DOI 10.36622/VSTU.2023.26.3.017
УДК 004.056

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

Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.С. Кривошеин

Предлагается методическое обеспечение для формирования частных политик защиты корпоративной сети. Представляемая методология построения частной политики разрабатывается на основании лучших практик и рекомендаций в области информационной безопасности, также учитывает окна, позволяющие адаптировать частную политику под специфику различных атак. Частная политика определяет основные цели и задачи организации в части противодействия сетевым атакам, задает основное направление в развитии структуры взаимоувязанных документов, таких как частные регламенты и инструкции сетевой безопасности. Разрабатывается план по формированию перечня мероприятий, включающий в себя требования и меры по защите информации с учетом специфики сетевой атаки. Производится разграничение зон ответственности по вопросам обеспечения безопасности должностных лиц и описываются методы и средства контроля за реализацией требований, определенных частной политикой.

Ключевые слова: частная политика, сетевая атака, меры защиты, объекты защиты, модель нарушителя.

Введение

Политика информационной безопасности (далее – политика) – это базовый документ организации, который устанавливает основные направления и взгляды на обеспечение ее безопасности. Данный документ должен соответствовать всем требованиям и рекомендациям в области защиты информации, предъявляемые законодательством и регуляторами.

Целью создания политики является установление определенных принципов, которые помогут обеспечить и управлять информационной безопасностью организации и защитить ее корпоративные сети от возникающих рисков и угроз.

Создание политики является одним из важных этапов защиты информации любой организации. Однако, многие ошибочно считают, что для достаточного уровня обеспечения безопасности, можно принимать готовые рекомендации или шаблоны политик без учета уникальных особенностей организации. Также, встречающиеся политики очень часто разработаны без учета актуальных требований. Данный пример показывает необходимость проведения исследований различных политик, выявления в них достоинств и недостатков для того, чтобы в дальнейшем принять только лучшие практики.

В нормативно-правовом поле существует множество стандартов, которые регламентируют создание политики [1-4]. Но ни в одном из стандартов не содержатся рекомендации по созданию политики в части защиты от конкретных видов сетевых атак. Поэтому, в связи с постоянным ростом сетевых атак, отсутствием реальных практик по разработке политики информационной безопасности в части защиты от сетевой атаки заданного типа, возникает необходимость разработать методологию создания частной политики обеспечения сетевой безопасности (далее – частная политика).

Частная политика будет выступать руководящим документом в организации в части обеспечения информационной безопасности от реализации сетевой атаки заданного типа. Представляемая методология построения частной политики, разрабатывается на основании лучших практик и рекомендаций, также учитывает окна, позволяющие адаптировать частную

политику под специфику различных атак. Еще одним преимуществом данной частной политики является то, что она сформирована как готовый документ.

Общие положения

1. Частная политика разработана в целях обеспечения безопасности корпоративной сети (далее – КС) - совокупности правил, процедур, регламентов и инструкций в области информационной безопасности (далее – ИБ), которыми руководствуется организация в деятельности при защите информации от сетевой атаки типа «…».

2. Для реализации частной политики создается взаимоувязанная структура документов. Все разрабатываемые и обновляемые документы, связанные с деятельностью в части обеспечения ИБ, структурируются по трехуровневой иерархической модели, от общих положений первого верхнего уровня до третьего нижнего уровня структуры частной политики (рис. 1).

Рис. 1. Трехуровневая иерархическая модель документов, связанная с деятельностью по обеспечению ИБ

Документы первого (верхнего) уровня содержат основополагающие положения частной политики и определяют: высокоуровневые цели и задачи организации по обеспечению ИБ в части защиты от сетевой атаки типа «…», содержание и основные направления деятельности организации по обеспечению ИБ, состав и краткую характеристику основных объектов защиты, организационную структуру системы ИБ, способы контроля реализации политики ИБ.

Документы второго, третьего уровня представлены локальными организационно-правовыми документами организации (регламенты и инструкции), определяющими:

− требования и рекомендации по применению процедур по обеспечению ИБ;

− правила и параметры выполнения процедур по обеспечению ИБ (порядок выполнения действий или операций);

− регламентацию вопросов обеспечения ИБ при выполнении организацией конкретных технологических процессов (реализации детально направленных мер и мероприятий по защите информации в рамках противодействия сетевой атаки типа «…»);

− регламентацию деятельности лиц или подразделений, ответственных за вопросы обеспечения ИБ.

3. Частная политика является основным документом организации, регулирующим отношения, связанные с обеспечением сетевой безопасности в рамках противодействия сетевой атаке типа «…».

4. Требования частной политики распространяются на все объекты защиты организации, ответственность за обеспечение которых возложена на организацию.

5. Все организационные и технические требования по реализации защиты организации от сетевой атаки типа «…», определенные частной политикой, формируются на основании риск-ландшафта, угроз нарушения ИБ.

6. Частная политика предназначена для сотрудников организации, на которых возложено решение задач обеспечения

безопасности информации при сетевой атаке типа «…».

Цели и задачи частной политики обеспечения сетевой безопасности

1. Частная политика направлена на достижение следующих целей:

– внедрение комплексного подхода к обеспечению безопасности организации при защите от сетевой атаки типа «…»;

– внедрение согласованной и взаимосвязанной системы документов по обеспечению ИБ в части противодействия сетевой атаке типа «…»;

– создание системы защиты информации для объектов защиты КС, реализации мер защиты информации;

– внедрение единых правил (регламентов и инструкций) деятельности лиц или подразделений, ответственных за вопросы обеспечения ИБ;

– создание системы мер по контролю за реализацией требований определенных частной политикой.

2. Задачами частной политики являются:

– определение основных типовых объектов защиты организации;

– определение основных направлений деятельности организации по обеспечению ИБ;

– определение зон ответственности по вопросам обеспечения ИБ должностных лиц или подразделений объектов защиты;

– определение регламентов и инструкций, позволяющих упорядочить процессы деятельности по защите информации;

– определение методов и средств контроля за реализацией требований, определенных частной политикой.

3. Для обеспечения защиты информации в организации в части противодействия сетевой атаке типа «…» необходимо опираться на следующие концептуальные аспекты:

− соблюдение законности при обработке информации конфиденциального характера, а также при реализации мер по обеспечению безопасности на объектах защиты КС;

− соответствие мер по защите информации нормативным и правовым требованиям в области обеспечения ИБ;

− построение риск-ландшафта с целью выявления наиболее опасных сочетаний сценариев атак и уязвимостей;

− адаптация мер по защите информации к актуальным угрозам и потенциальным нарушителям безопасности информации на объектах защиты КС;

− использование комплексных подходов к обеспечению ИБ, учитывающих различные нормативные требования;

− применение достаточных мер защиты информации, включая экономически целесообразные дополнительные и компенсирующие меры;

− своевременное реагирование на компьютерные инциденты безопасности и применение процедур по анализу и прогнозированию вероятных атак;

− обнаружение дополнительных факторов, которые могут повлиять на уровень обеспечения ИБ;

− непрерывность и преемственность мероприятий по обеспечению безопасности информации;

− проведение мероприятий по повышению осведомленности сотрудников организации о способах и методах защиты информации, методиках проведения атак потенциальными нарушителями.

Нормативно-правовое обеспечение

При организации и обеспечении работ по созданию частной политики могут быть использованы следующие нормативно-правовые источники и стандарты [1-10].

Информация, необходимая для построения плана мероприятий по обеспечению безопасности организации

Для того, чтобы разработать план мероприятий по обеспечению безопасности организации в части противодействия сетевой атаки типа «…» необходимо учитывать:

− объекты защиты для выделенных сценариев атаки (табл. 1):

Таблица 1

Объекты защиты

Идентификатор объекта защиты	Сценарий атаки	Объект защиты
O_1	VA_1	Файловая система
O_2	VA_2	Операционная системы
O_n	…	…

− модель нарушителя (табл. 2), которая формируется из следующих пунктов:

1) тип нарушителя, т.е. классификацию лица, которое совершает нарушение безопасности информации. Например:

− хакеры - это нарушители, которые специализируются на взломе систем и сетей, чтобы получить несанкционированный доступ к конфиденциальной информации или причинить иной ущерб атакуемой сети;

− киберпреступники - это нарушители, которые используют компьютеры и сети для совершения различных преступлений, таких как мошенничество, кража личных данных, кибершпионаж и др.;

− социальные инженеры - это нарушители, которые используют социальные навыки и манипуляцию, чтобы получить доступ к конфиденциальной информации;

2) мотивацию и цели нарушителя, т.е. внутренние или внешние факторы, которые побуждают нарушителя к совершению сетевой атаки типа «…», определяемые по наиболее опасным сочетаниям вектора атаки VA_i и уязвимостей VB_j.;

3) способ реализации, который нарушитель использует для сетевой атаки типа «…», определяется по наиболее опасным сочетаниям вектора атаки VA_i и уязвимостей VB_j.

Таблица 2

Модель нарушителя

Идентификатор нарушителя	Тип нарушителя	Способ реализации		Мотивация и цели нарушителя
		Сценарий атаки	Уязвимость	
M_1	Разработчик программных, программно-аппаратных средств	VA_1	CWE-XX	Цель нарушителя, находясь вне зоны сетевой инфраструктуры организации, получить доступ к любым компонентам организации, чтобы использовать их как основу для дальнейших действий
		При удаленной атаке могут быть использованы уязвимости компонент организации. Например, эксплуатируя уязвимости веб-сервера, нарушитель может выполнить произвольный код на этом сервере		
M_n	…	…		…

Требования и меры по защите информации в организации с учетом специфики сетевой атаки заданного типа

Перечень мероприятий по обеспечению безопасности организации при сетевой атаке типа «…» представляется в виде табл. 3.

Формируется перечень мероприятий, включающий в себя требования и меры по защите информации с учетом специфики сетевой атаки типа «…».

Для того, чтобы данный перечень был направлен исключительно на заданный тип атаки и отвечал всем параметрам безопасности, при его формировании необходимо выполнять этапы, указанные на рис. 2.

Таблица 3

Меры защиты информации в организации при сетевой атаке типа «…»

Последовательность и содержание действий злоумышленника в целях реализации сценариев атаки типа «…»	Меры защиты организации от сетевой атаки типа «…», адекватные действиям злоумышленника по каждому сценарию
Полное наименование рассматриваемого вектора атаки VA_1	
1.1 …	1.1 …
1.2 …	1.2 …
…	…
Полное наименование рассматриваемого вектора атаки VA_2	
…	…

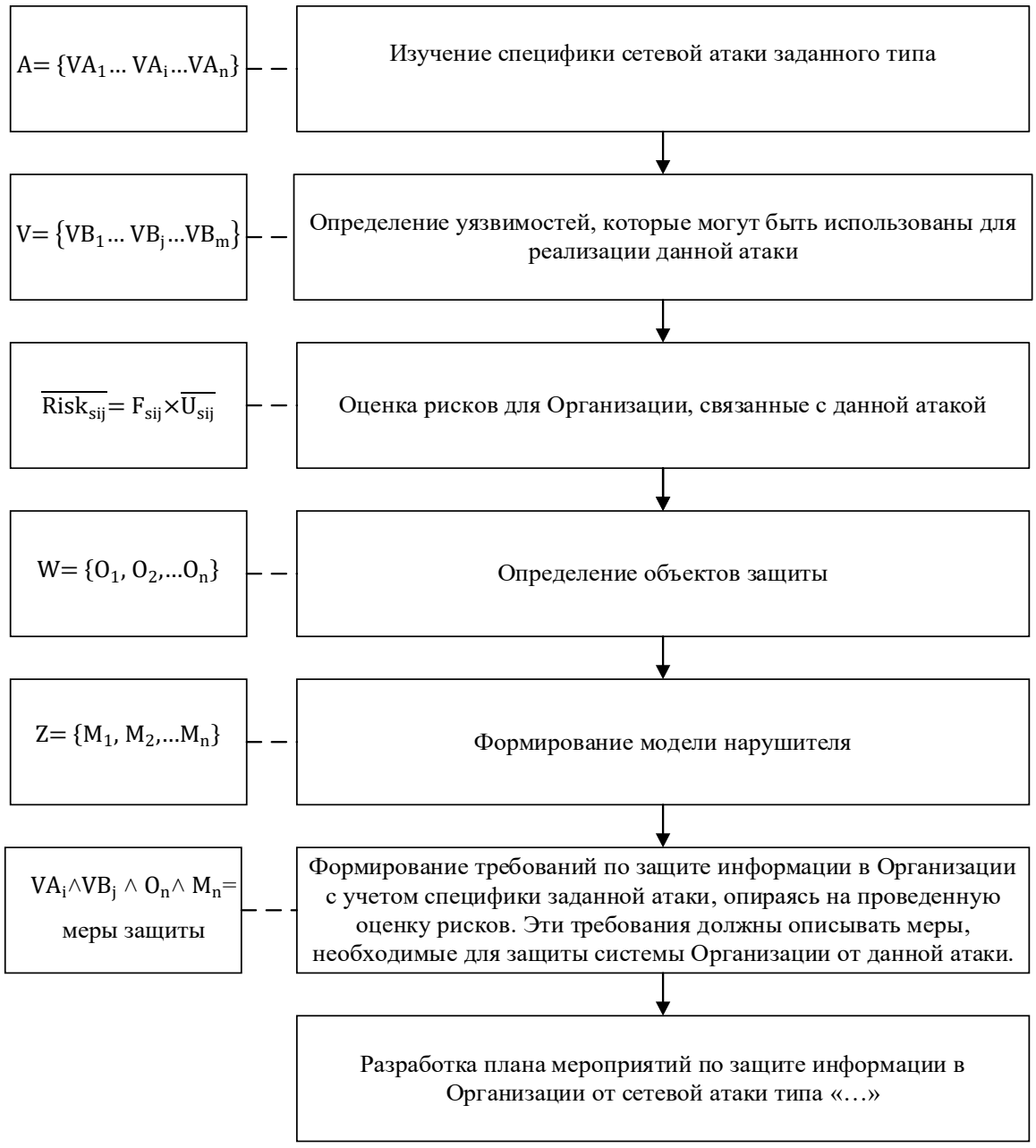

Рис. 2. План формирования мероприятий по обеспечению безопасности организации от сетевой атаки типа «…»

Документы, регламентирующие выполнение процедур по обеспечению безопасности организации

1. Частная политика безопасности с определенными мерами не может гарантировать полную защиту организации. Наличие уязвимостей в системе защиты может сделать ее неэффективной, а значит, возможны инциденты нарушения безопасности, отрицательно сказывающиеся на деятельности организации. К тому же, всегда будут возникать новые угрозы и риски, которые ранее не были идентифицированы или неизвестны. Если организация недостаточно подготовлена к обнаружению и реагированию в отношении инцидентов нарушения ИБ, это может увеличить степень ущерба негативного воздействия на КС. Поэтому важно учитывать эти риски и создавать Регламенты, которые позволят своевременно обнаруживать и адекватно реагировать на инциденты безопасности, а также оперативно ликвидировать последствия их наступления.

2. В рамках реализации положений, развития и детализации настоящей частной политики в зависимости от специфики сетевой атаки типа «…» разрабатываются и применяются следующие регламенты:

− регламент обнаружения и регистрации инцидентов нарушения сетевой безопасности организации;

− регламент реагирования на инциденты нарушения сетевой безопасности организации;

− регламент ликвидации последствий инцидентов нарушения сетевой безопасности организации.

Документы, устанавливающие требования к сотрудникам организации

1. Использование документов, которые устанавливают требования к знаниям и навыкам сотрудников в области защиты от сетевой атаки типа «…» и правилам безопасной работы в организации, является необходимым элементом обеспечения её безопасности. Такие документы представляют собой инструкции, которые помогают обучить сотрудников организации правилам обеспечения безопасности и нивелировать возможные угрозы, связанные с сетевой атакой типа «…». Они помогают создать единые правила в организации, что в свою очередь способствует повышению уровня защиты информации и снижению рисков. В целом, использование инструкций является важным элементом обучения безопасности в организации.

2. В рамках противодействия сетевой атаке типа «…» разрабатываются и внедряются в организации инструкции следующих видов:

− инструкция администратора;

− инструкция внутреннего и внешнего пользователя;

Определение общих ролей и обязанностей, связанных с обеспечением информационной безопасности в организации

1. Организационная структура системы обеспечения информационной безопасности организации представлена в табл. 4, где указывается перечень должностных лиц с их функциональными обязанностями в части противодействия сетевой атаке типа «…».

Таблица 4

Организационная структура системы обеспечения информационной безопасности организации

Сценарии атаки	Должностные лица	
	Администратор безопасности	Системный администратор
VA_1	Должен контролировать доступ к веб-серверу, используя фильтры IP-адресов, пароли, аутентификацию и другие механизмы обеспечения безопасности	Должны установить патчи для устранения уязвимостей, если они доступны. Патчи могут быть предоставлены производителем веб-сервера или известными поставщиками средств обеспечения безопасности
VA_i	…	…

Также в структуру организационной системы обеспечения информационной безопасности КС могут входить, например:

− инженеры безопасности - это сотрудники, которые занимаются разработкой и тестированием систем безопасности и их компонентов;

− этичные хакеры - это специалисты, которые занимаются тестированием на проникновение и анализом уязвимостей в целях обеспечения безопасности информации;

− сотрудники службы поддержки - это сотрудники, которые занимаются технической поддержкой пользователей и помогают им обеспечивать безопасность информации в рамках организации;

– сотрудники привлекаемых специализированных организаций – лицензиатов, осуществляющих мероприятия по установке, настройке и вводу в эксплуатацию средств защиты информации, а также - по аудиту и оценке соответствия требованиям безопасности объектов защиты организации.

2. Общее руководство работами по обеспечению ИБ и контроль выполнения положения частной политики возлагается на Руководителя организации.

3. Администратор информационной безопасности руководит и контролирует планирование и выполнение организационных мероприятий по вопросам обеспечения безопасности информации на объектах защиты согласно документам второго и третьего уровня (регламентам и инструкциям), а также отвечает за реализацию и актуализацию частной политики.

Контроль за реализацией частной политики

1. Текущий контроль за соблюдением выполнения требований частной политики возлагается на ответственных за систему обеспечения информационной безопасности КС. Реализация и соблюдение мер защиты, регламентов и инструкций должно контролироваться на регулярной основе.

2. Чтобы обеспечить эффективный контроль над выполнением требований определенных частной политикой в зависимости от специфики сетевой атаки типа «…» используется комплексная система мер и процедур, скоординированных и осуществляемых соответствующими службами организации.

3. Данная комплексная система мер и процедур состоит из действий, представленных в табл. 5, где указывается перечь мер и средств, необходимых для контроля выполнения требований определенных частной политикой для защиты от сетевой атаки типа «…».

Таблица 5

Комплексная система мер и процедур, отвечающая за контроль выполнения требований определенных частной политикой

Предложенные меры безопасности в рамках противодействия сетевой атаке типа «…»	Меры контроля
Наличие в системе механизмов, которые могут отфильтровать трафик, исходящий от заблокированных IP-адресов или с подозрительных источников	Тестирование на проникновение используется для проверки механизмов фильтрации трафика. В ходе тестирования на проникновение проверяется, насколько эффективно система блокирует вредоносный трафик и защищает от DDoS-атак.
…	…

Условия пересмотра (выпуска новой редакции) частной политики

Периодическая проверка актуальности настоящей частной политики проводится главным Администратором информационной безопасности по мере необходимости, при появлении новых угроз и объектов защиты, а также при изменении законодательства в области обеспечения ИБ.

Основанием для пересмотра и совершенствования настоящей частной политики являются результаты внутренних и внешних аудитов информационной безопасности, а также результаты риск-анализа системы управления информационной безопасностью КС, изменения штатной структуры организации.

Пример применения предложенной методики

В качестве иллюстрации вышеизложенного для организации, опасающейся атак троянскими программами, ниже предлагаются меры коррекции политики обеспечения информационной безопасности для отражения различных векторов атаки (табл. 6).

Таблица 6

Меры защиты сетей на уровне частной политики обеспечения безопасности

Учащенно зарегистрированные последовательности и содержание действий злоумышленника в целях реализации сценариев атаки	Возможные ответные меры защиты организации от сетевой атаки, адекватные действиям злоумышленника, по каждому ее сценарию
Письмо с вложенным троянцем	
Злоумышленник изучает корпоративную сеть и выявляет почтовый адрес жертвы.	Использование корпоративной учетной записи только в рабочих целях, указывание ее на сторонних сайтах запрещается.
Злоумышленник отправляет на почту корпоративному сотруднику письмо, замаскированное под важную информацию, прикрепляя файл, картинку, документ в который зашифрован троянец.	Исключение скачивания и открытия файлов, картинок, документов от неизвестного отправителя, перехода по неизвестной ссылке.
	Настройка фильтрации спам сообщений.
	Использование известных почтовых сервисов, в которых реализованы инструменты защиты пользователей.
	Отключение быстрого выполнения скриптов.
Когда пользователь откроет отправленный ему зараженный файл, то запустятся встроенные макросы. Тогда злоумышленник получит удаленный доступ к зараженной системе и сможет извлечь пароли и куки из браузеров, похищать письма из почтового ящика, перехватывать трафик.	Использование надежных антивирусных средств защиты для распознавания вредоносного ПО при запуске программы.
Доверительный архив	
Злоумышленник использует недостаток алгоритмов сжатия архивов и отправляет их пользователю на почту во вложении.	Настройка фильтрации спам-сообщений.
Когда система пытается извлечь содержимое архива, она может зациклиться на повторяющихся файловых структурах или просто исчерпать все доступные ресурсы, пытаясь разархивировать огромное количество данных.	Использование надежных антивирусных средств защиты.
	Мониторинг трафика, исходящий от определенной машины, и запретит его через встроенные средства брандмауэра.

Продолжение табл. 6

Учащенно зарегистрированные последовательности и содержание действий злоумышленника в целях реализации сценариев атаки	Возможные ответные меры защиты организации от сетевой атаки, адекватные действиям злоумышленника, по каждому ее сценарию
Доверительный архив	
Злоумышленник также может внедрить вредоносный эксплойт в архив для загрузки троянца. Что может привести к значительному замедлению или остановки работы системы, а также краже учётных записей.	Проведение мониторинга системы использованных ресурсов компьютера поможет обнаружить его необычное поведение.
Успешное выполнение эксплойта запустит троянскую программу, которая получит полный или ограниченный удаленный доступ к уязвимой системе.	Обновление ПО и операционных систем для исправления уязвимостей.
Троян-антивирус	
Злоумышленник разрабатывает фальшивый антивирус, который является троянцем, шифрует его и загружает на веб-ресурс, выставляя за легитимное ПО.	Использование только лицензионного ПО с официальных сайтов, а также блокировщиков рекламы, веб-фильтров и сетевых экранов.
После скачивания лже-антивирус имитирует поведение антивирусных программ или компонентов безопасности операционной системы.	Осуществление регулярного обновления ПО и операционных систем, исправление уязвимостей безопасности и предотвращение атак.
Отображается ряд нежелательных уведомлений, побуждая пользователя заплатить за обнаружение и удаление несуществующих угроз.	Разграничение прав пользователей с использованием групповой политики для запрета установки сторонних программ.
	Проведение в системе мониторинга использованных ресурсов компьютера поможет обнаружить его необычное поведение.
Аппаратный кейлоггер	
Злоумышленник получает доступ к АРМ, подключает аппаратный кейлоггер в виде небольшого USB-переходника и подключает его между клавиатурой и портом USB.	Совершенствование пропускного режима по периметру защиты организации.
Аппаратный кейлоггер USB автоматически начинает перехват всех данных, вписываемых с клавиатуры, и отправляет всю информацию злоумышленнику через электронную почту, FTP или другие средства передачи данных.	Использование надежных антивирусных средств защиты.
	Создание списка доверенных USB-носителей, разрешенных для использования на автоматизированном рабочем месте.
	С целью обнаружения аномальной сетевой активности, анализ сетевого трафика и журналов событий, что может выявить отправку данных злоумышленнику.
	Использование инструментов, блокирующих вредоносные скрипты.

Окончание табл. 6

Учащенно зарегистрированные последовательности и содержание действий злоумышленника в целях реализации сценариев атаки	Возможные ответные меры защиты организации от сетевой атаки, адекватные действиям злоумышленника, по каждому ее сценарию
Внедрение вредоносного скрипта скрытой загрузки	
Злоумышленник использует веб-ресурс компании для внедрения вредоносного скрипта скрытой загрузки (Drive-by attack). Этот код скрывается в JavaScript, Flash или других исполняемых файлах, которые автоматически загружаются и адаптируются при посещении сайта.	Исключение перехода по ссылкам из сообщений от неизвестных источников.
	Создание правил исходящего соединения для ведения списков белых адресов, что позволит переходить только на заранее разрешенные сайты.
Пользователь попадает на сайт, содержащий код, который перенаправляет запрос на сторонний сервер, на котором хранится эксплойт. Вредоносный скрипт автоматически загружается на устройство пользователя через его веб-браузер, а код используется для выполнения запуска троянских программ на конечном узле.	Использование последней версии браузера с встроенной анти-фишинговой защитой.
	Использование параметров брандмауэра для блокировки входящих соединений и предотвращения несанкционированного доступа к системе.
В процессе атаки устанавливаются дополнительные вредоносные программы.	Проверка названия организации, которой принадлежит сайт.
	Задействование надежных антивирусных средств защиты.
Троян-шифровальщик	
Злоумышленник шифрует троян в файл, что позволяет защитить вирус от обнаружения различными антивирусными ПО.	Использование параметров брандмауэра для блокировки входящих соединений и предотвращения несанкционированного доступа к системе.
Злоумышленник загружает закриптованный файл с вирусом на веб ресурс и ожидает пока пользователь скачает и запустит программу.	Использование надежных антивирусных средств защиты.
	Разграничение прав пользователей с использованием групповой политики для запрета установки сторонних программ.
Пользователь открывает файл, запускается троянец и делает хранимые данные недоступными, зашифровав диски. Шифровальщик запрашивает ключ за вознаграждение.	Резервное копирование системы.
	Включение функции отображения расширения файлов, что позволит увидеть замаскированное расширение.
	Использование средства мониторинга ресурсов системы, так как шифровальщик использует мощность процессора для зашифровки файлов, что будет видно при мониторинге загрузки процессора.

Заключение

Таким образом сформирована частная политика, которая адаптирована под защиту от возникающих угроз безопасности при реализации сетевой атаки. Частная политика определяет основные цели и задачи организации в части противодействия сетевым атакам, а также задает основное направление в развитии структуры взаимоувязанных документов, таких как

частные регламенты и инструкции сетевой безопасности.

Предложенная частная политика представляет возможным сформировать перечень мер защиты, учитывающих специфику сетевой атаки.

Важный момент, который должна учитывать каждая организация – это правильное распределение обязанностей сотрудников, обеспечивающих защиту информации, в связи с чем, частной политикой фиксируется перечень должностных лиц с их обязанностями в части противодействия сетевой атаке.

Также частная политика учитывает такой фактор, как контроль выполнения предложенных мер безопасности в рамках противодействия сетевой атаке.

Представленная методология разработки частной политики легко адаптируется под различные сетевые атаки и в полной мере учитывает их специфику, что делает данный документ эффективным и при борьбе с возникающими угрозами и рисками.

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. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. URL: https://docs.cntd.ru/document/1200179612 (дата обращения: 1.09.2023).

4. ГОСТ Р ИСО/МЭК 15408-2-2013.Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. URL: https://docs.cntd.ru/document/1200105710 (дата обращения: 1.09.2023).

5. 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).

6. 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).

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

8. ГОСТ Р ИСО/МЭК 27005:2010. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. URL: https://docs.cntd.ru/document/1200084141 (дата обращения: 1.09.2023).

9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (утв. ФСТЭК России 15 февраля 2008 г.). URL: https://docs.cntd.ru/document/902330983 (дата обращения: 1.09.2023).

10. NIST SP 800-53. Security and Privacy Controls for Information Systems and Organizations. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (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 3.09.2023

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

Кривошеин Александр Сергеевич – 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 I)

G.A. Ostapenko, D.V. Shcherbakova, T.Yu. Miroshnichenko, A.A. Ostapenko, A.S. Krivoshein

Proposed methodological support for the formation of private policies to protect the corporate network. The presented methodology for building a private policy is developed on the basis of best practices and recommendations in the field of information security, and also takes into account windows that allow you to adapt a private policy to the specifics of various attacks. Private policy defines the main goals and objectives of the organization in terms of countering network attacks, sets the main direction in the development of the structure of interrelated documents, such as private regulations and instructions for network security. A plan is being developed to form a list of measures, which includes requirements and measures for protecting information, taking into account the specifics of a network attack. The areas of responsibility for ensuring the security of officials are delineated and the methods and means of monitoring the implementation of the requirements defined by private policy are described.

Keywords: private policy, network attack, protection measures, objects of protection, intruder model.

Submitted 3.09.2023

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

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