DOI 10.36622/VSTU.2023.26.3.018
УДК 004.056

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

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

Предлагается методическое обеспечение для формирования частных регламентов защиты корпоративных сетей. Представляемая методология создания частных регламентов направлена на процесс управления инцидентами нарушения безопасности, возникающие вследствие реализации различных типов сетевых атак. Частные регламенты включают в себя: регламент обнаружения и регистрации инцидентов нарушения сетевой безопасности, регламент реагирования на инциденты нарушения сетевой безопасности, регламент ликвидации последствий инцидентов нарушения сетевой безопасности. Приведенная методика по построению регламентов позволяет классифицировать инциденты нарушения безопасности, учитывая их уровень критичности и приоритет, также определяет механизмы регистрации. Представлен алгоритм по реагированию на инциденты и по выявлению и ликвидации негативных последствий, вызванных инцидентами.

Ключевые слова: частные регламенты, сетевая атака, инцидент безопасности, события безопасности.

Введение

Регламент информационной безопасности (далее – регламент) – это документ, устанавливающий конкретные процедуры и правила, которые необходимо выполнять для обеспечения безопасности организации.

Создаваемые регламенты должны отражать в себе процессы, которые определены политикой информационной безопасности, а также – соответствовать своей полнотой и практичностью в части защиты информации.

Следуя определенным целям в частной политике сетевой безопасности необходимо предложить методологию создания частных регламентов, которые будут направлены на процесс управления инцидентами нарушения безопасности, которые возникают в следствии реализации различных типов сетевых атак. Данные частные регламенты можно классифицировать на следующие взаимоувязанные документы:

- 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.

Создание частных регламентов по данному направлению аргументируется тем, что управление инцидентами нарушения безопасности является важным вопросом в области информационной безопасности. Сетевые атаки стали более многочисленными и разнообразными, а также влекут за собой огромные риски и ущербы. Часто возникают новые типы инцидентов, тогда профилактические мероприятия, основанные на результатах оценки рисков, могут снизить их количество, но не все инциденты можно предотвратить. Поэтому для оперативного обнаружения и реагирования на инциденты нарушения безопасности необходимо создавать регламенты, которые позволят эффективно управлять данными процессами. Регламенты помогут свести к минимуму ущербы и риски, устранить уязвимости, которые были использованы, и восстановить работоспособность служб, затронутые инцидентом.

С этой целью в данной статье предложены методологии создания регламентов, позволяющие в конечном счете

адаптировать их структуру регламента для определения более конкретных процедур обработки инцидентов с учетом специфики сетевых атак различного типа.

Поскольку эффективное реагирование на инциденты является достаточно сложной задачей, для успешного её решения требуется значительное планирование. При этом необходим мониторинг атак, а также - установление четких процедур определения приоритетов при рассмотрении инцидентов, равно как и внедрение эффективных методов сбора, анализа данных и представления отчетности. Представленные регламенты могут помочь организациям в формализации процессов обнаружения, реагирования на инциденты нарушения безопасности, вызванных различными типами сетевых атак, а также - эффективно ликвидировать негативные последствия инцидентов.

Еще одно преимущество внедрения таких регламентов в организации – это способность использовать информацию, полученную в ходе обработки инцидентов, для лучшей подготовки к обработке будущих инцидентов и обеспечения более надежной защиты систем и данных.

Регламент обнаружения и регистрации инцидентов нарушения сетевой безопасности организации

Общие положения

1. Настоящий регламент определяет порядок регистрации и подтверждения возникновения инцидентов нарушения безопасности, произошедших в организации в ходе реализации сетевой атаки типа «…».

2. Регламент разработан с целью выявления инцидентов нарушения безопасности, а также своевременного и эффективного идентифицирования и регистрации событий в ходе реализации сетевой атаки типа «…».

3. Регламент является обязательным для всех сотрудников организации, отвечающих за координацию процедур регистрации и подтверждения инцидентов безопасности.

4. Администратор информационной безопасности организации назначается ответственным за выявление инцидентов безопасности и их регистрации.

5. Настоящий регламент действует на постоянной основе и подлежит периодическому обновлению и согласованию с частной политикой обеспечения сетевой безопасности, которая определяет меры защиты информации в части противодействия сетевым атакам заданного типа.

6. Настоящий регламент разработан в соответствии со следующими нормативными и методическими документами [1-18].

Термины и определения

В настоящем регламенте используются следующие термины и определения:

Для разрабатываемого регламента необходимо привести определения терминов, уточняющих специфику векторов и уязвимостей заданного типа атак.

1. Инцидент безопасности - любое непредвиденное событие в информационной системе, которое может привести к нарушению целостности, конфиденциальности или доступности информации.

2. Компьютерный ресурс - любой компонент информационной системы, включая аппаратное и программное обеспечение, данные и сетевые ресурсы.

3. Признаки возможного инцидента - любые аномальные события или поведение компьютерных ресурсов, которые могут указывать на вероятное нарушение безопасности.

4. Подтверждение инцидента - процесс подтверждения факта наличия инцидента при помощи сбора и анализа информации.

5. Регистрация инцидента - процесс документирования факта инцидента в соответствии с установленными процедурами.

6. Классификация инцидента - процесс определения категории и серьезности инцидента.

7. Ликвидация последствий инцидента - это процесс восстановления нормального функционирования системы после возникновения инцидента информационной безопасности или другого негативного события.

Состав и содержание информации, необходимой для регистрации и подтверждения инцидентов

Общие сведения, необходимые для обнаружения и регистрации инцидентов безопасности, таковы:

1. Реализация процессов обнаружения и регистрации инцидентов безопасности достигается путем, формирования перечня сведений, состоящего из:

− контролируемых информационных ресурсов организации;

− типов инцидентов, которые подлежат обнаружению и регистрации с указанием их уровней критичности и приоритетов.

2. Контролируемые информационные ресурсы организации в рамках защиты от сетевой атаки типа «…» представлены в табл. 1, где перечисляются состав и технические характеристики контролируемых ресурсов организации, необходимые для выявления инцидентов.

Таблица 1

Перечень информационных ресурсов организации

Идентификатор информационного ресурса	Информационный ресурс	Состав	Технические характеристики
R_1	Сайт	Система управления контентом (CMS)	Язык программирования; Скорость загрузки страниц сайта
R_2	…	…	…
…	…	…	…

3. Для формирования перечня типов инцидентов безопасности, которые необходимо обнаруживать и регистрировать в организации, используются сведения об определении инцидентов, в частности выделяются всевозможные инциденты, которые могут произойти в рамках реализации сетевой атаки типа «…». В дополнение к этому перечню может быть предусмотрен дополнительный тип инцидентов (например, «иное»), который позволяет зарегистрировать инциденты, не соответствующие ни одному из заранее определенных типов.

Инциденты, которые могут возникнуть в ходе реализации сетевой атаки, классифицируются по типам, также приводится уровень критичности и приоритет инцидента безопасности (табл. 2).

4. Для определения уровня критичности инцидента используется табл. 3.

5. Для определения приоритета инцидента безопасности используется табл. 4, где указываются все инциденты, которые подлежат обнаружению и регистрации в рамках защиты от сетевой атаки типа «…».

Таблица 2

Классификация инцидентов, возникающих в ходе реализации сетевой атаки типа «…»

Сценарии атаки	Тип инцидента	Описание	Критичность	Приоритет инцидента
VA_1	Получение доступа к системам и данным организации	Инцидент, связан с несанкционированным доступом и компрометацией информации	4	Высокий
VA_2	…	…	…	

Таблица 3

Уровень критичности инцидента

Значение	Критическое значение	Время реагирования	Описание
4	Критичный	30 минут	Был зафиксирован инцидент, свидетельствующий о том, что система подверглась успешной атаке, при этом были поражены критические ресурсы организации. Как следствие, может возникнуть компрометация системы или утечка важной информации, нарушена работа критически важной инфраструктуры, что может привести к недоступности сервисов и полному отсутствию работоспособности системы. В этом случае планируются и проводятся меры по ликвидации инцидента.
3	Высокий	30 + X минут	Инцидент определяет событие, которое может привести к компрометации данных системы. Если такой инцидент произошел, ему необходимо незамедлительно уделить внимание, провести тщательное исследование и принять меры, направленные на уменьшение риска и снижение вероятности успешной атаки. В этом случае планируются и проводятся меры по ликвидации инцидента.
3	Высокий	30 + X минут	Инцидент определяет событие, которое может привести к компрометации данных системы. Если такой инцидент произошел, ему необходимо незамедлительно уделить внимание, провести тщательное исследование и принять меры, направленные на уменьшение риска и снижение вероятности успешной атаки. В этом случае планируются и проводятся меры по ликвидации инцидента.
2	Средний	30 + X минут	Инцидент может привести к компрометации системы. Возможно применение мер по ликвидации инцидента.
1	Низкий	30 + X минут	Инцидент указывает на низкий риск или служит предупреждением. В таких случаях, инцидент потенциально может привести к компрометации данных системы. Меры по ликвидации инцидента необязательны. Риск может быть принят.

Таблица 4

Форма определения приоритета инцидента

Масштаб инцидента	Значимость контролируемых информационных ресурсов		
	Высокий	Средний	Низкий
Высокий	Высокий	Высокий	Высокий
Средний	Высокий	Средний	Средний
Низкий	Высокий	Средний	Низкий

6. В табл. 3 необходимо самостоятельно определить время реагирования. Чем выше критичность, тем время должно быть ниже. Минимально допустимое время реагирования 30 минут.

Приведенное в табл. 3 значение X подразумевает под собой добавку к минимально допустимому времени, чтобы в конечном итоге получилось время, которое необходимо затратить на реагирование возникающих инцидентов.

7. Приоритет инцидентов безопасности формируется на основе использования характеристик регистрируемых инцидентов:

− значимость контролируемых информационных ресурсов, на которых выявлены признаки идентифицируемого инцидента;

− масштаб инцидента.

При определении значимости инцидента учитываются функционирующие контролируемые информационные ресурсы, находящаяся на них информация и возможность распространения инцидента на другие, более значимые системы организации.

Инциденты, которые имеют высокий приоритет - это те, которые оказывают негативное влияние на работу наиболее критических сервисов организации и могут привести к остановке или повреждению ключевых бизнес-процессов. Также среди них могут быть инциденты, связанные с обработкой информации, которая необходима для обеспечения этих процессов.

Инциденты, которые имеют средний приоритет - это те, которые могут быстро распространиться на системы, на которых работают сервисы, нарушение которых может привести к остановке или повреждению критически важных процессов.

К инцидентам с низким приоритетом относятся все остальные инциденты.

Масштаб инцидента зависит от количества контролируемых ресурсов, на которых обнаружены признаки инцидента.

Если инциденты зафиксированы на 30% или более контролируемых ресурсов, то они считаются с высоким приоритетом, что может привести к серьезным нарушениям в работе системы.

Если инциденты обнаружены на 20% контролируемых ресурсов, то они считаются со средним приоритетом, что может привести к нарушениям в работе системы.

Если инциденты обнаружены на менее чем 10% контролируемых ресурсов, то они считаются с низким приоритетом, что может иметь незначительное влияние на работу системы.

Регистрация и подтверждение инцидентов безопасности

Этап обнаружения и регистрации инцидентов безопасности состоит из следующих стадий:

− регистрация признаков возможного возникновения инцидентов;

− подтверждение инцидентов.

Описание средств, предназначенных для обнаружения и регистрации инцидентов безопасности таково:

Описание средств, предназначенных для обнаружения и регистрации инцидентов, включает в себя информацию о программном и аппаратном обеспечении, используемых для мониторинга сетевой безопасности организации на предмет возможных инцидентов. Оно может включать в себя специализированные программы-агенты, которые устанавливаются на компьютерные системы, а также инструменты для анализа сетевого трафика и журналов событий. Описание может также содержать информацию о методах обнаружения инцидентов безопасности, которые

используются для выявления отклонений в работе системы и анализа потенциальных угроз для безопасности данных.

1. Администратором информационной безопасности используются следующие средства, предназначенные для обнаружения и регистрации инцидентов безопасности:

Здесь указывается перечень необходимых и достаточных средств, предназначенных для обнаружения и регистрации инцидентов, в рамках защиты от сетевой атаки типа «…». Например:

− программное обеспечение для мониторинга компьютерных систем, такое как системы управления журналами событий, мониторинг сетевых устройств и т.д.;

− аппаратное обеспечение для мониторинга компьютерных систем, такое как сетевые коммутаторы, маршрутизаторы, межсетевые экраны (firewalls) и другие устройства;

− системы обнаружения вторжений (IDS), которые могут использоваться для обнаружения необычной сетевой активности;

− системы защиты от вирусов и злоумышленного ПО, которые могут обнаруживать и блокировать вредоносные программы и другие угрозы;

− методы анализа сетевого трафика и журналов событий, которые могут использоваться для обнаружения аномальной сетевой активности;

− анализ поведения пользователей, который может помочь обнаружить необычную активность, связанную с потенциальным компьютерным инцидентом;

− системы мониторинга и анализа уязвимостей, которые позволяют выявить уязвимости в системах и приложениях и принять меры для их устранения;

− методы машинного обучения и искусственного интеллекта, которые могут использоваться для обнаружения необычной и аномальной сетевой активности.

2. В случае, если информация о инцидентах была предоставлена сотрудниками организации, необходимо собрать следующую информацию, как время и место возникновения инцидента, его характер и обстоятельства, а также имя сотрудника, который сообщил о нем.

Правила регистрации признаков возможного возникновения инцидентов безопасности таковы:

1. Сотрудники отдела информационной безопасности для обнаружения и регистрации инцидентов безопасности должны проводить мониторинг состояния защищенности организации. В рамках мониторинга осуществляется сбор информации о событиях безопасности и других данных мониторинга из различных источников. Эта деятельность позволяет быстро обнаруживать признаки возможных инцидентов и осуществлять их регистрацию в соответствии с установленными процедурами.

2. Администратор информационной безопасности должен регулярно пересматривать перечень событий безопасности, которые подлежат регистрации. В ходе пересмотра Администратор информационной безопасности должен проанализировать существующие правила и процедуры, а также убедиться в их актуальности. Обновление перечня событий, которые должны быть зарегистрированы, позволит улучшить общую стратегию защиты при сетевой атаке типа «…».

3. Перечень событий о возможной угрозе безопасности организации в ходе реализации сетевой атаки типа «…»:

Указывается перечень таких событий в зависимости от особенностей сетевой атаки (заданной атаки). Например:

− необычная активность в сети;

− аномальные запросы на сервер;

− попытки удаленного доступа.

Регистрации признаков возможного возникновения инцидентов безопасности на основании информации, поступившей из систем безопасности организации, выглядит следующим образом:

1. Сотрудник отдела информационной безопасности обращается к Администратору информационной безопасности с описанием обнаруженных признаков возможных угроз безопасности.

2. Администратор информационной безопасности регистрирует информацию об возможном инциденте.

3. После того, как обнаружены признаки возможных угроз безопасности,

Администратор информационной безопасности проводит анализ и оценку уровня риска, связанного с этими признаками угрозы. Это позволяет определить, насколько серьезной может быть угроза и какие меры следует принять для ее предотвращения.

4. Если в записях регистрации событий обнаружены признаки возможного инцидента безопасности, то Администратор информационной безопасности проводит расследование и подтверждает факт возникновения инцидента безопасности. В противном случае, если признаки угрозы не подтверждаются, Администратор информационной безопасности опровергает возможность инцидента безопасности.

5. Информацию об инциденте Администратор информационной безопасности должен занести в отчет.

6. Для регистрации инцидента нарушения безопасности Администратор информационной безопасности заполняет карточку регистрации инцидента, принимает решение о регулировании инцидента безопасности.

При заполнении карточки регистрации инцидента Администратору информационной безопасности необходимо делать следующие шаги:

− проверять и уточнять сведения о возможном инциденте нарушения безопасности;

− подтверждать факт возникновения инцидента и принимать решение о начале действий по реагированию на него;

− определять первоочередные меры реагирования на инцидент, определять ответственных лиц и направлять им задания на реагирование.

В ходе проверки и уточнения сведений о возможном инциденте Администратор информационной безопасности:

− отправляет запрос работникам информационных ресурсов, которые, вероятно, задействованы в инциденте, с просьбой проверить информацию, содержащуюся в карточке инцидента информационной безопасности;

− самостоятельно проводит проверку заполненной карточки регистрации инцидента путем сопоставления данных, содержащихся в ней, с результатами инвентаризации.

7. После регистрации признаков возможных инцидентов безопасности и факта их подтверждения, необходимо предпринять меры для их предотвращения или устранения. Данный процесс осуществляется в соответствии с регламентом реагирования на инциденты нарушения сетевой безопасности организации.

Регламент реагирования на инциденты нарушения сетевой безопасности организации

Общие положения

1. Настоящий регламент определяет порядок реагирования на инциденты безопасности, произошедших в организации в ходе реализации сетевой атаки типа «..».

2. Регламент разработан с целью определения процедур и шагов, которые необходимо выполнить для обеспечения быстрого и эффективного реагирования на возможные инциденты безопасности в ходе реализации сетевой атаки типа «..».

3. Регламент является обязательным для всех сотрудников организации, отвечающих за процедуру реагирования на инциденты безопасности.

4. В организации создается рабочая группа, состоящая из начальника отдела по защите информации, Администратора информационной безопасности и сотрудников отдела системного администрирования, которая будет участвовать в процедуре реагирования на инциденты безопасности.

5. Настоящий регламент действует на постоянной основе и подлежит периодическому обновлению и согласованию с частной политикой обеспечения сетевой безопасности, которая определяет меры защиты информации в части противодействия сетевым атакам заданного типа.

6. Настоящий регламент разработан в соответствии с действующими нормативными и методическими документами в области защиты информации, предусмотренными в регламенте обнаружения и регистрации инцидентов безопасности. Эти документы содержат

основные требования и рекомендации по обеспечению безопасности информации и помогают определить правила и процедуры для регистрации и анализа инцидентов безопасности.

Порядок реагирования на инциденты безопасности

1. После получения сведений о подтверждении факта возникновения инцидента рабочая группа определяет элементы контролируемых информационных ресурсов, которые были вовлечены в инцидент.

2. В случае возникновения нескольких инцидентов безопасности рабочая группа устанавливает последовательность реагирования на них.

3. Рабочая группа должна незамедлительно предпринять первоочередные меры по предотвращению инцидента безопасности.

4. Последовательность реагирования и первоочередные меры представлены в табл. 5, где указываются инциденты, которые могут произойти в ходе реализации сетевой атаки типа «..», последовательность реагирования на них, первоочередные меры предотвращения. Последовательность реагирования определяется с помощью табл. 6.

Таблица 5

Меры локализации инцидентов безопасности

Идентификатор инцидента	Произошедший инцидент	Последовательность реагирования	Первоочередные меры предотвращения
I_2	Получение доступа к системам и данным организации	1-я	Ограничение доступа к объекту атаки
I_2	…	…	…

Последовательность реагирования на инциденты (табл. 6) формируется из параметров уровня критичности и приоритета инцидента, значения устанавливаются табл. 3 и 4 регламента обнаружения и регистрации инцидентов безопасности.

В табл. 6 приняты следующие обозначения: К– критический, В – высокий, С – средний, Н – низкий.

Таблица 6

Порядок определения последовательности реагирования на инциденты

Последовательность реагирования	1-я	2-я	3-я	4-я	5-я	6-я	7-я	8-я	9-я
Уровень критичности	К	В	В	С	С	С	Н	Н	Н
Приоритет инцидента	В	В	С	В	С	Н	В	С	Н

5. После выполнения первоочередных мер защиты необходимо реализовать план мероприятий по противодействию сетевой атаки типа «…», который приведен в табл. 7, где перечисляются мероприятия, которые направлены на устранение инцидентов безопасности с указанием срока исполнения.

Таблица 7

План мероприятий по противодействию сетевой атаки типа «..»

Мероприятия по противодействию сетевой атаки	Срок исполнения	Дополнительно
Проверка наличия установленного ПО последней версии	В течение 5 часов с моменты получения информации об инциденте безопасности	В случае, если актуальное ПО не установлено, необходимо его обновить
Анализ событий безопасности, изучение сведений о векторе сетевой атаки	В течение 30 мин. после получения информации об инциденте	Анализ данных средств, предназначенных для обнаружения и регистрации инцидентов. Установка последовательности реагирования на инциденты для противодействия вероятной атаке
…	…	…

6. После того, как инцидент был нивелирован, Администратор информационной безопасности должен составить отчет о реагировании на данный инцидент.

Определение последствий инцидентов безопасности

1. После процедуры реагирования на инциденты безопасности и принятия мер по их устранению, рабочая группа должна выявить признаки отрицательного воздействия на информационную инфраструктуру организации, затронутые инцидентом.

2. При обнаружении признаков отрицательного воздействия на информационную инфраструктуру организации, затронутые инцидентом, рабочая группа проводит тщательный анализ имеющейся информации о произошедшем инциденте.

3. Необходимо определить какие элементы информационной инфраструктуры были повреждены или уничтожены, а также какие данные были утрачены или скомпрометированы. На основе этого анализа будет разработан план мероприятий по восстановлению нормального функционирования информационной инфраструктуры организации и восстановлению утраченных данных.

4. К негативным последствиям инцидента безопасности, произошедшего в ходе реализации сетевой атаки (заданного типа), относятся:

Перечисляются все негативные последствия, которые порождает инцидент в результате реализации сетевой атаки типа «..». Например:

− индикаторы возможных проблем в работе операционной системы, программных средств защиты информации, приложений, такие как сбои, перезагрузки, остановки и иные нарушения в штатной работе;

− признаки нарушения функционирования сетевых служб, ненормального использования ресурсов системы;

− другие сведения, характерные для специфических видов инцидентов нарушения безопасности и сетевых атак, заданного типа по наиболее опасным.

5. Процесс устранения негативных последствий, возникших в результате инцидента безопасности, и восстановления функционирования информационной системы или элементов информационной инфраструктуры организации в целом осуществляется в рамках регламента ликвидация последствий инцидентов нарушения сетевой безопасности.

Регламент ликвидации последствий инцидентов нарушения сетевой безопасности организации

Общие положения

1. Настоящий регламент определяет порядок ликвидации последствий инцидентов нарушения безопасности, произошедших в организации в ходе реализации сетевой атаки типа «…».

2. Регламент разработан с целью установления процедур и мер по ликвидации последствий инцидентов нарушения безопасности, восстановления работоспособности систем и данных, а также предотвращения повторения инцидентов, которые могут возникнуть в ходе реализации сетевой типа «…».

3. Регламент является обязательным для всех сотрудников организации, участвующих в процедуре ликвидации последствий инцидентов безопасности.

4. В организации создается служба по работе с инцидентами, состоящая из Администратора информационной безопасности и сотрудников отдела системного администрирования, которая будет ликвидировать последствия инцидентов нарушения безопасности, выявлять причины и условия возникновения. Служба по работе с инцидентами также разрабатывает план действий по предотвращению повторного возникновения инцидентов.

5. Настоящий регламент действует на постоянной основе и подлежит периодическому обновлению и согласованию с частной политикой обеспечения сетевой безопасности, которая определяет меры защиты информации в части противодействия сетевым атакам заданного типа.

6. Настоящий регламент разработан в соответствии с нормативными и методическими документами в области защиты информации, определенными в регламенте обнаружения и регистрации инцидентов безопасности.

Ликвидация последствий инцидентов безопасности

1. Специалисты службы по работе с инцидентами должны провести работы по устранению негативных последствий инцидентов безопасности, которые возникли в ходе реализации сетевой атаки типа «…», описанные в регламенте реагирования на инциденты безопасности, согласно плану по ликвидации последствий инцидентов.

2. План по ликвидации последствий инцидентов состоит из следующих мероприятий:

Далее приводятся меры по устранению по устранению негативных последствий. Например:

− изоляция скомпрометированной системы или сети от остальной части инфраструктуры, чтобы предотвратить распространение вредоносных программ или доступ злоумышленников к другим системам;

− остановка процессов, связанных с инцидентом, например, удаление вредоносных программ или блокировка учетных записей злоумышленников;

− восстановление системных файлов или резервных копий, если они были созданы до инцидента;

− восстановление данных, если они были утрачены или скомпрометированы в результате инцидента.

3. После проведения мероприятий по ликвидации последствий службой по работе с инцидентами проводится анализ произошедших инцидентов.

4. Специалисты службы по работе с инцидентами должны выявить причины и условия возникновения инцидентов безопасности в организации, ходе реализации сетевой атаки типа «…». Соотношение инцидентов безопасности с потенциально возможными причинами и условиями представлено в табл. 8.

Таблица 8

Причины и условия возникновения инцидентов безопасности

Инцидент безопасности	Причины и условия возникновения инцидентов безопасности
Получение доступа к системам и данным организации	Недостаточное обучение персонала по соблюдению конфиденциальности информации, в том числе персональных данных
…	…

5. По результатам реагирования на инциденты безопасности и установления причин и условий их появления должны быть разработаны рекомендации по предотвращению повторного возникновения инцидентов нарушения безопасности. Эти рекомендации включают:

Указываются рекомендации, которые будут минимизировать вероятность повторного возникновения инцидентов нарушения сетевой безопасности. Например:

− требования к знаниям и навыкам специалистов организации в области защиты от атак заданного типа по наиболее опасным сочетаниям вектор-уязвимость;

− модернизация материально-техническое обеспечения организации для защиты от атак заданного типа по наиболее опасным сочетаниям вектор-уязвимость;

− уточнение плана мероприятий по реагированию на инциденты нарушения сетевой безопасности от атак заданного типа по наиболее опасным сочетаниям вектор-уязвимость.

6. В результате процесса работ по обнаружению, регистрации, регулированию инцидента безопасности и ликвидации его последствий заполняется Карточка закрытого инцидента безопасности. Карточки с закрытыми инцидентами в дальнейшем могут служить образцовыми моделями реагирования на аналогичные события в организации. Они позволяют создавать базу знаний, которая доступна специалистам, входящим в группы реагирования на инциденты, чтобы научиться эффективно работать с новыми случаями.

7. После выполнения всех мероприятий по ликвидации последствий инцидентов безопасности специалисты службы по работе с инцидентами выполняют проверку, в ходе которой рассматривается степень проработанности выполненных действий по реагированию на инцидент безопасности.

Пример применения предложенной методики

В качестве иллюстрации вышеизложенного для организации, опасающейся атак троянскими программами, ниже предлагаются меры коррекции регламентов обеспечения информационной безопасности для отражения различных векторов атаки (табл. 9, 10).

Таблица 9

Меры регламентации защиты сети организации на стадии обнаружения и регистрации инцидентов безопасности

Разновидности инцидентов, которые могут возникнуть при реализации сетевой атаки	Описание инцидента	Возможные средства фиксации инцидента
Письмо с вложенным троянцем		
Утечка конфиденциальных данных	Сотрудник организации получает письмо от якобы страховой компании, где содержится договор, который необходимо скачать и открыть Этот файл имеет встроенные макросы - небольшие	Спам - фильтр, встроенный в почтовое приложение; Фильтрация отправителей.

Продолжение табл. 9

Разновидности инцидентов, которые могут возникнуть при реализации сетевой атаки	Описание инцидента	Возможные средства фиксации инцидента
Утечка конфиденциальных данных	программы, которые выполняются прямо внутри файла. Злоумышленник использовал их, как скрипты для скачки вредоносов. Теперь троян способен извлекать пароли и куки из браузеров, письма из почтового ящика, перехватывать трафик, давать операторам удаленный доступ к зараженной системе. В результате будут потеряны данные и получен несанкционированный доступ	Спам - фильтр, встроенный в почтовое приложение; Фильтрация отправителей. Проверка адреса отправителя. Антивирусное программное обеспечение. Мониторинг логов работы WAF.
Доверительный архив		
Компрометация учётных записей	Похищение учетных записей, а также получение удаленного доступа к системе, из-за вредоносного архива, который при открытии исчерпал все доступные ресурсы системы, и через который был запущен эксплойт для загрузки и установки трояна.	Средства защиты, встроенные в браузер. Антивирусное программное обеспечение. Спам - фильтр, встроенный в почтовое приложение. Системы обнаружения вторжений (IDS).
Троян-антивирус		
Вирусная атака фальшивым антивирусом	Сотрудник организации решил установить бесплатное антивирусное ПО с «пиратского» сайта, но установил троян-лже-антивирус. После установки лже-антивирус имитирует поведение антивирусных программ или компонентов безопасности операционной системы. Через некоторое время программа якобы нашла критическую угрозы для системы и для её удаления запросила вознаграждение за её удаление. Пользователь перевел деньги и потерял их.	Лицензионное антивирусное программное обеспечение. Разграничение прав пользователей с использованием групповой политики для запрета установки сторонних программ. Применение методов проверки типов данных и допустимых значений входных параметров.
Аппаратный кейлоггер		
Внедрение незаконного устройства с целью перехвата данных	Злоумышленник получил доступ к АРМ. Имея при себе устройство KeyLogger PRO, подключил его между клавиатурой и мышкой. Довольно сложно обнаружить в компьютер под столом.	Мониторинг активности USB портов. Физический осмотр компьютера для

Продолжение табл. 9

Разновидности инцидентов, которые могут возникнуть при реализации сетевой атаки	Описание инцидента	Возможные средства фиксации инцидента
Внедрение незаконного устройства с целью перехвата данных	Злоумышленник получил доступ к АРМ. Имея при себе устройство KeyLogger PRO, подключил его между клавиатурой и мышкой. Довольно сложно обнаружить это устройство, когда оно подключается в компьютер под столом. В KeyLogger PRO есть собственная система управления в виде веб-приложения. Используя возможности устройства, злоумышленник настроил SMTP для отправки отчетов по электронной почте со всеми собранными данными. Все вводимые данные с клавиатуры отправляются злоумышленнику на почту.	Мониторинг активности USB портов. Физический осмотр компьютера для поиска неизвестных периферийных устройств. Ограничение физического доступа в компанию. Ограничение физического доступа к системному блоку.
Внедрение вредоносного скрипта скрытой загрузки		
Получение несанкционированного удалённого доступа к системе	Злоумышленник обнаружил уязвимость кода JavaScript на сайте корпоративной сети. Загрузил вредоносный скрипт для скрытой загрузки (Drive-by attack). Пользователь открывает сайт, содержащий код, который перенаправляет запрос на сторонний сервер, на котором хранится эксплойт. Вредоносный скрипт автоматически загружается на устройство пользователя через его веб-браузер. Запущенный эксплойт загрузил бэкдор-троянца для полного контроля над удаленной машиной.	Мониторинг логов работы WAF для выявления атак и аномального поведения. Системы обнаружения вторжений (IDS). Антивирусное программное обеспечение позволяет выявлять сигнатуры вирусов. Фильтрация входного потока данных для предотвращения использования опасных HTML-тегов.
Троян-шифровальщик		
Отказ в доступе к файлам пользователю, у которого есть на это права	Сотрудник организации получается письмо на почту с вредоносным вложением в формате docx. Пользователь скачивает и открывает документ, активирует разрешение на редактирование содержимого, тем самым запускает вредоносный макрос. В результате происходит заражение вирусом-шифровальщиком Maze, который, как правило,	Антивирусное программное обеспечение. Мониторинг логов работы WAF для выявления атак и аномального поведения.

Окончание табл. 9

Разновидности инцидентов, которые могут возникнуть при реализации сетевой атаки	Описание инцидента	Возможные средства фиксации инцидента
Отказ в доступе к файлам пользователю, у которого есть на это права	распространяется в виде бинарного PE-файла (EXE или DLL в зависимости от конкретного сценария). Запущенный на компьютере шифровальщик Maze пытается определить тип системы зараженного компьютера. Эта информация используется в сообщении с требованием выкупа, чтобы заставить жертву думать, что злоумышленники знают все о зараженной сети.	Применение методов проверки типов данных и допустимых значений входных параметров. Спам фильтр, встроенный в почтовое приложение.

Таблица 10

Меры регламентации защиты сети организации на стадии реагирования на инциденты безопасности

Зафиксированные инциденты	Возможные меры реагирования на инцидент	Возможные последствия, вызванные инцидентом
Письмо с вложенным троянцем		
Утечка конфиденциальных данных	Отключение зараженного узла от сети. Установление обновления для антивирусного ПО. Сканирование системы с использованием антивируса. Настройка спам-фильтр. Смена данных учетной записи. Исключение использования рабочего почтового ящика для личных писем.	Получение удалённого доступа. Блокировка работы почты. Пользователь становится источником спам-рассылок. Увеличение нежелательного трафика. Нарушение тайны переписки.
Доверительный архив		
Компрометация учётных записей	Отключение зараженного узла от сети. Обновление базы антивирусного ПО, полное сканирование. Сканирование системы с использованием инструментов для поиска уязвимостей. Обновление установленных программ до последней версии. Удаление файлов «куки» и очистка кэша браузера. Отключение синхронизации, сброс настроек.	Утечка конфиденциальных данных. Финансовые потери. Получение несанкционированного доступа к системе. Нарушение целостности системы.

Продолжение табл.10

Зафиксированные инциденты	Возможные меры реагирования на инцидент	Возможные последствия, вызванные инцидентом
Троян-антивирус		
Вирусная атака фальшивым антивирусом	Отключение зараженного узла от сети. Установка обновления для антивирусного ПО. Выполнение полного сканирования системы с использованием антивируса. Использование инструментов для удаления троянов. Удаление всех лишних процессов из автозагрузки. Удаление временных файлов. Детальный анализ системной папки. Детальный анализ запущенных процессов после перезагрузки системы.	Потеря денежных средств. Скрытая установка вредоносных программных утилит. Утечка конфиденциальной информации. Пропажа данных. Финансовые потери. Снижение производительности системы.
Аппаратный кейлоггер		
Внедрение незаконного устройства с целью перехвата данных	Отключение зараженного узла от сети. Осмотр всех периферийных устройств. Детальный анализ запущенных процессов. Удаление всех лишних процессов из автозагрузки. Просмотр сетевой активности. Блокирование через FireWall соединение трояна. Выполнение полного сканирования системы с использованием антивируса.	Потеря всех данных, которые вводит пользователь. Перехват конфиденциальных данных. Кража учетной записи. Финансовые потери. Репутационные потери. Публикация коммерческой тайны.
Внедрение вредоносного скрипта скрытой загрузки		
Получение несанкционированного удалённого доступа к системе	Установление обновления для антивирусного ПО. Проверка настройки автозапуска системы на наличие зловредных скриптов. Анализ реестра. Полное сканирование системы с использованием антивируса. Обновление версии браузера.	Получение ложной информации с веб-сайта. Осуществление несанкционированного доступа. Репутационные потери. Кража конфиденциальных данных. Навязывание вирусной рекламы.

Окончание табл.10

Зафиксированные инциденты	Возможные меры реагирования на инцидент	Возможные последствия, вызванные инцидентом
Троян-шифровальщик		
Отказ в доступе к файлам пользователю, у	Отключить зараженный узел от сети. − Полное сканирование системы	Утечка конфиденциальной информации. − Финансовые потери.
которого есть на это права	с использованием антивируса. Загрузка в безопасном режиме и удаление сомнительных приложений. Удаление временных файлов. Анализ реестра. Использование только защищённого метода удаленного подключения к локальной сети. Очищение системы и восстановление бэкапа. Использование дешифратора. − Сохранение зашифрованных данных на внешнем носителе для дальнейшей расшифровки данных.	Ограничение доступа к файловой системе. Репутационные потери. Шифрование файлов. − Нарушение работоспособности и целости системы.

Заключение

Таким образом предложены методики создания частных регламентов, позволяющие адаптировать их структуру для определения более конкретных процедур обработки инцидентов с учетом специфики сетевых атак различного типа.

Регламент обнаружения и регистрации инцидентов нарушения безопасности позволяет классифицировать инциденты, учитывая их уровень критичности и приоритет, также определить механизмы их регистрации и средства для выполнения поставленной задачи.

На следующем этапе разработки регламентов был представлен алгоритм по реагированию на инциденты, а также учтены пункты по выявлению негативных последствий, вызванных инцидентом, что позволило разработать план по ликвидации последствий инцидентов.

На основании классификации инцидентов и порядка реагирования на них и устранения негативных последствий были определены частные регламенты обеспечения сетевой безопасности, позволяющие управлять рисками и, устраняя уязвимости, восстановить работоспособность служб, затронутых инцидентом.

Список литературы

1. ИСО/МЭК 13335-1:2006. Информационная технология - Методы обеспечения безопасности - Управление безопасностью информационных и телекоммуникационных технологий - Часть 1 - Концепция и модели управления безопасностью информационных и телекоммуникационных технологий. URL: https://docs.cntd.ru/document/1200048398 (дата обращения: 1.09.2023).

2. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения. URL: https://docs.cntd.ru/document/1200180385 (дата обращения: 1.09.2023).

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

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

5. 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).

6. 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).

7. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. URL: https://docs.cntd.ru/document/1200068822 (дата обращения: 1.09.2023).

8. Приказ Федеральной службы безопасности Российской Федерации от 06.05.2019 № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты». URL: http://www.consultant.ru/document/cons_doc_LAW_325824/ (дата обращения: 1.09.2023).

9. Приказ Федеральной службы безопасности Российской Федерации от 19.06.2019 № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_329209/ (дата обращения: 1.09.2023).

10. ГОСТ Р 57429-2017. Судебная компьютерно-техническая экспертиза. Термины и определения. URL: https://docs.cntd.ru/document/1200144960 (дата обращения: 1.09.2023).

11. NIST SP 800-83. Guide to Malware Incident Prevention and Handling. URL: http://dx.doi.org/10.6028/NIST.SP.800-83r1 (дата обращения: 1.09.2023).

12. NIST SP 800-84. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50889 (дата обращения: 1.09.2023).

13. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50875 (дата обращения: 1.09.2023).

14. NIST SP 800-92. Guide to Computer Security Log Management. URL: https://csrc.nist.rip/library/alt-SP800-92.pdf (дата обращения: 1.09.2023).

15. NIST SP 800-94. Guide to Intrusion Detection and Prevention Systems (IDPS). URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (дата обращения: 1.09.2023).

16. NIST SP 800-115.Technical Guide to Information Security Testing and Assessment. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspec-ialpublication800-115.pdf (дата обращения: 1.09.2023).

17. NIST SP 800-128. Guide for Security-Focused Configuration Management of Information Systems. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf (дата обращения: 1.09.2023).

18. Рекомендации по первоочередным мерам, направленным на обнаружение, предупреждение и ликвидацию последствий компьютерных атак. URL: https://safe-surf.ru/upload/ALRT/ALRT-20220316.1.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

Краснобородкин Александр Геннадьевич – 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 II)

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

Proposed methodological support for the formation of private regulations for the protection of corporate networks of the organization. The presented methodology for creating private regulations is aimed at managing incidents of security breaches arising from the implementation of various types of network attacks. Private regulations include: the regulation for detecting and registering incidents of network security violations, the regulation for responding to incidents of network security violations, the regulation for eliminating the consequences of incidents of network security violations. The above methodology for the construction of regulations allows classifying security breach incidents, taking into account their level of criticality and priority, and also determines the registration mechanisms. An algorithm for responding to incidents and for identifying and eliminating the negative consequences caused by incidents is presented.

Keywords: private regulations, network attack, security incident, security events.

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 G. Krasnoborodkin – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com