопасности информации становится все более сложной задачей, требующей внимания и комплексного подхода. В рамках данного исследования мы обращаемся к разработке и реализации частной политики обеспечения информационной безопасности в организациях.

Одной из основных составляющих этой политики являются российские и международные стандарты, такие как ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения" и ГОСТ Р 51275-2006 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения", а также международный стандарт ISO/IEC 27001 [5]. Эти стандарты определяют ключевые понятия и принципы обеспечения информационной безопасности, которые будут использованы при разработке нашей частной политики.

В рамках обеспечения информационной безопасности объектов защиты в организации от сетевых атак на уровне компьютерных вирусов представлено в табл. 2.

Таблица 2

Объекты защиты

Идентификатор вектора атаки	Сценарий атаки	Объект защиты
VA_1	Проникновение в систему через сетевой периметр	Компьютеры и серверы
	Получение доступа к ключевым системам	Центральные системы управления доступом
	Развитие атаки на целевые системы и реализация недопустимых событий	Веб-серверы Базы данных
	Обход механизмов обнаружения и защиты	Системы с описанием мониторинга и журналирования событий
VA_2	Введение вредоносных макросов	Электронная почта и почтовый клиент
	Маскировка и обход защитных механизмов	Периметр сети и сетевые устройства
	Распространение через документы и сетевые ресурсы	Файловые серверы и широкополосные сети
	Использование обновлений и патчей	Корпоративные системы и программное обеспечение
VA_3	Заражение хостов	Сетевое оборудование Сетевые службы
	Эксплуатация уязвимостей	Операционные системы и приложения
VA_4	Заражение устройств	Компьютеры и серверы Мобильные устройства
	Формирование ботнета	Коммуникационные каналы

Продолжение табл. 2

Идентификатор вектора атаки	Сценарий атаки	Объект защиты
	Маскировка и уклонение от обнаружения	Периметр сети и сетевые устройства
	Распространение	Сетевая инфраструктура
VA_5	Внедрение вредоносного кода в рекламные баннеры	Фильтрация трафика
	Маскировка под легитимное рекламное ПО	Рекламные блокировщики
	Кража данных	Устройства и серверы

Для составления плана мероприятий требуется определить последовательность шагов, которые могут быть предприняты злоумышленником, а также разработать общие меры по защите организации от сетевых атак (табл. 3).

Таблица 3

Соответствие действий злоумышленника и меры противодействия им

Последовательность и содержание действий злоумышленника в целях реализации сценариев атаки компьютерными вирусами	Меры защиты Организации от сетевой атаки компьютерными вирусами, адекватные действиям злоумышленника по каждому сценарию
1	2
Атака с помощью стелс-вирусов (VA_1)	
1.1 Проникновение в систему через сетевой периметр	1.1 Разработка и внедрение комплексных систем защиты сетевого периметра, включающих сетевые фаерволлы, системы обнаружения вторжений и механизмы контроля доступа.
1.2 Получение доступа к ключевым системам	1.2 Реализация принципа "наименьших привилегий" для ограничения прав доступа пользователей к ключевым системам. Постоянный мониторинг и аудит доступа к системам.
1.3 Развитие атаки на целевые системы и реализация недопустимых событий	1.3 Регулярное обновление и усиление механизмов обнаружения и предотвращения вторжений на целевые системы. Разработка и применение стратегии отделения сетей для ограничения распространения атак.
1.4 Обход механизмов обнаружения и защиты	1.4 Реализация многоуровневой защиты, эвристический анализ, облачные технологии и машинное обучение для раннего обнаружения и предотвращения новых вирусных атак.
Атака с использованием макровирусов(VA_2)	
2.1 Введение вредоносных макросов	2.1 Ограничение выполнения макросов в документах, настройка политик безопасности, запрещающих автоматическое выполнение макросов. Обновление и патчинг приложений для устранения уязвимостей, которые могут быть использованы злоумышленниками для внедрения вредоносных макросов.

Продолжение табл. 3

1	2
Атака с использованием макровирусов(VA_2)	
2.2 Маскировка и обход защитных механизмов	2.2 Установка и конфигурирование систем обнаружения вредоносного кода с функциями распознавания и блокирования макровирусов. Использование технологий облачной безопасности для анализа и блокировки потенциально вредоносных файлов.
2.3 Распространение через документы и сетевые ресурсы	2.3 Управление системами контроля доступа, обеспечивающими надлежащий контроль доступа к данным и предотвращение распространения атак через документы и сетевые ресурсы. Регулярное сканирование и мониторинг сетевых ресурсов на предмет обнаружения и удаления вредоносных документов и файлов.
2.4 Использование обновлений и патчей	2.4 Реализация мер по обнаружению и предотвращению утечки конфиденциальной информации при использовании обновлений и патчей, включая управление процессом обновления и контроль целостности систем.
Атака с помощью сетевого червя (VA_3)	
3.1 Заражение хостов	3.1 Установка и настройка брандмауэров для мониторинга и фильтрации сетевого трафика, блокировки подозрительных подключений и предотвращения распространения червей. Регулярное сканирование и мониторинг устройств на предмет обнаружения и удаления вредоносных программ.
3.2 Эксплуатация уязвимостей	3.2 Внедрение и настройка систем обнаружения вторжений для обнаружения и предотвращения попыток эксплуатации уязвимостей. Изоляция и сегментация сетей для предотвращения быстрого распространения червей между хостами.
Атака вирус-ботнетом (VA_4)	
4.1 Заражение устройств	4.1 Установка и настройка межсетевых экранов (firewalls) для фильтрации сетевого трафика и блокировки подозрительных подключений.
4.2 Формирование ботнета	4.2 Разработка и реализация стратегии управления устройствами с использованием централизованного мониторинга и управления, обнаружения и блокировки подозрительной активности.
4.3 Маскировка и уклонение от обнаружения	4.3 Установка и настройка систем обнаружения вторжений и систем защиты конечных точек для обнаружения и блокировки вредоносных программ и повышения общей безопасности устройств.
4.4 Распространение	4.4 Регулярное обновление прикладного программного обеспечения и устройств для закрытия известных уязвимостей и предотвращения распространения вирусов через уязвимые точки входа

Окончание табл. 3

1	2
Атака вирусом с функцией рекламного ПО (VA_5)	
5.1 Внедрение вредоносного кода в рекламные баннеры	5.1 Использование специализированных программных решений для обнаружения и блокировки вредоносных кодов, включая анализ рекламных баннеров на предмет наличия вредоносных элементов. Регулярное обновление и проверка механизмов фильтрации рекламного трафика.
5.2 Маскировка под легитимное рекламное ПО	5.2 Внедрение многоуровневой защиты, включая облачные сервисы для фильтрации рекламного трафика, а также регулярное обновление программных компонентов для предотвращения использования уязвимостей.
5.3 Кража данных	5.3 Реализация системы защиты данных, включающей шифрование конфиденциальной информации, установку системы контроля доступа, резервное копирование данных и мониторинг активности пользователей для обнаружения подозрительной активности.

Учитывая данные из табл. 3, возможно составить описание средств обнаружения инцидентов, связанных с компьютерными вирусами (табл. 4), меры предотвращения таких инцидентов (табл. 5) и меры по устранению их последствий (табл. 6). В основе этих таблиц лежат регламенты, определяющие процессы обнаружения и регистрации инцидентов, реагирования на них, а также ликвидации возможных последствий, связанных с сетевыми атаками компьютерными вирусами на уровне систем и приложений в организации. В табл. 4 в первом столбце перечислены типы инцидентов, которые могут возникнуть при реализации действий злоумышленника в ходе сетевой атаки компьютерными вирусами.

Таблица 4

Обнаружение и регистрация инцидентов безопасности

Типы инцидентов	Описание инцидента	Средства для обнаружения заданного типа инцидента
Атака с помощью стелс-вирусов (VA_1)		
Нарушение безопасности информационной системы	Несанкционированное проникновение в информационную систему компании путем использования уязвимостей в сетевом периметре.	Система мониторинга сетевого периметра с анализом сетевого трафика, включающая системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS).
Незаконное проникновение в критические системы	Несанкционированное получение доступа к системам, содержащим критическую информацию и ключевые компоненты	− Мониторинг активности пользователей. − Системы аутентификации и авторизации. − Системы контроля доступа. Системы логирования и анализа журналов.

Продолжение табл. 4

Типы инцидентов	Описание инцидента	Средства для обнаружения заданного типа инцидента
Атака с использованием макровирусов (VA_2)		
Несанкционированный доступ при эксплуатации макросов для инъекции вредоносного кода в документы и файлы с целью нанесения ущерба	Использование макровирусов для внедрения вредоносного кода в документы и файлы, с целью нанесения вреда или получения доступа.	− Системы антивирусной защиты с обновляемыми базами сигнатур. − Системы обнаружения вредоносного кода. − Системы контроля и фильтрации содержимого электронной почты и файлов. − Системы обнаружения аномалий в поведении приложений. − Системы контроля и управления программными обновлениями.
Атака с помощью сетевого червя (VA_3)		
Инфицирование хостов в корпоративной сети с целью заражения и использования их в дальнейших актах вредоносного характера	Атака на хосты в сети компании с целью их заражения и использования в дальнейших вредоносных действиях.	− Системы обнаружения вторжений. − Системы контроля доступа и аутентификации. − Системы мониторинга и анализа событий. Системы управления патчами и обновлениями.
Атака вирус-ботнетом (VA_4)		
Компрометация устройств в сети компании с целью их включения в ботнет или последующего использования в других формах атак, контроль над зараженными устройствами с целью координированных атак или использования в качестве ресурсов	Заражение устройств в сети компании с целью включения их в ботнет или использования в дальнейших атаках, выполнение координированных атак или использование в качестве ресурсов.	− Системы мониторинга и обнаружения зараженных устройств в сети. − Инструменты для обнаружения отклонений от нормального поведения, связанных с ботнет-активностью. − Использование анализа сетевого трафика для выявления связанных с ботнетом активностей, таких как соединение или взаимодействие между зараженными устройствами в ботнете и известными командными и контрольными серверами ботнета
Атака вирусом с функцией рекламного ПО (VA_5)		
Внедрение вредоносного кода в рекламные баннеры с целью нанесения ущерба компании, а также сбора данных	Внедрение вредоносного кода в рекламные баннеры, с целью нанесения вреда пользователям, просматривающим эти баннеры.	− Использование систем мониторинга и анализа рекламных баннеров для обнаружения вредоносного кода и нежелательных действий.

Окончание табл. 4

Типы инцидентов	Описание инцидента	Средства для обнаружения заданного типа инцидента
	Несанкционированное получение доступа к конфиденциальным данным и кража информации для дальнейшего использования или утечки.	− Технологии машинного обучения для выявления аномальных паттернов в поведении рекламных компонентов. − Реализация систем детектирования утечки данных (DLP - Data Loss Prevention) для обнаружения и контроля потока конфиденциальных данных. − Методы анализа сетевого трафика. − Контроль доступа к файловым системам. − Мониторинг использования конфиденциальных ресурсов.

К первоочередным мерам по предотвращению инцидента, а также негативным результатам инцидента безопасности, возникшего в процессе сетевой атаки, относятся данные предоставленные в табл. 5. В левом столбце табл. 5 перечислены произошедшие инциденты в ходе действий злоумышленника в целях реализации сценариев сетевой атаки компьютерными вирусами.

Таблица 5

Реагирование на инциденты безопасности

Произошедшие инциденты	Первоочередные меры по предотвращению инцидента	Негативные последствия, вызванные инцидентом безопасности
1	2	3
Атака с помощью стелс-вирусов (VA_1)		
Несанкционированное проникновение в информационную систему компании путем использования уязвимостей в сетевом периметре	• Изоляция компрометированного сетевого периметра от остальной сети. • Анализ и закрытие уязвимостей сетевых устройств и серверов. • Проверка и обновление правил фильтрации сетевого трафика. • Мониторинг сетевой активности для выявления подозрительной активности.	Обход механизмов обнаружения и блокирования, позволяющий злоумышленникам получить несанкционированный доступ к сети и системам. Компрометация конфиденциальности данных путем перехвата и прослушивания сетевого трафика в результате успешного проникновения. Открытие обратных дверей и создание тайных точек входа для дальнейшей эксплуатации системы и возможного распространения атак на внутренние узлы.

Продолжение табл. 5

1	2	3
Несанкционированное получение доступа к системам, содержащим критическую информацию и ключевые компоненты	• Изоляция компрометированных систем от остальной сети. • Проверка и обновление системных и прикладных компонентов. • Анализ журналов системных событий для обнаружения подозрительной активности.	• Использование полученных привилегий для получения доступа к системам, содержащим важную и конфиденциальную информацию. • Компрометация целостности данных и возможность их изменения или удаления без разрешения. • Нарушение доступности систем и сервисов путем блокировки или отказа в обслуживании, наносящее ущерб бизнесу и репутации организации.
Атака с использованием макровирусов (VA_2)		
Несанкционированный доступ при эксплуатации макросов для инъекции вредоносного кода в документы и файлы с целью нанесения ущерба	• Отключение выполнения макросов в офисных приложениях. • Установка и настройка антивирусных программ с функцией обнаружения макросов.	• Использование макросов в офисных приложениях для введения вредоносного кода и запуска вредоносных действий без ведома пользователя. • Автоматическое распространение вредоносных макросов через электронные письма, документы и другие файлы, в результате чего возможно заражение большого количества систем.
Атака с помощью сетевого червя (VA_3)		
Инфицирование хостов в корпоративной сети с целью заражения и использования их в дальнейших актах вредоносного характера	Изоляция зараженных хостов от сети. Анализ журналов событий на зараженных хостах для выявления дополнительных компрометаций	Заражение уязвимых узлов в сети, таких как компьютеры и серверы, в результате успешной атаки. Компрометация локальных данных, установка вредоносного программного обеспечения и использование зараженных хостов для распространения атаки на другие устройства в сети. Потеря контроля над зараженными хостами и возможное использование их в дальнейших кибератаках или ботнетах.
Атака вирус-ботнетом (VA_4)		
Компрометация устройств в сети с целью включения их в ботнет или использования в других формах атак, контроль над зараженными устройствами с целью координированных	Изоляция зараженных устройств от сети. Сканирование и удаление вредоносных программ на зараженных устройствах. Обновление операционных систем и приложений на	Заражение встроенных систем, умных устройств и промышленных контроллеров, приводящее к нарушению их функциональности и возможности дистанционного управления. Использование компрометированных устройств в качестве точек входа или прокси-

Окончание табл. 5

1	2	3
атак или использования в качестве ресурсов	зараженных устройствах. Идентификация и блокировка коммуникации с серверами управления ботнетом. Сбор информации о компрометированных устройствах и их изоляция.	серверов для дальнейших атак на внутренние сети или системы. Распространение вредоносного кода через сеть устройств и создание ботнета, служащего инструментом для массовых кибератак. Создание сети компьютеров и устройств, зараженных вредоносными программами, под управлением злоумышленников.
Атака вирусом с функцией рекламного ПО (VA_5)		
Внедрение вредоносного кода в рекламные баннеры с целью нанесения ущерба компании, а также сбора и утечки конфиденциальных данных	Анализ и фильтрация входящего трафика, связанного с рекламными баннерами. Остановка несанкционированного доступа и прекращение дальнейшей утечки данных. Восстановление систем безопасности и проведение расследования инцидента. Уведомление клиентов и заинтересованных сторон об инциденте.	Заражение системы пользователя и получение доступа к конфиденциальным данным или использование устройства для дальнейших кибератак. Маскировка вредоносного кода среди легитимного рекламного контента для обхода систем обнаружения и блокировки вредоносных программ. Кража персональных данных, финансовых сведений, интеллектуальной собственности или других чувствительных данных. Возможное использование украденной информации в целях шантажа, мошенничества или нарушения приватности.

Составим меры по устранению предотвращения повторного возникновения инцидентов безопасности для подобных нарушений (табл. 6).

Таблица 6

Ликвидация последствий инцидента безопасности

Негативные последствия, вызванные инцидентом безопасности	Меры по устранению инцидента
Атака с помощью стелс-вирусов (VA_1)	
Обход механизмов обнаружения и блокирования, позволяющий злоумышленникам получить несанкционированный доступ к сети и системам. Компрометация конфиденциальности данных путем перехвата и прослушивания сетевого трафика в результате успешного проникновения. Открытие обратных дверей и создание тайных точек входа для дальнейшей эксплуатации системы и возможного распространения атак на внутренние узлы.	разработать и реализовать стратегию сегментации сети, включая использование межсетевых экранов для ограничения доступа между сетевыми зонами; обеспечить правильную конфигурацию сетевого оборудования, включая настройку правил фильтрации трафика и механизмов обнаружения сетевых атак; установить политику использования защиты и обеспечить регулярное обновление и патчинг систем.

Продолжение табл. 6

Негативные последствия, вызванные инцидентом безопасности	Меры по устранению инцидента
Использование полученных привилегий для получения доступа к системам, содержащим важную и конфиденциальную информацию. Компрометация целостности данных и возможность их изменения или удаления без разрешения. Нарушение доступности систем и сервисов путем блокировки или отказа в обслуживании, наносящее ущерб бизнесу и репутации организации.	установить строгий контроль доступа к системам и ресурсам, основанный на принципе наименьших привилегий; проводить регулярную проверку и обновление конфигурации систем для исключения возможности использования скомпрометированных учетных записей.
Атака с использованием макровирусов (VA_2)	
Использование макросов в офисных приложениях для введения вредоносного кода и запуска вредоносных действий без ведома пользователя. Автоматическое распространение вредоносных макросов через электронные письма, документы и другие файлы, в результате чего возможно заражение большого количества систем. Нарушение целостности и конфиденциальности данных, кража информации или внедрение дополнительного вредоносного кода для дальнейшей эксплуатации.	разработать и применять механизмы обнаружения вредоносных макросов, включая использование антивирусного программного обеспечения с функцией анализа макросов. регулярное обновление и патчинг операционных систем и приложений на хостах; установка и активация эффективного антивирусного программного обеспечения. обеспечение многоуровневой защиты сетевого периметра, включая использование брандмауэров и сетевых мониторов; обучение сотрудников основам кибербезопасности, включая распознавание фишинговых писем и подозрительных вложений.
Атака с помощью сетевого червя (VA_3)	
Заражение уязвимых узлов в сети, таких как компьютеры и серверы, в результате успешной атаки. Компрометация локальных данных, установка вредоносного программного обеспечения и использование зараженных хостов для распространения атаки на другие устройства в сети. Потеря контроля над зараженными хостами и возможное использование их в дальнейших кибератаках или ботнетах.	обновлять устройства, включая операционные системы и приложения, для устранения уязвимостей повышения привилегий; настроить правильную конфигурацию устройств, отключение ненужных сервисов; обеспечить регулярное обновление и замену устройств с устаревшими или не обновленными версиями программного обеспечения.
Атака вирус-ботнетом (VA_4)	
Заражение встроенных систем, умных устройств и промышленных контроллеров, приводящее к нарушению их функциональности и возможности дистанционного управления. Использование компрометированных устройств в качестве точек входа или прокси-серверов для дальнейших атак на внутренние сети или системы. Распространение вредоносного кода через сеть устройств и создание ботнета, для массовых кибератак.	регулярное сканирование сети на наличие уязвимых устройств и своевременное устранение обнаруженных проблем; внедрение средств мониторинга сетевого трафика для обнаружения подозрительной активности и поведения устройств; ограничение доступа к сетевым сервисам и портам, необходимым для нормального функционирования;

Окончание табл. 6

Негативные последствия, вызванные инцидентом безопасности	Меры по устранению инцидента
Создание сети компьютеров и устройств, зараженных вредоносными программами, под управлением злоумышленников. Контроль и координация действий ботнета для выполнения различных целей, включая кибератаки, спам, фишинг и распространение вредоносного кода. Использование ресурсов ботнета для генерации дохода, такого как майнинг криптовалюты или выполнение вычислительных задач.	регулярное обновление и обучение сотрудников по политикам безопасности, использованию безопасных аутентификационных методов и основам безопасного поведения в сети.
Атака вирусом с функцией рекламного ПО (VA_5)	
Внедрение вредоносного программного кода в рекламные баннеры на веб-сайтах, с целью компрометации устройств пользователей при их просмотре. Заражение системы пользователя и получение доступа к конфиденциальным данным или использование устройства для дальнейших кибератак. Маскировка вредоносного кода среди легитимного рекламного контента для обхода систем обнаружения и блокировки вредоносных программ. Кража персональных данных, финансовых сведений, интеллектуальной собственности или других чувствительных данных. Возможное использование украденной информации в целях шантажа, мошенничества или нарушения приватности.	разработать и применять механизмы обнаружения вредоносных рекламных баннеров, с функцией анализа рекламного контента; установить строгий контроль над рекламными платформами, включая использование только доверенных и проверенных рекламных провайдеров; провести фильтрацию рекламных баннеров, исключая не доверенные и потенциально вредоносный рекламный контент. внедрение механизмов шифрования для защиты хранящихся данных, особенно конфиденциальной информации; ограничение доступа к конфиденциальным данным только необходимым сотрудникам;

Заключение

В ходе исследования были разработаны частные политика и регламенты, которые специально адаптированы для обеспечения информационной безопасности корпоративных сетей и борьбы с атаками компьютерными вирусами. Полученные регламенты представляют собой важные инструменты для организаций, позволяющие эффективно защищать свои сети, предотвращать атаки и минимизировать возможные последствия.

Результаты данного исследования имеют практическую значимость и могут быть применены в компаниях и организациях в качестве основы для разработки и внедрения собственных политик и стратегий обеспечения информационной безопасности. Частные регламенты, разработанные в рамках исследования, предоставляют организациям четкие руководящие принципы для защиты и обеспечения безопасности их информационной инфраструктуры.

Список литературы

1. Кибератаки. URL: https://www.tadviser.ru/index.php/Статья:Кибератаки (дата обращения 08.02.2024).

2. Обнаружение распространенных угроз ИБ в сетевом трафике. URL: https://www.ptsecurity.com/ru-ru/research/analytics/network-traffic-analysis-2022/ (дата обращения 08.02.2024).

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 08.02.2024).

4. Common Attack Pattern Enumeration and Classification. URL: https://capec.mitre.org (дата обращения 08.02.2024).

5. Стандарты в области информационной безопасности. URL: https://www.altell.ru/legislation/standards/ (дата обращения 08.02.2024).

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

Пастернак Юрий Геннадьевич – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Макаров Юрий Вадимович – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

NETWORK ATTACKS BY COMPUTER VIRUSES: SPECIFIC INFORMATION SECURITY POLICY

O.E. Kobcev, A.I. Shenshin, V.M. Pitolin, L.V. Parinova, Y.G. Pasternak, Y.V. Makarov

This scientific article is dedicated to the study of network attacks carried out by computer viruses on corporate networks, specifically focusing on the development of a set of measures to ensure the information security of the enterprise. During the research, based on information about scenarios (vectors) of network attacks by computer viruses, a specific policy and regulations for ensuring the information security of the enterprise were developed. The research results represent a significant contribution to the field of ensuring the information security of enterprises, are adapted for practical use, and can serve as a basis for further development of measures to protect against network attacks by computer viruses.

Keywords: corporate network, computer viruses, vulnerabilities, impact, specific policy, specific regulations.

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

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

Yuriy V. Makarov – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com