DOI 10.36622/VSTU.2023.26.3.019
УДК 004.056

ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЗАЩИТА ОТ СЕТЕВЫХ АТАК: МЕТОДИКИ ФОРМИРОВАНИЯ ЧАСТНЫХ ПОЛИТИК, РЕГЛАМЕНТОВ И ИНСТРУКЦИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ (ЧАСТЬ III)

Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.Ю. Егоров

Предлагается методическое обеспечение для формирования частных инструкций защиты корпоративной сети. Частные инструкции включают в себя: инструкцию администратора безопасности и инструкцию внутреннего и внешнего пользователя. Предложенная методика построения инструкции администратора безопасности определяет основные требования к его должностным обязанностям. Проработаны рекомендации в части выбора и настройки средств защиты информации, необходимых и достаточных для защиты при сетевой атаке заданного типа. Также представлен план по построению разграничительной матрицы доступа, которая позволяет обеспечить защиту от несанкционированного доступа и каких-либо преднамеренных ошибок пользователей. Представленная структура инструкции пользователя регламентирует его безопасную работу, также определяет план обучения и инструктирования, который позволит повысить грамотность пользователей в части защиты информации.

Ключевые слова: частные инструкции, сетевая атака, администратор безопасности, пользователь.

Введение

Инструкции информационной безопасности – это документы, которые предписывают детализированные шаги и действия по выполнению поставленных задач политикой информационной безопасности.

Частной политикой сетевой безопасности были определены ключевые векторы создания и развития частных инструкций сетевой безопасности. Данными инструкциями выступают: инструкция администратора информационной безопасности и инструкции внутренних и внешних пользователей.

В рамках создания инструкции администратора информационной безопасности (далее – администратор), большое внимание необходимо уделить требованиям к его функциональным знаниям и умениям в части защиты от сетевой атаки заданного типа. Только знающий и грамотно владеющий всеми тонкостями мер противостояния атакам человек может соответствовать компетенциям специалиста, который обеспечивает защиту информации в организации. Важными аспектами в работе администратора являются выбор, настройка и управление средствами защиты информации, а также – умение разграничивать доступ к защищаемым объектам. Все вышеперечисленные требования к компетенциям администратора информационной безопасности отображены в методологии построения инструкции администратора.

Также важную роль в обеспечении безопасности организации играют пользователи. Пользователи могут осуществлять свою работу как внутри организации (внутренние), так и за ее периметром (внешние). Инструкция для данных пользователей должна регламентировать их безопасную работу. В рамках обеспечения безопасной работы пользователь должен знать, какие действия ему запрещено предпринимать, чтобы не спровоцировать начало наступления сетевой атаки, а также уметь оперативно реагировать на обнаруженные аномалии на своем рабочем месте. Еще одной из главных задач инструкции – это ее обучающий характер. Пользователю необходимо регулярно проходить обучение и повышать свою грамотность в части защиты информации. Все эти меры регламентированы предложенной методологией по созданию инструкции пользователей.

Инструкция администратора

Общие положения

1. Инструкция администратора безопасности (далее – администратор) определяет основные полномочия, обязанности, функции и ответственность администратора по защите информации в организации в рамках противодействия сетевой атаке типа «…».

2. Администратор в своей работе действует согласно настоящей инструкции, частной политики сетевой безопасности, частным регламентам сетевой безопасности и документам, содержащим руководящие указания и нормативные требования, установленные ФСТЭК и ФСБ России.

3. Настоящая инструкция разработана с учетом законодательных и нормативно-правовых актов, перечисленных в частной политике сетевой безопасности и частных регламентах сетевой безопасности [1-10].

Функции и обязанности администратора

1. Администратор обязан знать (табл. 1):

Указывается перечень требований к функциональным знаниям администратора, которыми он должен обладать, чтобы успешно защитить сеть организации от различных векторов сетевой атаки типа «…».

Таблица 1

Функциональные знания администратора

Сетевая атака типа «…»	Необходимо знать
Наиболее опасные сочетания векторов атаки VA_i и уязвимостей VB_j	Сетевые протоколы: TCP, UDP, HTTP/HTTPS
	Различные инструменты мониторинга сети и обнаружения вторжений
…	…

2. Администратор должен уметь (табл. 2):

Указывается перечень требований к умениям администратора, которыми он должен владеть, чтобы успешно защищать сеть организации от векторов сетевой атаки типа «…».

Таблица 2

Требования к умениям администратора

Сетевая атака типа «…»	Необходимо уметь
Наиболее опасные сочетания векторов атаки VA_i и уязвимостей VB_j	Настраивать межсетевой экран, чтобы он эффективно отфильтровывал деструктивный трафик
	Проводить анализ журналов (логов) и другой информации для определения источников атаки и принятия мер по предотвращению повторной реализации атаки
	Работать в тесном сотрудничестве с провайдерами услуг Интернета, регуляторами и другими организациями в целях регулярного обмена актуальной информацией по инцидентам и инструментам нарушения ИБ
…	…

Полномочия администратора

Администратор имеет следующие права:

Необходимо расширить указанный ниже перечень прав администратора правами, в части отражения специфики выполнения обязанностей и обеспечения безопасности информации в организации в рамках защиты её при сетевой атаке заданного типа. При этом, нужно учесть, что все права администратора должны быть сбалансированы с правами и интересами других сотрудников организации, а также - должны соответствовать действующему законодательству в области защиты

персональных данных и конфиденциальной информации.

− право на доступ к конфиденциальной информации, необходимой для выполнения своих обязанностей, например, к информации о настройках сетевых устройств, базах данных, пользователях системы и другой конфиденциальной информации,

− право на установку и настройку средств защиты,

− право на мониторинг системы для обнаружения уязвимостей и предотвращения возможных атак,

− право на анализ данных для обнаружения аномалий и неистовой активности, которые могут быть связаны с угрозами безопасности,

− право на реагирование на инциденты нарушения безопасности и принятие мер по их устранению,

− право на участие в разработке и реализации частной политики сетевой безопасности,

− право на участие в процессе принятия решений по вопросам безопасности и на предоставление рекомендаций руководству организации,

− право на подготовку и организацию инструктажа и повышения квалификации пользователей по защите информации от сетевых атак.

Ответственность администратора

1. Администратор несет ответственность за обеспечение безопасности информации в организации в части защиты информации при сетевой атаке типа «…».

2. Администратор должен обеспечить оперативное информирование руководства организации об уровне риска, связанном с реализацией сетевой атаки типа «…», и принимаемых мерах по его снижению, также своевременно инструктировать сотрудников организации по вопросам защиты от сетевой атаки типа «…» и сотрудничать со службами организации в целях обеспечения единой политики информационной безопасности.

Автоматизированное рабочее место администратора и управление системой защиты информации

1. Одним из главных компонентов системы защиты информации от сетевой атаки типа «…» является автоматизированное рабочее место (далее – АРМ) администратора.

2. Поскольку администратор выполняет настройки безопасности, устанавливает обновления защитных инструментов, следит за конфигурацией системы и проводит периодические сканирования уязвимостей, анализирует журналы безопасности, чтобы выявлять любые нарушения и инциденты безопасности данных, то установка его АРМ должна проводиться с тщательным контролем, исключающим любые попытки взлома или утечки информации.

3. Администратор обязан следить за состоянием своего АРМ, которое должно быть оснащено передовыми средствами защиты информации, такими как антивирусы, брандмауэры, системы защиты от взломов, антишпионские программы. Причем, набор средств защиты будет зависеть от специфики сети и потенциальных угроз нарушения ее безопасности.

Установка и настройка средств защиты информации

Ключевой мерой для обеспечения безопасности при сетевой атаке типа «…» для администратора являются определение адекватных средств защиты информации (далее – СЗИ) и их настройка. Не все СЗИ одинаково эффективны при защите от сетевой атаки типа «…», поэтому необходимо установить, какое именно средство защиты соответствует заданной атаке. Кроме того, правильная настройка СЗИ является критически важным аспектом для его эффективной работы. В связи с чем, предлагается план действий для администратора, который будет учитывать шаги выбора и настройки необходимого СЗИ от сетевой атаки заданного типа:

Для реализации данного плана необходимо пользоваться рис. 1.

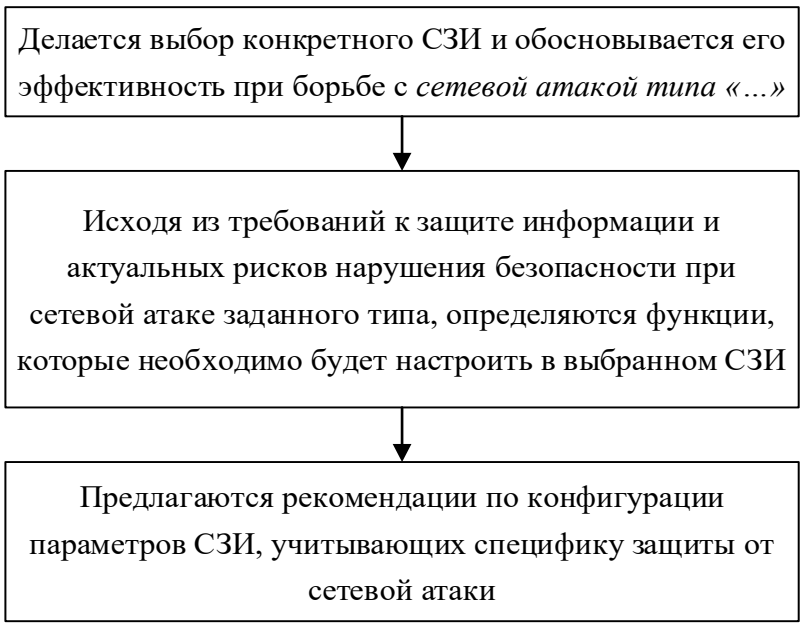

Рис. 1. Рекомендации по созданию инструкции в части выбора и настройки администратором СЗИ, необходимых и достаточных для защиты при сетевой атаке типа «…»

Пример плана действий администратора при выборе и настройке СЗИ приведен в табл. 3.

Таблица 3

Пример плана действий администратора при выборе и настройке СЗИ

Выбор наиболее опасных сочетаний векторов атаки VA_i и уязвимостей VB_j	Требование к защите информации	Выбранное СЗИ	Рекомендация по настройке параметров
$VA_i \wedge VB_j$ в части наиболее значимых рисков, определенных риск-ландшафтом рассматриваемого типа атак	Обеспечения уровня рисков на предмет не превышения заданного порога целостности	СЗИ от несанкционированного доступа «Dallas Lock 8.0»	На выбранном объекте защите включить контроль целостности и рассчитать его контрольную сумму
Администратор с помощью механизмов СЗИ от НСД Dallas Lock 8.0 производит настройку заданного параметра (рис. 2).			
…	…	…	…
…			

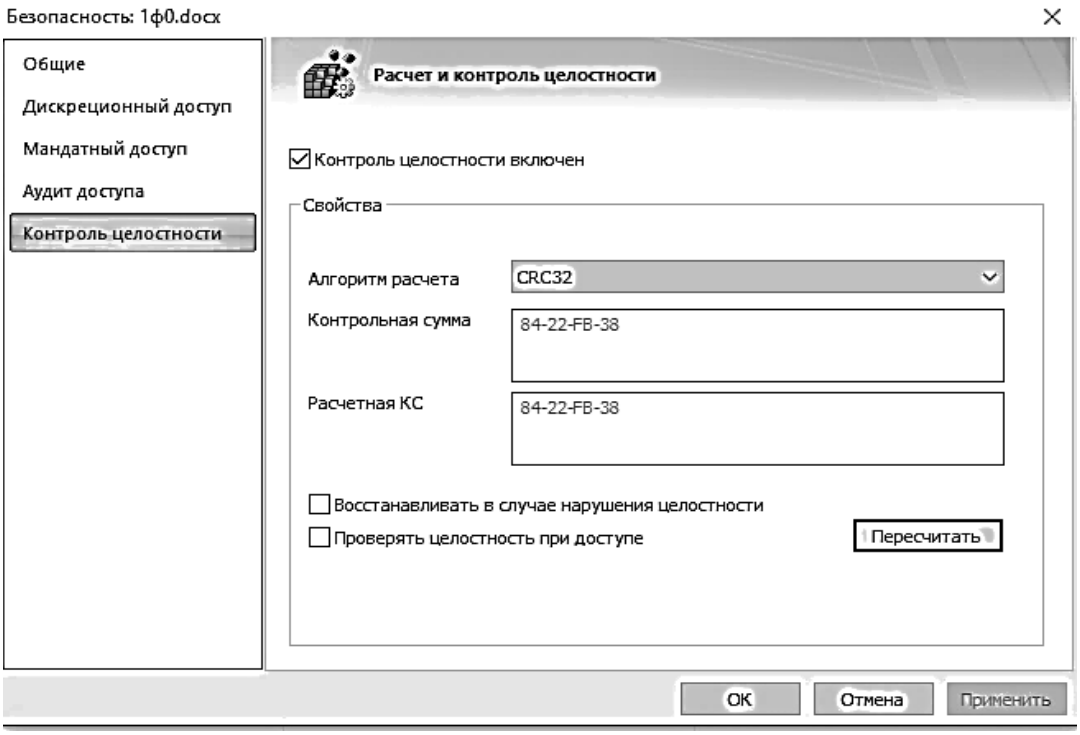

Рис. 2. Пример настройки контроля целостности в СЗИ от НСД Dallas Lock 8.0-C

Сопровождение средств защиты информации

Для того, чтобы гарантировать работоспособность средства защиты информации, администратору следует осуществлять их сопровождение:

− контролировать целостность аппаратно-программной среды СЗИ,

− периодически тестировать работу СЗИ в случае их установки на АРМ сотрудников организации, особенно после изменения программного обеспечения и полномочий пользователей,

− регулярно контролировать установку обновлений ПО СЗИ и фиксировать информацию об этом в журналах,

− восстанавливать программные настройки и средства СЗИ в случае сбоя,

− поддерживать соответствующий порядок и правила антивирусной защиты на АРМ,

− проводить регулярно инструктажи для сотрудников организации по правилам работы с используемыми СЗИ.

Разграничительная матрица доступа

1. Администратор должен разграничивать доступ к информации на уровне пользователя, определять, какую информацию каждый пользователь может видеть и редактировать, а также устанавливать правила для работы с информацией.

2. Администратор обязан устанавливать правильные привилегии для каждого пользователя в соответствии с его ролью и обязанностями в организации с учетом части защиты информации от сетевой атаки типа «…».

3. Для построения разграничительной матрицы доступа администратор должен следовать схеме, приведенной на рис. 3. После чего сформировать матрицу, пример которой приведен в табл. 4.

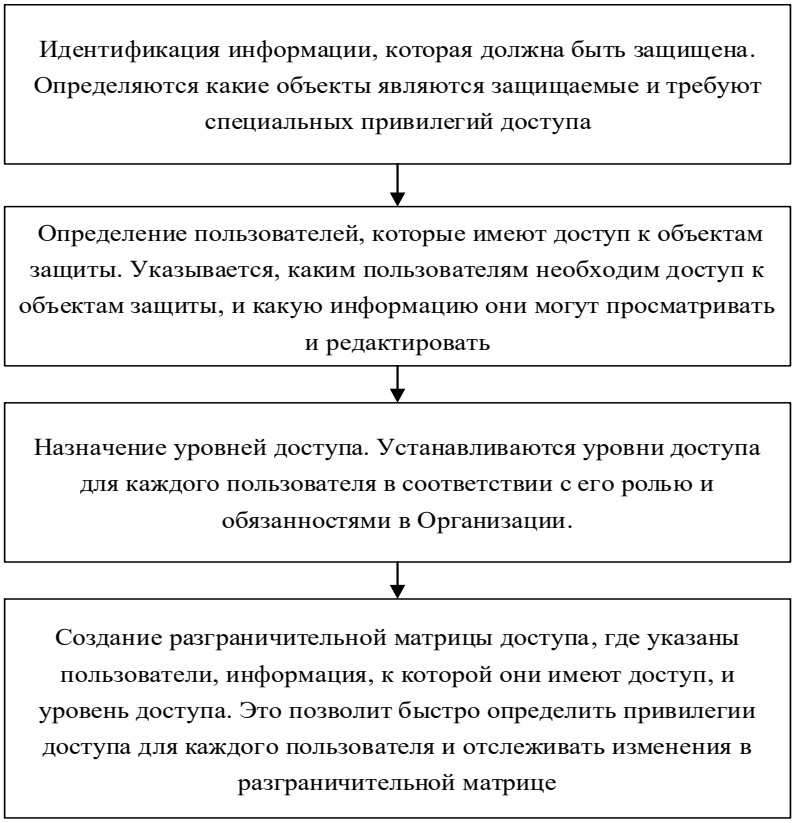

Рис. 3. Схема создания разграничительной матрицы доступа

Таблица 4

Пример разграничительной матрицы доступа

Объекты защиты	Роли пользователей		
	Администратор	Внутренний пользователь	Внешний пользователь
Сервер безопасности «Dallas Lock»	Полный доступ	Доступ запрещен	Доступ запрещен
Прикладное ПО	Полный доступ	Полный доступ	Полный доступ
…	…	…	…

4. Разграничительная матрица доступа позволяет обеспечить защиту от несанкционированного доступа к защищаемой информации, уменьшить вероятность ошибок пользователей и их злонамеренных действий, а также улучшить контроль за доступом к информации в организации.

5. Администратор должен регулярно проверять разграничительную матрицу доступа на наличие ошибок и обновлять ее в соответствии с изменениями в организации.

Рекомендации по работе с инцидентами нарушения безопасности

1. В случае возникновения инцидента нарушения безопасности, администратор должен быстро и точно действовать, чтобы минимизировать ущерб. Если он не знает, как управлять возникшим инцидентом, то организация, подвергшаяся атаке, может понести значительные потери. Недостаточная эффективность реагирования на инциденты безопасности может способствовать достижению целей злоумышленников и обеспечить им возможность успешного удаления следов присутствия в информационной системе.

2. Для формализации действий сотрудников, ответственных за безопасность, были сформированы регламенты по управлению инцидентами, но для безошибочного выполнения этих шагов необходимо иметь инструкцию по регулированию инцидентов нарушения безопасности. В связи с чем для администратора разработаны рекомендации по управлению инцидентами при реализации сетевой атаки типа «...», представленные ниже.

Инструкция действий администратору безопасности по управлению инцидентами при обеспечении сетевой безопасности

I. Действия на этапе подготовки по управлению инцидентом

1. Назначить группу лиц, ответственную за управление инцидентами.

2. Установить рабочие контакты с внутренней командой, ответственной за управление инцидентами.

3. Выработать процедуры по управлению инцидентами.

4. Собрать необходимую информацию и ознакомиться с доступными системами обнаружения угроз безопасности для оптимизации временных затрат на момент инцидента.

5. Убедиться в дееспособном функциональном и актуализированном состоянии специализированных средств мониторинга и анализа, антивирусов, IDS и т. п.

6. Формализовать процесс уведомлений об обнаружении инцидента.

7. Убедиться в наличии актуализованной версии картографии сети и инвентаря аппаратного оборудования.

8. Выполнять регулярный мониторинг безопасности и своевременно информировать ответственных лиц о направлениях угрозы.

9. Убедиться в существовании формализованных и регулярно тестируемых процессов непрерывности функционирования организации.

II.Действия на этапе обнаружения и регистрации инцидента

Цель этапа - вовремя обнаружить инцидент и определить затрагиваемый периметр инфраструктуры организации.

1. Собрать, проанализировать и упорядочить информацию, поступающую из различных источников. Возможными источниками обнаружения могут выступать:

• уведомление пользователей/рабочей группы;

• IDS:

• DLP;

• жалобы из внешнего источника и т. п.

2. Провести анализ сетевой атаки заданного типа:

• проанализировать поступившие оповещения;

• просмотреть статистику логов и сетевых устройств;

• постараться определить цели вектора атаки и затронутые компоненты инфраструктуры.

3. Определить уровень критичности и приоритет инцидента.

III. Действия на этапе реагирования на инцидент

Принять меры для пресечения инцидента, вызванного сетевой атакой заданного типа.

1. Используя ранее выполненные результаты аналитических действий по обнаружению и локализации угрозы, идентифицировать источник инцидента, используемый атакующей стороной, и заблокировать его.

2. Применить меры по регулированию инцидента, которые были ранее определены, исходя от типа сетевой атаки.

3. Перед применением мер необходимо протестировать их для того, чтобы убедиться, что процесс работает корректно и эффективно.

IV. Действия на этапе ликвидация последствий инцидента

1. Формализовать процесс ликвидации последствий инцидента.

2. Протестировать меры ликвидации последствий инцидента. Убедиться, что они работают корректно и не ставят под угрозу никакие процессы организации.

3. Применить процессы ликвидации последствий инцидента после получения одобрения результатов тестов.

4. Вернуться к нормальному режиму работы системы.

Инструкция внутреннего и внешнего пользователя

Общие положения

1. Инструкция внутреннего и внешнего пользователя (далее – инструкция) определяет обязанности и перечень требований к безопасной работе пользователя в части защиты информации в организации в рамках противодействия сетевой атаке типа «…».

2. Пользователь в своей работе действует согласно настоящей инструкции.

3. Настоящая инструкция разработана с учетом законодательных и нормативно-правовых актов, определенных в частной политике сетевой безопасности и частных регламентах сетевой безопасности.

Обязанности пользователя по защите информации в организации

1. Пользователь, должен осуществлять только те действия, которые регламентированы его трудовыми обязанностями. Любые посторонние действия строго запрещены.

2. Пользователь перед началом работы с информацией ограниченного доступа обязан подписать соглашение о ее неразглашении.

3. Пользователь должен незамедлительно уведомлять администратора безопасности о любых подозрительных действиях.

4. Пользователь не должен использовать оборудование организации для личных целей.

5. Пользователь обязан участвовать в инструктажах по информационной безопасности, изучать полученные материалы и совершенствовать свои знания в области защиты информации.

6. Пользователю запрещается производить любые работы на автоматизированном рабочем месте, пока он не пройдет идентификацию и аутентификацию.

7. Пользователь не может самостоятельно устанавливать/удалять и изменять настройки ПО на своем АРМ. Установка разрешенного ПО может быть выполнена только администратором безопасности или системными администраторами.

8. Пользователь должен препятствовать любым попыткам несанкционированного доступа к его учетным данным, конфиденциальной информации, ключевой информации криптосредства и другой защищаемой информации.

Ответственность пользователей

Пользователь несет ответственность за соблюдение положений настоящей инструкции и других локально-нормативных документов организации. В случае нарушения пользователем требований по защите информации, он может быть уволен и/или привлечен к ответственности в соответствии с действующим законодательством и внутренними правилами организации.

Требования к безопасной работе пользователя

1. Чтобы не допустить реализацию сетевой атаки типа «…» пользователю запрещается:

Здесь указывается список рекомендаций для пользователя, описывающий действия, которые он не должен совершать, чтобы не спровоцировать начало сетевой атаки типа «…». Например:

− направлять конфиденциальную информацию не через защищенный канал;

− отвечать на подозрительные сообщения и электронные письма, которые могут содержать вредоносный код или фишинговые ссылки.

2. В случае, если пользователь заметил какие-либо аномалии в системе, он незамедлительно должен сообщить о них администратору безопасности. Данными аномалиями могут выступать:

Здесь, с учетом специфики сетевой атаки заданного типа, необходимо привести список аномалий, на которые пользователь может ориентироваться и незамедлительно среагировать. Например:

− недоступность информационной

системы или отдельных ее ресурсов, которые обычно доступны и функционируют нормально;

− неожиданное поведение компьютера или программного обеспечения, которое не было замечено ранее, такое как медленная работа, частые сбои и ошибки;

− появление новых файлов или программ на компьютере, которые не были установлены пользователем и не являются частью обычных рабочих процессов;

− появление всплывающих окон, рекламы и других подозрительных сообщений, которые могут содержать вредоносный код;

− зашифрованные файлы или письма, которые появляются без уведомления пользователя, что может свидетельствовать о шифровании данных злоумышленником.

Обучение и инструктирование пользователя

В целях повышения защищенности системы и противодействия сетевой атаке типа «…» пользователю необходимо пройти обучение, которое будет включать в себя:

Здесь указывается план мероприятия по обучению пользователей в части просвещения и защиты от сетевой атаки типа «…». Это обучение должно предоставить пользователям понимание особенностей заданного типа сетевых атак, умение их распознавать и рекомендации по предотвращению ошибок, которые могут способствовать началу атаки. В результате обучения пользователи должны получить необходимые знания и навыки для эффективного противодействия указанной сетевой атаке.

Требования к внешнему пользователю в части обеспечения безопасности устройств для удаленного доступа

1. Многие внешние пользователи, находящиеся за периметром организации, так же, как и внутренние, получают доступ к непубличной информации. Следовательно, если устройство для удаленной работы внешнего пользователя не защищено должным образом, то оно также может подвергаться сетевым атакам различного типа, что создает дополнительный риск не только для информации, к которой получает доступ пользователь, но и для других систем и сетей организации.

2. Внешний пользователь также должен следовать требованиям и рекомендациям организации по защите информации, определенных данной инструкцией.

3. В своей работе внешний пользователь может использовать различные устройства для удаленной работы, такие как компьютеры, смартфоны и планшеты. В связи с чем возникает необходимость выполнять следующие рекомендации по обеспечению безопасности своих устройств для удаленной работы, чтобы поддерживать необходимый и достаточный уровень защиты информации в организации:

1. Пользователь должен осуществлять подключение к ресурсам организации только с помощью использования следующих методов:

− виртуальной частной сети (VPN);

− интернет-протокола (IPsec) VPN;

− защищенных сокетов (SSL) VPN;

− дистанционного управления системой.

2. Пользователь, прежде чем получить доступ к ресурсам организации, должен пройти многократную аутентификацию, а также периодически проходить повторную аутентификацию во время длительных сеансов удаленного доступа.

3. Пользователю необходимо обеспечить надлежащим образом защиту своих средств проверки подлинности для удаленного доступа, таких как пароли, личные идентификационные номера (PIN) и аппаратные токены. Такие аутентификаторы не должны храниться вместе с устройством удаленной работы, а также не должны храниться вместе.

4. Пользователь должен использовать устройства для удаленного доступа исключительно приобретенные, настроенные и управляемые организацией.

5. Пользователь не должен оставлять без присмотра устройства для удаленной работы.

6. Пользователь должен осуществлять шифрование файлов, хранящихся на устройствах удаленной работы и съемных носителях

7. Пользователь должен выполнять резервное копирование в соответствии с

рекомендациями организации и проверять правильность и полноту резервных копий. Важно, чтобы резервные копии на съемных носителях были защищены так же, как и устройство, для которого они были созданы.

8. Пользователь обеспечивает уничтожение информации, выполняя базовую очистку информации. Он должен очищать кеши веб-браузера, которые могут непреднамеренно содержать конфиденциальную информацию, а также обязательно использовать специальные утилиты для затирания данных, которые обеспечивают удаление всех следов информации с устройства.

9. Если пользователь подозревает, что произошло нарушение безопасности (включая потерю или кражу материалов) с использованием устройства удаленной работы, средств удаленного доступа, съемных носителей или других компонентов удаленной работы, то пользователь должен незамедлительно сообщить организации для сообщения о возможном нарушении.

10. Пользователь должен обеспечить надлежащую защиту всех устройств в своих домашних сетях, к которым обычно подключаются устройства удаленной работы. Важным компонентом безопасности домашней сети является защита других компьютеров и мобильных устройств. Если какое-либо из этих устройств будет подвергнуто сетевой атакой или иным образом скомпрометировано, они могут быть использованы для атаки на устройство удаленной работы или прослушивания его сообщений. Для этого необходимо между интернет-провайдером и удаленным устройством установить устройство безопасности. Это защитное устройство должно быть настроено так, чтобы компьютеры за пределами домашней сети не могли инициировать связь с любым из устройств в домашней сети, включая устройство удаленной работы.

11. Пользователи должны защищать свои беспроводные домашние сети, следуя рекомендациям по безопасности из документации по беспроводной точке доступа домашней сети.

Противодействие социальной инженерии

1) Пользователь должен уметь справляться с угрозами, связанными с социальной инженерией, когда злоумышленник пытается обманом заставить его раскрыть конфиденциальную информацию или произвести определенные действия, такие как загрузка и выполнение файлов, которые кажутся безопасными, но на самом деле являются вредоносными.

2) Пользователь должен с осторожностью относиться к любым получаемым запросам, которые могут привести к нарушению безопасности или краже информации.

3) Пользователь должен предотвращать все возможные инциденты, связанные с социальной инженерией, для чего необходимо изучить и выполнять рекомендации по регулированию данного инцидента, представленные ниже.

Рекомендации пользователю по борьбе с инцидентом социальной инженерии

I. Подготовка

1. Подготовиться к ведению диалога со злоумышленниками с целью выявления природы собираемой информации, целей атаки и идентификации атакующей стороны.

2. Отработать план по переадресации подозрительный входящих звонков писем на специально организованную группу «Социальная инженерия». Сотрудники данной группы легко могут идентифицировать возникающие атаки.

3. Совершенствовать свои знания по проблематике данного типа инцидента. Повышение уровня осведомленности возможно посредством изучения специальных информационных программ и семинаров.

II. Обнаружение

1. Если злоумышленник действует через телефонный звонок, то:

• внимательно выслушайте суть запросов звонящих и попросите их контактные данные для того, чтобы связаться ними «после уточнения информации по их запросам». Если есть возможность вовлечь звонящих в двусторонний диалог, постарайтесь

уточнить: имя звонящего, использование профессионального сленга, знания об атакуемой организации;

• на любую запрашиваемую информацию, входящую в область интересов конкурентов, ответить отказом. После выполнения данных действий следовать фазе «Реагирование».

2. Если злоумышленник действует через e-mail: подозрительные письма с ссылками или вложениями, получение неавторизованных запросов на разглашение конфиденциальной информации, то необходимо уведомить руководство об атаке методами социальной инженерии.

III. Реагирование

До перехода к данной фазе вы должны удостовериться в том, что имеете дело именно с социальной инженерией.

1. Телефонный звонок: необходимо немедленно связаться с группой «Социальная инженерия», передать суть инцидента и характер запрашиваемой злоумышленниками информации.

2. E-mail: необходимо переадресовать сообщение вместе со служебными заголовками группе «Социальная инженерия» для расследования профайлинга и геолокализации злоумышленника.

IV. Ликвидация

1. Оповестить/подать жалобу в правоохранительные органы.

2. Обсудить инцидент и обменяться опытом с коллегами.

3. Пригрозить злоумышленнику применением юридических методов воздействия.

V. Восстановление

1. Проинформировать руководство об инциденте.

2. Оповестить о принятых решениях, совершенных действиях и их результатах

Пример применения предложенной методики

В качестве иллюстрации вышеизложенного для организации, опасающейся атак троянскими программами, ниже предлагаются меры коррекции инструкций обеспечения информационной безопасности для отражения различных векторов атаки (табл. 5).

Таблица 5

Компетенции администратора безопасности, необходимые при защите от сетевой атаки

Администратор безопасности должен обладать знаниями о	Администратор безопасности должен владеть навыками
Письмо с вложенным троянцем	
Методах анализа содержимого писем для автоматического обнаружения и блокирования вредоносных вложений.	Фильтрации и сортировки спам-писем.
Способах фильтрации писем встроенными почтовыми службами.	Фильтрации почты для автоматического обнаружения и блокировки вредоносных вложений или писем.
Создании и ведении политики безопасности пользователей, а также установке групповой политики и ограничении прав пользователей.	Настройки политики безопасности почтового сервера.
Доверительный архив	
Настройке межсетевого экрана и системе обнаружения вторжений	Использования специализированных инструментов сканирования уязвимостей, такие как Nessus, OpenVAS, Acunetix.
Специализированных инструментах сканирования сетевой инфраструктуры.	Фильтрации почты для автоматического обнаружения и блокировки вредоносных вложений или писем.
Архитектуре, используемой в системе и циркулировании в ней трафика.	Мониторинга трафика и выявлениия подозрительного сетевого трафика.

Продолжение табл.5

Администратор безопасности должен обладать знаниями о	Администратор безопасности должен владеть навыками
Троян-антивирус	
Инструментах обеспечения безопасности АРМ.	Установки с официального сайта лицензионного антивирусного ПО и поддержания его в актуальном состоянии.
Управлении настройками безопасности, политиками доступа и правами пользователей.	Разграничения прав пользователей с использованием групповой политики для запрета установки сторонних программ.
Аппаратный кейлоггер	
Протоколах: TCP/IP, UDP, ICMP, структуре сети, включая сегменты сети, IP-адреса, подсети, маршрутизации.	Настройки межсетевого экрана по контролю входящего и исходящего сетевого трафика.
USB-носителях в системе.	Разработки правил использования USB-носителей в системе.
Методах фильтрации трафика на сетевом уровне.	Настройки мониторинга и аудита для отслеживания подключаемых USB-носителей и проверки их соответствие списку доверенных устройств.
Настройке системы мониторинга подключаемых устройств.	
Внедрение вредоносного скрипта скрытой загрузки	
Механизмах преобразования сетевых адресов (NAT) и безопасного подключения к сети интернет (VPN).	Установки обновлений безопасности для операционной системы и программного обеспечения.
Унаследованных приложениях и поддержке в актуальном состоянии рабочих приложений.	Выведения из эксплуатации не актуального или устаревшего программного обеспечения, плагинов, расширений для браузеров, которые уязвимы для атак.
Настройках фильтрации пакетов, анализ заголовков в межсетевом экране.	Установки и настройки FireWall или системы обнаружения вторжений на сетевом уровне.
Троян-шифровальщик	
Создании резервных копий всех важных данных на отдельном носителе или в облачном хранилище.	Создания резервных копий всех важных данных на отдельном носителе или в облачном хранилище.
Работе антивирусного ПО.	Поддержки антивирусного ПО в актуальном состоянии
Особенностях инструкции безопасности пользователей.	Создания политик безопасности для ограничения загрузки и запуска программ без необходимых разрешений.
Принципах работы системы мониторинга загрузки системы.	Мониторинга загрузки процессора.

Заключение

Поскольку частной политикой были заданы принципы работы с инцидентами нарушения безопасности, а частные регламенты установили порядок и правила осуществления данной деятельности, то для администратора была разработана инструкция, описывающая шаги и действий по управлению инцидентами при обеспечении сетевой безопасности.

Кроме инструкции администратора информационной безопасности была разработана инструкция для внутренних и внешних пользователей. Рядовые сотрудники играют немаловажную роль в обеспечении безопасности организации, в связи с чем для пользователей были подготовлены требования и правила для борьбы с сетевыми атаками, а также обозначена необходимость прохождения обучения по направлению защиты организации от сетевых атак. Также созданы рекомендации пользователю по борьбе с инцидентом социальной инженерии.

Список литературы

1. ГОСТ Р ИСО/МЭК 27001:2021. Информационная технология. Системы менеджмента информационной безопасности. Требования. URL: https://docs.cntd.ru/document/1200181890 (дата обращения: 1.09.2023).

2. ГОСТ Р ИСО/МЭК 27002:2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. URL: https://docs.cntd.ru/document/1200179669 (дата обращения: 1.09.2023).

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 1.09.2023).

4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 1.09.2023).

5. Методический документ от 05.02.2021 ФСТЭК России. Методика оценки угроз безопасности информации. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 1.09.2023).

6. ГОСТ Р 59709-2022. Защита информации. Управление компьютерными инцидентами. Термины и определения. URL: https://docs.cntd.ru/document/1200194355 (дата обращения: 1.09.2023).

7. ГОСТ Р 59710-2022. Защита информации. Управление компьютерными инцидентами. Общие положения. URL: https://docs.cntd.ru/document/1200194356 (дата обращения: 1.09.2023).

8. ГОСТ Р 59711-2022. Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами. URL: https://docs.cntd.ru/document/1200194357 (дата обращения: 1.09.2023).

9. ГОСТ Р 59712-2022. Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты. URL: https://docs.cntd.ru/document/1200194358 (дата обращения: 1.09.2023).

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 4.09.2023

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, проректор, Финансовый университет 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 – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

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

Егоров Анатолий Юрьевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

ORGANIZATIONAL AND LEGAL PROTECTION AGAINST NETWORK ATTACKS: METHODS FOR FORMING PRIVATE POLICIES, REGULATIONS AND INSTRUCTIONS TO ENSURE ORGANIZATION SECURITY (PART III)

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

Proposed methodological support for the formation of private instructions for the protection of the corporate network. Private instructions include: security administrator instruction and internal and external user instruction. The proposed methodology for constructing instructions for a security administrator defines the basic requirements for his job responsibilities. Recommendations have been worked out regarding the selection and configuration of information protection tools that are necessary and sufficient to protect against a network attack of a given type. A plan is also presented for building a delimiting access matrix, which allows you to provide protection against unauthorized access and any deliberate user errors. The presented structure of the user manual regulates its safe operation, and also defines a training and instruction plan that will increase the literacy of users in terms of information protection.

Keywords: private instructions, network attack, security administrator, user.

Submitted 4.09.2023

Information about the authors

Grigory A. Ostapenko – Dr. Sc. (Technical), Vice-Rector, 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 – graduate student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

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

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