Приложение 2.

УТВЕРЖДЕНО
Распоряжением Администрации
Качканарского городского округа
Свердловской области
от 29.09.2023 № 83
«Об информационной безопасности
(защите информации) в
Администрации Качканарского
городского округа Свердловской
области»

Методическое руководство по организации технических мероприятий, направленных на проведение служебных проверок при возникновении компьютерных инцидентов

2023 г.

Оглавление

1. ВВЕДЕНИЕ

Настоящее Типовое методическое руководство по организации технических мероприятий, направленных на проведение служебных проверок при возникновении компьютерных инцидентов (далее – Методическое руководство), разработано для Администрации Качканарского городского округа Свердловской области (далее – Администрации Качканарского ГО СО).

Методическое руководство определяет порядок обнаружения, регистрации, классификации, оценки ущерба, реагирования и анализа причин компьютерных инцидентов.

Данное Методическое руководство разработано в соответствии со следующими документами:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– ГОСТ Р 59709 – 2022 Защита информации. Управление компьютерными инцидентами. Термины и определения;

– ГОСТ Р 59710 – 2022 Защита информации. Управление компьютерными инцидентами. Общие положения;

– ГОСТ Р 59711 – 2022 Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты;

– ГОСТ Р 59712 – 2022 Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами;

– Постановление Правительства Свердловской области от 01.07.2021 № 383-ПП «О Министерстве цифрового развития и связи Свердловской области»;

– Концепция технической защиты информации на территории Свердловской области № 01-01-41/58, утвержденная Губернатором Свердловской области, от 08.09.2021;

– Методический документ. Руководство по организации процесса управления уязвимостями в органе (организации). Утвержден ФСТЭК России 17 мая 2023 года.

Положения Методического руководства обязательны для всех сотрудников, имеющих доступ к программным и программно-аппаратным средствам Организации, информационным системам и ресурсам, защищаемой информации. Все сотрудники Организации обязаны ознакомиться под роспись с положениями данного Методического руководства до начала обработки информации с использованием программных и программно-аппаратных средств Организации.

Цель и задачи Методического руководства:

– создание условий для осуществления своевременного обнаружения и оперативного реагирования на инциденты информационной безопасности, в том числе их закрытия;

– предотвращение и (или) снижение негативного влияния инцидентов информационной безопасности на выполнение технологических процессов обработки информации, информационные системы и ресурсы;

– оперативное совершенствование системы защиты информации в Организации.

2. ТЕРМИНЫ И СОКРАЩЕНИЯ

Исполнительный орган государственной власти Свердловской области, осуществляющий полномочия по вопросам технической защиты информации: Министерство цифрового развития и связи Свердловской области (далее – Министерство).

Инцидент информационной безопасности; инцидент ИБ: непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (может привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации, или нарушению требований по защите информации.

Компьютерный инцидент: факт нарушения и (или) прекращения функционирования информационного ресурса, сети электросвязи, используемой для организации взаимодействия информационных ресурсов, и (или) нарушения безопасности обрабатываемой в информационном ресурсе информации, в том числе произошедший в результате компьютерной атаки.

Карточка компьютерного инцидента: документ установленной формы, предназначенный для формализованного описания компьютерных инцидентов.

Тип компьютерного инцидента: классификация разновидностей компьютерных инцидентов.

Компьютерная атака: целенаправленное воздействие программных и (или) программно-аппаратных средств на информационный ресурс в целях нарушения и (или) прекращения его функционирования и (или) создания угрозы безопасности обрабатываемой таким ресурсом информации.

Источник компьютерной атаки: лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

Тактика (проведения компьютерной атаки): совокупность приемов и способов действий, используемых для проведения компьютерной атаки.

Техника (проведения компьютерной атаки): совокупность и порядок действий, используемых для проведения компьютерной атаки в рамках соответствующих тактик.

Тип компьютерной атаки: классификация разновидностей компьютерных атак.

3. СТРУКТУРА МЕТОДИЧЕСКОГО РУКОВОДСТВА

Настоящее Методическое руководство определяет содержание трех стадий управления компьютерными инцидентами, которые включают в себя соответствующие этапы:

1. Обнаружение и регистрация компьютерных инцидентов:

1.1. Регистрация признаков возможного возникновения компьютерных инцидентов;

1.2. Подтверждение компьютерных инцидентов;

2. Реагирование на компьютерные инциденты:

2.1. Определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;

2.2. Локализация компьютерного инцидента;

2.3. Выявление последствий компьютерного инцидента;

2.4. Ликвидация последствий компьютерного инцидента;

2.5. Закрытие компьютерного инцидента;

2.6. Фиксация материалов, связанных с возникновением компьютерного инцидента;

2.7. Установление причин и условий возникновения компьютерного инцидента;

3. Анализ результатов деятельности по управлению компьютерными инцидентами:

3.1. Приобретение и накопление опыта по результатам управления компьютерными инцидентами;

3.2. Разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов;

3.3. Оценка результатов и эффективности реагирования на компьютерные инциденты.

4. ОБНАРУЖЕНИЕ И РЕГИСТРАЦИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

4.1. Общие положения

Деятельность по обнаружению и регистрации компьютерных инцидентов основывается на результатах проводимого в Организации мониторинга информационной безопасности, в рамках которого осуществляется сбор информации о событиях безопасности и иных данных мониторинга из различных источников.

Стадия «обнаружение и регистрация компьютерных инцидентов» включает в себя следующие этапы:

- регистрация признаков возможного возникновения компьютерных инцидентов;
- подтверждение компьютерных инцидентов.

4.2. Регистрация признаков возможного возникновения компьютерных инцидентов

Регистрация признаков возможного возникновения компьютерных инцидентов может осуществляться как автоматизированным способом (с использованием средства управления событиями информационной безопасности) на основе правил регистрации признаков возможного возникновения компьютерных инцидентов, так и неавтоматизированным способом (специалистами подразделения, ответственного за управление компьютерными инцидентами, при самостоятельном анализе событий безопасности в ходе мониторинга или при получении соответствующей информации от сотрудников Организации).

Информация об инцидентах ИБ может поступать по следующим каналам:

- журналы регистрации сетевого и межсетевого оборудования;
- журналы регистрации общесистемного программного обеспечения;
- журналы систем управления базами данных;
- журналы регистрации инфраструктурного программного обеспечения;
- журналы регистрации прикладного программного обеспечения;
- журналы средств защиты информации;
- оповещения антивирусных подсистем;
- оповещения подсистем обнаружения атак;
- оповещения других подсистем Организации;
- информация, получаемая от сотрудников Организации по любым каналам связи (телефон, электронная почта, речевой канал, др.).

Подсистема мониторинга о событиях ИБ включает в себя журналы программных и программно-аппаратных средств, перечисленных выше. Срок хранения событий ИБ должен быть не менее 3 месяцев, если иное не установлено требованиями законодательства Российской Федерации.

Минимальный перечень типов событий ИБ, подлежащих регистрации приведен в Приложении 2 к настоящему Методическому руководству.

4.2.1. Регистрация признаков возможного возникновения компьютерных инцидентов автоматизированным способом

Регистрация признаков возможного возникновения компьютерных инцидентов автоматизированным способом осуществляется с использованием средства управления событиями информационной безопасности (при наличии такового, при отсутствии с использованием средств защиты информации и журналов безопасности программных

и программно-аппаратных средств) на основе правил регистрации признаков возможного возникновения компьютерных инцидентов.

Правила регистрации признаков возможного возникновения компьютерных инцидентов должны позволять реализовать один или совокупность следующих методов анализа, направленных на выявление причинно-следственной связи между событиями безопасности и иными данными мониторинга:

– сигнатурные методы, основанные на сопоставлении конкретных признаков и условий взаимосвязей событий безопасности и иных данных мониторинга;

– бессигнатурные методы, основанные на выявлении статистической и иной зависимости между событиями безопасности и иными данными мониторинга, и формировании профилей функционирования информационных ресурсов.

Сигнатурные методы анализа включают правила регистрации признаков возможного возникновения компьютерных инцидентов, создание и настройку которых осуществляет специалист подразделения, ответственного за управление компьютерными инцидентами.

Бессигнатурные методы анализа реализуются разработчиком средства управления событиями информационной безопасности в программном коде средства, алгоритмы которых не могут быть изменены специалистом подразделения, ответственного за управление компьютерными инцидентами.

Решение о наличии или отсутствии признака возможного возникновения компьютерного инцидента принимается на основе правил регистрации признаков возможного возникновения компьютерных инцидентов.

4.2.2. Регистрация признаков возможного возникновения компьютерных инцидентов неавтоматизированным способом

Регистрация признаков возможного возникновения компьютерных инцидентов неавтоматизированным способом осуществляется специалистами подразделения, ответственного за управление компьютерными инцидентами, при самостоятельном анализе событий безопасности в ходе мониторинга или при получении соответствующей информации от сотрудников Организации. Неавтоматизированная регистрация признаков возможного возникновения компьютерных инцидентов осуществляется в средстве управления инцидентами путем внесения в карточку признака возможного возникновения компьютерного инцидента необходимой информации (при отсутствии средства управления инцидентами в Журнал регистрации инцидентов ИБ, Приложение 1 к настоящему Методическому руководству).

4.3. Подтверждение компьютерных инцидентов

Подтверждение компьютерного инцидента осуществляется в ходе проведения проверки зарегистрированного признака возможного возникновения компьютерного инцидента.

Такая проверка проводится специалистами, ответственными за реагирование на компьютерные инциденты (руководителями рабочих групп реагирования на компьютерные инциденты).

Специалисты, ответственные за реагирование на компьютерные инциденты (руководители рабочих групп реагирования на компьютерные инциденты), осуществляют следующую деятельность:

– проведение проверки фактов возникновения компьютерных инцидентов с целью их подтверждения;

– регистрация компьютерных инцидентов в случае их подтверждения;

– контроль выполнения этапов реагирования на компьютерные инциденты.

При осуществлении контроля выполнения этапов реагирования на компьютерные инциденты специалист, ответственный за реагирование на компьютерный инцидент (руководитель рабочей группы реагирования на компьютерные инциденты), должен принимать решение о необходимости привлечения организации, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

Проверка факта возникновения компьютерного инцидента предусматривает выполнение следующих процедур:

1) анализ информации, содержащейся в карточке признака возможного возникновения компьютерного инцидента;

2) сбор дополнительной информации, требуемой для подтверждения факта возникновения компьютерного инцидента (при необходимости), в ходе которого могут выполняться:

а) опрос пользователей информационных ресурсов, вовлеченных в компьютерный инцидент;

б) опрос специалистов подразделений, ответственных за эксплуатацию информационных ресурсов, вовлеченных в компьютерный инцидент;

в) получение данных о функционировании сервисов, обеспечивающих реализацию критических процессов организации;

г) проверка журналов событий на предмет наличия свидетельств о несанкционированном просмотре, изменении или удалении информации;

д) иные действия, позволяющие получить информацию, необходимую для принятия решения о регистрации компьютерного инцидента.

Карточка признака возможного возникновения компьютерного инцидента должна содержать информацию обо всех событиях безопасности и иных данных мониторинга, которые послужили основанием для регистрации признака возможного возникновения компьютерного инцидента.

Для проведения проверки факта возникновения компьютерного инцидента специалисту, ответственному за реагирование на компьютерный инцидент (руководителю рабочей группы реагирования на компьютерные инциденты), требуется следующая информация:

– подтверждающая или опровергающая факт приведения информационного ресурса в состояние, при котором он полностью или частично не может обрабатывать информацию, необходимую для обеспечения критических процессов, и/или осуществлять управление, контроль или мониторинг критических процессов;

– подтверждающая или опровергающая факт нарушения безопасности информации, необходимой для обеспечения критических процессов (нарушение ее конфиденциальности, целостности и/или доступности).

3) принятие решения о регистрации компьютерного инцидента, его приоритете и уровне влияния.

После подтверждения факта возникновения компьютерного инцидента осуществляется немедленное уведомление специалистов, входящих в состав рабочей группы, назначенной для реагирования на зарегистрированный компьютерный инцидент.

Также осуществляется уведомление исполнительного органа государственной власти Свердловской области (Министерства), осуществляющего полномочия по вопросам технической защиты информации о компьютерном инциденте. Если компьютерный инцидент входит в зону ответственности Министерства или назначенного им для этого подведомственного учреждения, данное учреждение и/или Министерство включается в рабочую группу по решению компьютерного инцидента.

В зависимости от типа компьютерного инцидента Организация или Министерство принимает решение об уведомлении правоохранительных органов или контролирующих органов в области информационной безопасности об компьютерном инциденте.

5. РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

5.1. Общие положения

Стадия «реагирование на компьютерные инциденты» состоит из следующих последовательных этапов:

– определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;
– локализация компьютерного инцидента;
– выявление последствий компьютерного инцидента;
– ликвидация последствий компьютерного инцидента;
– закрытие компьютерного инцидента.

Отдельными этапами в рамках стадии «реагирование на компьютерные инциденты» являются:

– фиксация материалов, связанных с возникновением компьютерного инцидента;
– установление причин и условий возникновения компьютерного инцидента.

Данные этапы могут проводиться параллельно с остальными этапами реагирования и даже после этапа «закрытие компьютерного инцидента». Выполнение данных этапов не влияет на закрытие компьютерного инцидента.

5.2. Определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры

На этапе «определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры» специалистами, входящими в состав рабочей группы реагирования на компьютерный инцидент, должны выполняться действия, направленные на определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры, на которых имеются признаки зарегистрированного компьютерного инцидента, с целью их дальнейшей локализации.

На рисунке 1 представлена схема организационного процесса этапа «определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры».

Схема организационного процесса этапа «определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры»

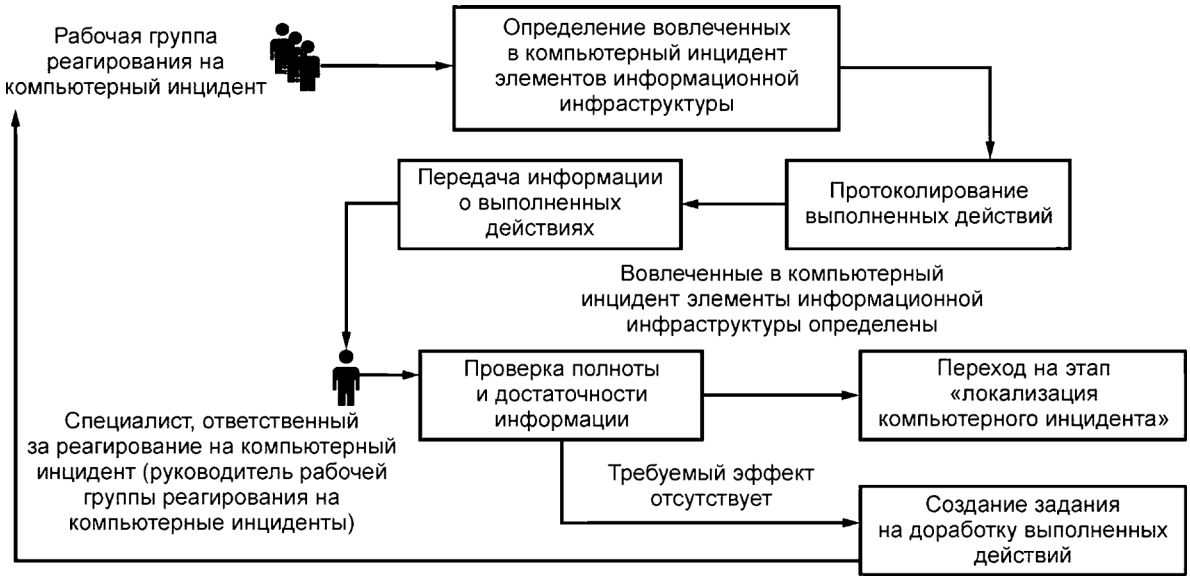

Рис. 1

Для определения вовлеченных в компьютерный инцидент элементов информационной инфраструктуры следует изучить состояние элементов информационной инфраструктуры.

Изучение состояния элементов информационной инфраструктуры допускается осуществлять с использованием программных и/или программно-технических средств, предназначенных:

1) для получения доступа к файловой системе;

2) получения доступа к журналам регистрации событий безопасности:

а) операционной системы (ОС);

б) средств защиты информации (антивирусные средства, средства обнаружения компьютерных атак и иные средства защиты информации);

в) прикладного программного обеспечения (ПО);

3) сканирования файловой системы с целью выявления вредоносного ПО;

4) проведения инвентаризации;

5) проведения анализа уязвимостей;

6) оценки работоспособности и производительности элементов информационной инфраструктуры;

7) получения информации из службы каталогов;

8) получения параметров сетевых настроек и информации о сетевой активности элементов информационной инфраструктуры;

9) анализа сетевого трафика, циркулирующего между элементами информационной инфраструктуры, а также другими функционирующими в сети Интернет ресурсами, в том числе зафиксированного в момент возникновения компьютерного инцидента (при наличии такой возможности);

10) обнаружения компьютерных атак.

5.3. Локализация компьютерного инцидента

На этапе «локализация компьютерного инцидента» специалистами, входящими в состав рабочей группы реагирования на компьютерный инцидент, должны выполняться

действия, направленные на ограничение функционирования элементов информационной инфраструктуры, вовлеченных в компьютерный инцидент, с целью предотвращения его дальнейшего распространения.

На рисунке 2 представлена схема организационного процесса этапа «локализация компьютерного инцидента».

Схема организационного процесса этапа «локализация компьютерного инцидента»

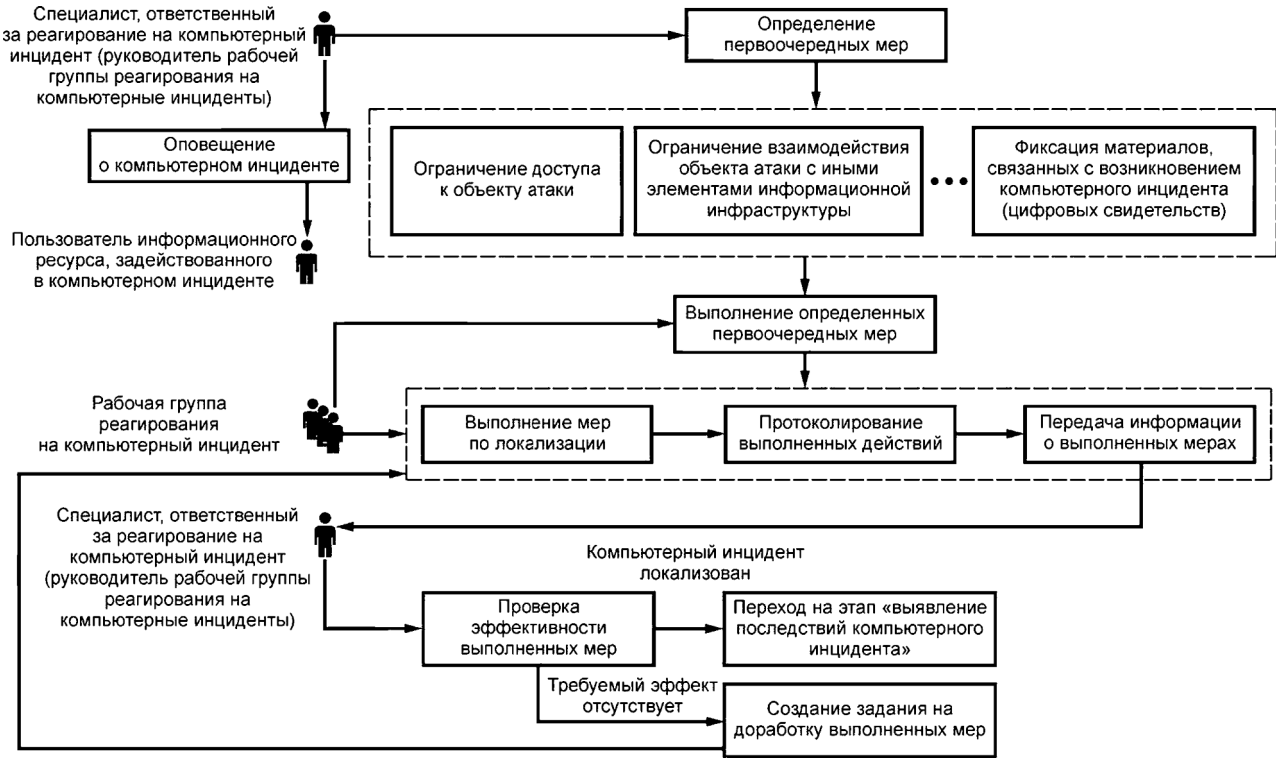

Рис. 2

К примерам возможных действий, которые могут выполняться при локализации компьютерных инцидентов, можно отнести:

– применение блокировок (использование межсетевого экрана).

Блокировки с использованием межсетевых экранов используются для предотвращения несанкционированного воздействия. Например, с использованием межсетевого экрана можно заблокировать информационные потоки с IP-адресов, с которых распространяется вредоносное ПО, шпионское ПО, а также IP-адресов почтовых ретрансляторов, источников фишинга и спама. Почтовые блокировки включают в себя фильтрацию вложений, строк темы и адреса отправителей. Для предотвращения доступа к неразрешенным или вредоносным веб-сайтам или хостам (узлам) могут применяться блокировки URL-адресов и доменных имен;

– отключение (изоляция, исключение).

Отключение зараженного элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом) от локальной вычислительной сети может предотвратить заражение остальной части информационной инфраструктуры. Отключение зараженного элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом) от сети Интернет или любых других общедоступных сетей связи может предотвратить несанкционированный доступ и, соответственно, нарушение конфиденциальности, целостности и доступности информации. В некоторых случаях

целесообразно осуществлять мониторинг вредоносной активности, ограничив при этом возможности злоумышленника атаковать другие информационные ресурсы;

– выключение.

Если дальнейшее функционирование элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом) приведет к уничтожению (потере) данных, может быть принято решение о прекращении функционирования элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом). Следует учитывать, что выключение элемента информационной инфраструктуры может отрицательно сказаться на работе конкретных пользователей, сервисов и различных критических процессов. Данное решение должно приниматься в координации с соответствующим руководителем и/или ответственными за эксплуатацию информационных ресурсов организации;

– изменения маршрутизации.

Изменения маршрутизации осуществляются с целью устранения маршрута, по которому действует злоумышленник, препятствуя ему в получении доступа к информационным ресурсам, которые могут являться объектами атаки, а также блокирования механизмов передачи (распространения) вредоносного ПО;

– отключение или блокирование процессов.

В данном случае осуществляется отключение или блокирование процессов, которые могли быть использованы злоумышленником;

– отключение учетных записей пользователей.

В данном случае осуществляется отключение учетных записей пользователей, которые могли быть использованы злоумышленником.

Любые изменения в информационных ресурсах, включая действия по локализации компьютерного инцидента, могут привести к потере (уничтожению) информации, связанной с возникновением компьютерного инцидента (цифровых свидетельств). Следует убедиться, что вся информация, необходимая для установления причин и условий возникновения компьютерных инцидентов (цифровые свидетельства), собрана в полном объеме перед внесением каких-либо системных изменений.

5.4. Выявление последствий компьютерного инцидента

На этапе «выявление последствий компьютерного инцидента» специалистами, входящими в состав рабочей группы реагирования на компьютерный инцидент, должны выполняться действия, направленные на выявление признаков негативного воздействия на элементы информационной инфраструктуры, вовлеченные в компьютерный инцидент.

При выявлении признаков негативного воздействия на элементы информационной инфраструктуры, вовлеченные в компьютерный инцидент, специалисты, входящие в состав рабочей группы реагирования на компьютерный инцидент, должны провести детальный анализ имеющихся данных о компьютерном инциденте.

На рисунке 3 представлена схема организационного процесса этапа «выявление последствий компьютерного инцидента».

К примерам признаков негативного воздействия на элементы информационной инфраструктуры, вовлеченные в компьютерный инцидент, которые выявляются в ходе анализа имеющихся данных о компьютерном инциденте, можно отнести следующее:

– нештатная сетевая активность элемента информационной инфраструктуры;

– созданные, модифицированные, удаленные файлы, каталоги, параметры настройки ОС, средств защиты информации, прикладного ПО;

– отклонения от эталонных (допустимых) параметров конфигурации ОС, средств защиты информации, прикладного ПО;

– отклонения от эталонного (допустимого) состава прикладного ПО, установленного в ОС;

– отклонения от эталонного (допустимого) содержания системных и защищаемых файлов;

– выполненные потенциально вредоносные команды, в том числе расположенные в оперативной памяти;

– признаки, идентифицирующие источник компьютерной атаки;

– признаки сбоев, перезагрузок, остановок и других нарушений в штатной работе ОС, средств защиты информации, прикладного ПО;

Схема организационного процесса этапа «выявление последствий компьютерного инцидента»

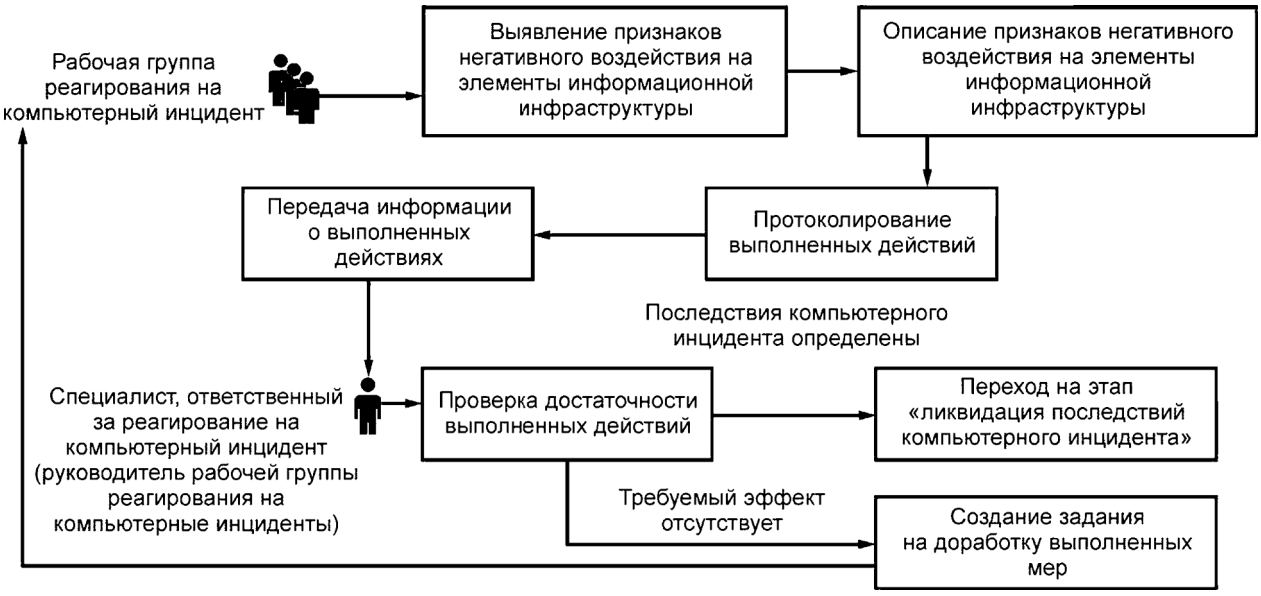

Рис. 3

– признаки нарушений функционирования сетевых служб, аномального использования системных ресурсов;

– другая информация, характерная для отдельных типов компьютерных инцидентов и компьютерных атак.

5.5. Ликвидация последствий компьютерного инцидента

На этапе «ликвидация последствий компьютерного инцидента» специалистами, входящими в состав рабочей группы реагирования на компьютерный инцидент, должны выполняться действия, направленные на устранение последствий негативного влияния компьютерного инцидента на информационный ресурс (по возможности) и/или восстановление элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом) и/или обрабатываемой в нем информации.

На рисунке 4 представлена схема организационного процесса этапа «ликвидация последствий компьютерного инцидента».

Схема организационного процесса этапа «ликвидация последствий компьютерного инцидента»

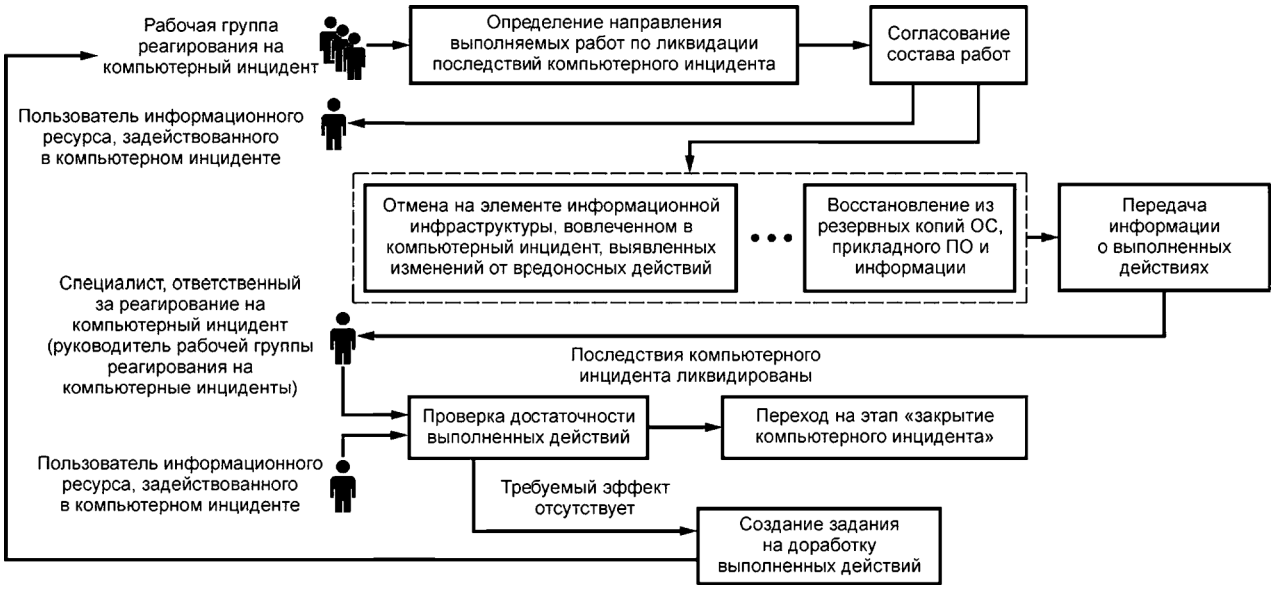

Рис. 4

К примерам возможных действий, которые могут быть выполнены для ликвидации последствий компьютерного инцидента, приведшего к негативным последствиям на уровне сети, можно отнести:

1) внесение изменений в параметры настроек ОС, средств защиты информации и прикладного ПО, функционирующего в информационных ресурсах, вовлеченных в компьютерный инцидент;

2) отключение неиспользуемых функций телекоммуникационного оборудования (например, отключение уязвимых сервисов или протоколов, которые использовались для распространения вредоносного ПО);

3) смена аутентификационной информации скомпрометированных учетных записей пользователей:

а) на телекоммуникационном оборудовании;

б) средствах межсетевого экранирования;

в) средствах защиты от компьютерных атак, направленных на отказ в обслуживании;

4) внесение изменений в правила фильтрации межсетевых экранов;

5) внесение изменений в параметры очистки трафика в средствах защиты от компьютерных атак, направленных на отказ в обслуживании;

6) подключение резервных ресурсов (каналы связи, серверное оборудование, виртуальные машины, оборудование из состава запасных инструментов и принадлежностей);

7) миграция (перемещение) виртуальных машин в сторонние виртуальные инфраструктуры.

К примерам возможных мер, которые могут быть приняты для ликвидации последствий компьютерного инцидента, приведшего к негативным последствиям на уровне прикладного ПО, можно отнести:

– выполнение настройки безопасной конфигурации прикладного или специального ПО, вовлеченного в компьютерный инцидент;

– восстановление из актуальных резервных копий файлов, баз данных, конфигурационных файлов, подвергшихся модификации при компьютерном инциденте;

– восстановление удаленных файлов, в том числе с использованием специальных

инструментальных средств;

– удаление ПО, вовлеченного в компьютерный инцидент, и всех его файлов с последующей установкой актуальной версии данного ПО и актуальных обновлений безопасности.

К примерам возможных мер, которые могут быть приняты для ликвидации последствий компьютерного инцидента, приведшего к негативным последствиям на уровне ОС, можно отнести:

– удаление вредоносного ПО;

– отмена изменений, внесенных вредоносным ПО (например, удаление созданных вредоносным ПО файлов, отмена выполненных изменений в конфигурации и настройках ОС, удаление созданных вредоносным ПО учетных записей);

– смена аутентификационной информации для скомпрометированных учетных записей пользователей в ОС;

– восстановление средств защиты информации, функционирующих в среде ОС;

– восстановление ОС в целом;

– настройка безопасной конфигурации средств защиты информации, функционирующих в среде ОС;

– настройка безопасной конфигурации ОС;

– переустановка ОС и прикладного ПО с последующей установкой актуальных обновлений безопасности.

5.6. Закрытие компьютерного инцидента

Решение о закрытии компьютерного инцидента принимается по результатам проверки специалистом, ответственным за реагирование на компьютерный инцидент (руководителем рабочей группы реагирования на компьютерный инцидент), в ходе которой определяется полнота выполненных и запротоколированных действий по реагированию на компьютерный инцидент, выполненных на каждом этапе реагирования на компьютерный инцидент.

Карточки компьютерных инцидентов после закрытия соответствующих компьютерных инцидентов не должны удаляться, так как они могут быть использованы в дальнейшем как типовые шаблоны действий по реагированию на аналогичные компьютерные инциденты и при проведении анализа деятельности по их управлению.

Карточки закрытых компьютерных инцидентов могут использоваться в качестве типовых шаблонов действий по реагированию на аналогичные компьютерные инциденты в организации с целью формирования базы знаний, доступной специалистам, входящим в состав рабочих групп реагирования на компьютерные инциденты при работе с новыми компьютерными инцидентами.

6. ФИКСАЦИЯ МАТЕРИАЛОВ, СВЯЗАННЫХ С ВОЗНИКНОВЕНИЕМ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ, И УСТАНОВЛЕНИЕ ПРИЧИН И УСЛОВИЙ ИХ ВОЗНИКНОВЕНИЯ

6.1. Фиксация материалов, связанных с возникновением компьютерных инцидентов

Состав материалов, связанных с возникновением компьютерных инцидентов (цифровых свидетельств), подлежащих фиксации, зависит от типа компьютерного инцидента и его последствий.

В рамках реагирования на компьютерные инциденты могут фиксироваться следующие материалы, связанные с возникновением компьютерных инцидентов (цифровые свидетельства):

– электронные образы штатных машинных носителей информации средств вычислительной техники и/или съемных машинных носителей информации;

– содержимое рабочей памяти (дамп) процесса, ядра ОС или ОС в целом;

– сетевой трафик, циркулирующий между вовлеченными в компьютерный инцидент элементами информационной инфраструктуры, а также между этими элементами и элементами других функционирующих в сети Интернет ресурсов;

– образцы вредоносного ПО;

– отдельные файлы, такие как журналы регистрации событий безопасности, файлы реестра ОС, системные и пользовательские файлы;

– сообщения электронной почты;

– снимки состояния виртуальных машин.

6.2. Установление причин и условий возникновения компьютерных инцидентов

Деятельность по установлению причин и условий возникновения компьютерных инцидентов направлена на определение факторов, обусловивших возможность возникновения компьютерного инцидента и/или способствовавших его возникновению.

Существуют различные виды анализа зафиксированных материалов, связанных с возникновением компьютерных инцидентов (цифровых свидетельств), которые могут быть выполнены для установления причин и условий их возникновения. К таким видам относятся:

– анализ действий пользователей.

К сведениям, подлежащим изучению в ходе анализа действий пользователей, относятся:

– действия пользователей, которые выполнялись до и во время регистрации компьютерного инцидента (например, посещение веб-сайта, открытие сообщения электронной почты, открытие электронного документа, подключение носителя информации и другие);

– сведения об игнорировании пользователем появляющихся сообщений ОС, средств защиты информации и прикладного ПО (например, о необходимости выполнить обновление ОС, ее перезагрузку, о выявленном потенциально вредоносном файле);

– анализ ОС элемента информационной инфраструктуры.

К сведениям, подлежащим изучению в ходе анализа ОС элемента информационной инфраструктуры, относятся:

– журналы (протоколы) регистрации событий безопасности ОС, средств защиты информации и прикладного ПО;

– информация о запущенных программных процессах;

– информация об установленных сетевых сессиях и открытых сетевых портах;

– реестр ОС (при наличии);

– информация об атрибутах объектов файловой системы;

– состав учетных записей пользователей и их прав;

– анализ защищенности.

Анализ защищенности является процессом изучения информации об актуальных уязвимостях ОС, средств защиты информации и прикладного ПО, функционирующего в информационных ресурсах, вовлеченных в компьютерный инцидент.

К сведениям, подлежащим изучению в ходе анализа защищенности, относятся:

– существующие результаты проведения мероприятий по анализу защищенности информационных ресурсов;

– сетевая конфигурация ОС, прикладного ПО;

– групповые политики безопасности ОС;

– функциональные параметры настроек прикладного ПО, служб ОС;

– состав установленных (неустановленных) актуальных обновлений безопасности

ОС, средств защиты информации и прикладного ПО;

– состав программного и аппаратного обеспечения элементов информационной инфраструктуры, вовлеченных в компьютерный инцидент;

– анализ сетевого трафика.

К сведениям, подлежащим изучению в ходе анализа сетевого трафика, относятся:

– копия сетевого трафика и/или его фрагменты, зафиксированные средствами записи (анализа) сетевого трафика, из (в) сегмента (сегмент) локальной вычислительной сети, в котором расположен элемент информационной инфраструктуры, вовлеченный в компьютерный инцидент;

– копия сетевого трафика и/или его фрагменты, зафиксированные средством обнаружения компьютерных атак (системой обнаружения вторжений) или иными средствами выявления угроз безопасности информации;

– статистическая и иная информация о потоках сетевого трафика между элементом информационной инфраструктуры, вовлеченным в компьютерный инцидент и вероятным источником компьютерной атаки, а также между элементом информационной инфраструктуры, вовлеченным в компьютерный инцидент, и другими сетевыми устройствами локальной вычислительной сети;

– статистическая и иная информация о потоках сетевого трафика, зафиксированная телекоммуникационным оборудованием или специализированными средствами;

Потоком сетевого трафика считается набор сетевых кадров, проходящих в одном направлении к одному сетевому устройству в рамках одного сетевого сеанса.

– анализ программных и информационных объектов.

Для анализа программных объектов допускается выполнять следующие процедуры:

– обратная разработка исполняемых и бинарных файлов путем дизассемблирования их машинного кода, декомпиляции (восстановления) программного кода до исходного (первоначального), использования режима отладки программного кода;

– изучение поведения программных объектов и влияния их на среду функционирования, файловую систему в автоматизированной замкнутой системе (среде) предварительного выполнения программ.

При установлении причин и условий возникновения компьютерного инцидента допускается проводить несколько видов анализа. Уровень или глубина проводимого анализа часто может зависеть от поставленной в организации задачи.

7. АНАЛИЗ РЕЗУЛЬТАТОВ ДЕЯТЕЛЬНОСТИ ПО УПРАВЛЕНИЮ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

7.1. Общие положения

Стадия «анализ результатов деятельности по управлению компьютерными инцидентами» включает в себя следующие этапы:

– приобретение и накопление опыта по результатам управления компьютерными инцидентами;

– разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов;

– оценка результатов и эффективности реагирования на компьютерные инциденты.

7.2. Приобретение и накопление опыта по результатам управления компьютерными инцидентами

Процесс приобретения и накопления опыта является важной составляющей ведения деятельности по управлению компьютерными инцидентами. После завершения всех этапов реагирования на компьютерный инцидент важно, чтобы организация приобрела и накопила опыт управления компьютерными инцидентами.

Приобретение и накопление опыта по результатам управления компьютерными инцидентами позволяет:

– идентифицировать методы и способы обнаружения и регистрации компьютерных инцидентов и реагирования на компьютерные инциденты, которые показали свою эффективность в отношении уже закрытых компьютерных инцидентов;

– доработать (актуализировать) документацию в части управления компьютерными инцидентами, в том числе настоящее Методическое руководство и план реагирования на компьютерные инциденты.

Все изменения (корректировки, дополнения), предлагаемые к внесению в план реагирования на компьютерные инциденты, относящиеся к этапам «обнаружение и регистрация компьютерных инцидентов» и «реагирование на компьютерные инциденты», должны быть надлежащим образом проверены и протестированы, т. е. должны быть проведены тренировки по отработке мероприятий плана реагирования на компьютерные инциденты в соответствии с положениями ГОСТ Р 59711.

7.3. Разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов

По результатам реагирования на компьютерные инциденты и установления причин и условий их возникновения следует разрабатывать рекомендации по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов. Такие рекомендации могут включать:

– рекомендации по принятию дополнительных мер защиты информации в соответствии с нормативными правовыми актами и методическими документами уполномоченных федеральных органов исполнительной власти (ФСБ России и ФСТЭК России), в том числе доработку (актуализацию) и/или разработку документации, регламентирующей вопросы обеспечения безопасности организации;

– рекомендации по повышению защищенности информационных ресурсов от компьютерных атак;

– рекомендации по устранению технических причин и условий, способствующих проведению деструктивного воздействия на информационные ресурсы.

7.4. Оценка результатов и эффективности реагирования на компьютерные инциденты

После завершения всех этапов реагирования на компьютерный инцидент следует проводить оценку результатов и эффективности предпринятых действий.

Такая оценка направлена на то, чтобы определить, насколько эффективны те или иные процессы и процедуры реагирования на компьютерные инциденты.

Оценку результатов и эффективности действий, предпринятых на каждом этапе реагирования на компьютерный инцидент, целесообразно проводить в отношении компьютерных инцидентов со средним, высоким и критическим уровнями влияния и на основании задокументированных результатов реагирования.

Также, после завершения всех этапов реагирования на компьютерный инцидент, целесообразно проводить рабочие совещания со специалистами всех подразделений, участвующих в деятельности по управлению компьютерными инцидентами на стадиях «обнаружение и регистрация компьютерных инцидентов» и «реагирование на компьютерные инциденты».

На рабочем совещании целесообразно обсудить следующие вопросы:

– оценка достаточности и эффективности процессов и процедур реагирования на компьютерные инциденты, изложенных в плане;

– предложения по включению в план реагирования на компьютерные инциденты дополнительных процессов и процедур, которые могли бы повысить эффективность действий, выполняемых на стадиях «обнаружение и регистрация компьютерных инцидентов» и «реагирование на компьютерные инциденты»;

– предложения по использованию дополнительных инструментальных средств с целью повышения эффективности реагирования и установления причин и условий возникновения компьютерных инцидентов;

– оценка эффективности обмена информацией о компьютерных инцидентах между всеми сторонами, принимающими участие на стадиях «обнаружение и регистрация компьютерных инцидентов» и «реагирование на компьютерные инциденты».

Оценка результатов и эффективности реагирования на компьютерные инциденты может осуществляться на основании следующих показателей:

– среднее время проведения проверки признаков возможного возникновения компьютерных инцидентов;

– среднее время определения вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;

– среднее время локализации компьютерных инцидентов;

– среднее время выявления последствий компьютерных инцидентов;

– среднее время ликвидации последствий компьютерных инцидентов;

– среднее время реагирования на компьютерные инциденты;

– процент компьютерных инцидентов, для которых были нарушены сроки выполнения этапов реагирования.

8. ОТВЕТСТВЕННОСТЬ

Требования настоящего документа обязательны для выполнения всеми сотрудниками Организации согласно назначенным ролям и должностным (трудовым) обязанностям.

Сотрудники, нарушившие положения настоящего документа, привлекаются к ответственности, установленной законодательством Российской Федерации.

Настоящее Методическое руководство, в том числе предупреждение об ответственности, доводится до всех сотрудников под роспись.

Приложение № 1.
к типовому методическому руководству
по организации технических мероприятий,
направленных на проведение служебных проверок
при возникновении компьютерных инцидентов

Таблица 1

ЖУРНАЛ
Регистрации инцидентов ИБ

№ п/п	Время и дата обнаружения инцидента	Время и дата закрытия инцидента	Описание инцидента	Участники реагирования	Затронутые ресурсы Организации и процессы	Причины	Выводы и рекомендации по результатам закрытия инцидента
1							
2							
3							

Приложение № 2
к типовому методическому руководству
по организации технических мероприятий,
направленных на проведение служебных проверок
при возникновении компьютерных инцидентов

Таблица 2

МИНИМАЛЬНЫЙ ПЕРЕЧЕНЬ ТИПОВ СОБЫТИЙ ИБ

№ п/п	Уровень инцидента ИБ	Тип событий ИБ
1.	Физический уровень информационной инфраструктуры	**1.** Физический доступ работников и иных лиц в здания и помещения; **2.** Физический доступ работников и иных лиц к средствам вычислительной техники и их использование; **3.** Использование работниками и иными лицами устройств копирования и многофункциональных устройств; **4.** Изменение параметров настроек средств вычислительной техники, телекоммуникационного оборудования; **5.** Изменение параметров настроек оборудования, обеспечивающего функционирование средств вычислительной техники; **6.** Сбои и отказы в работе: средств вычислительной техники, телекоммуникационного оборудования, оборудования, обеспечивающего функционирование средств вычислительной техники, средств защиты информации, сетей передачи данных; **7.** Физическое воздействие на средства вычислительной техники, телекоммуникационное оборудование, средства защиты информации и сети передачи данных; **8.** Изменения параметров функционирования сетей передачи данных; **9.** Замена и (или) модификация программных и (или) аппаратных частей средств вычислительной техники, телекоммуникационного оборудования; **10.** Осуществление действий с носителями информации, в том числе вынос за пределы

№ п/п	Уровень инцидента ИБ	Тип событий ИБ
		контролируемой зоны носителей информации; **11.** Вынос за пределы контролируемой зоны переносных средств вычислительной техники; **12.** Использование переносных средств вычислительной техники на территории организации; **13.** Передача средств вычислительной техники между структурными подразделениями; **14.** Передача средств вычислительной техники во внешние организации; **15.** Проведение работниками и иными лицами фото- и (или) видеосъемки в зданиях или помещениях; **16.** Проведение мероприятий по доступу к телевизионным системам охранного наблюдения, охранной сигнализации, системам контроля и управления доступом; **17.** События, формируемые телевизионными системами охранного наблюдения, охранной сигнализации, системами контроля и управления доступом; **18.** Осуществление действий с носителями информации и системами, позволяющими осуществить физический доступ в здания и помещения.
2.	Уровень сетевого оборудования	**1.** Изменение параметров настроек сетевого оборудования и программного обеспечения сетевого оборудования; **2.** Изменение состава и версий программного обеспечения сетевого оборудования; **3.** Обнаружение аномальной сетевой активности; **4.** Аутентификация и завершение сеанса работы на сетевом оборудовании; **5.** Обнаружение вредоносного кода и его проявлений; **6.** Изменение топологии вычислительных сетей; **7.** Подключение оборудования к вычислительным сетям; **8.** Сбои в работе программного обеспечения сетевого оборудования; **9.** Обновление программного обеспечения сетевого оборудования; **10.** Выполнение операций по техническому обслуживанию сетевого оборудования; **11.** Использование средств анализа уязвимостей сетевого оборудования; **12.** Отключение/перезагрузка сетевого оборудования; **13.** Обнаружение атак типа «отказ в обслуживании»; **14.** Смена и (или) компрометация аутентификационных данных, используемых для доступа к сетевому оборудованию;

№ п/п	Уровень инцидента ИБ	Тип событий ИБ
		15. Сбои в работе средств защиты информации; **16.** Изменение параметров работы средств защиты информации; **17.** Запуск средств анализа топологии вычислительной сети.
3.	Уровень сетевых приложений и сервисов	**1.** Идентификация, аутентификация, авторизация и завершение сеанса работников и иных лиц; **2.** Изменение параметров настроек, состава и версий программного обеспечения; **3.** Обнаружение вредоносного кода и его проявлений; **4.** Установление соединений и обработка запросов, в том числе удаленных, на уровне сетевых приложений и сервисов; **5.** Сбои и отказы в работе сетевых приложений и сервисов; **6.** Выполнение операций, связанных с эксплуатацией и администрированием сетевых приложений и сервисов; **7.** Обнаружение нетипичных (аномальных) запросов на уровне сетевых приложений и сервисов; **8.** Отключение/перезагрузка или приостановление работы сетевых приложений и сервисов; **9.** Выполнение операций по предоставлению доступа к использованию сетевых приложений и сервисов, в том числе использованию электронной почты и сети Интернет; **10.** Выполнение операции по архивированию данных сетевых приложений и сервисов, в том числе данных электронной почты; **11.** Сбои в осуществлении обменом сообщениями; **12.** Завершение/приостановка выполнения сетевых приложений и сервисов по ошибке; **13.** Распространение и (или) сбор информации с использованием сетевых приложений и сервисов; **14.** Выполнение операций со списками рассылки и адресными книгами; **15.** Наделение работников и (или) иных лиц правами пользователя конкретного пакета сервисов, в том числе сервисов и ресурсов сети Интернет; **16.** Использование средств анализа уязвимостей сетевых приложений и сервисов; **17.** Смена и (или) компрометация аутентификационных данных, используемых для осуществления доступа к сетевым приложениям и сервисам; **18.** Сбои в работе средств защиты информации; **19.** Распространение информации, побуждающей работника сообщать информацию, необходимую для осуществления действий от его имени; **20.** Распространение информации, побуждающей работника совершить действия (переход по

№ п/п	Уровень инцидента ИБ	Тип событий ИБ
		ссылке, открытие вложения, тд.) не характерную для штатного режима его работы (например, требования по совершению действий, которые он ранее не получал/совершал) и (или) канала информационного взаимодействия, который он использует; **21.** Внешние воздействия из сети Интернет, в том числе сетевые атаки; **22.** Выполнение операций со средствами криптографической защиты информации и ключевой информацией. **23.** Выделение и назначение ролей, в том числе ролей, связанных с обеспечением ИБ.
4.	Уровень операционных систем	**1.** Аутентификация и завершение работы работников и иных лиц, в том числе на уровне системного программного обеспечения, систем управления базами данных и прикладного программного обеспечения, программного обеспечения ИСПДн (далее – ПО ИС); **2.** Изменение параметров конфигурации, состава и версий ПО ИС; **3.** Запуск, остановка и (или) отключение/перезагрузка ПО ИС; **4.** Обнаружение вредоносного кода и его проявлений; **5.** Установление соединений и обработка запросов с использованием ПО ИС; **6.** Сбои в работе ПО ИС; **7.** Выполнение операций, связанных с эксплуатацией и администрированием ПО ИС; **8.** Обнаружение нетипичных запросов с использованием ПО ИС; **9.** Сбои и отказы в работе средств защиты информации; **10.** Изменение параметров конфигурации средств защиты информации; **11.** Выполнение операций по предоставлению доступа к ПО ИС и информационным ресурсам, обрабатываемым с использованием ПО ИС; **12.** Выполнение операций по архивированию, резервированию и восстановлению информации; **13.** Завершение/приостановка работы ПО ИС по ошибке; **14.** Использование средств анализа уязвимостей ПО ИС; **15.** Смена и (или) компрометация аутентификационных данных, используемых для доступа к ПО ИС, и информационным ресурсам, обрабатываемым с использованием ПО ИС; **16.** Изменение параметров конфигурации средств защиты информации; **17.** Внешние воздействие из сети Интернет на ПО ИС; **18.** Создание, уничтожение или изменение информационных ресурсов, баз данных и (или) иных массивов информации;

№ п/п	Уровень инцидента ИБ	Тип событий ИБ
		19. Компрометация аутентификационных данных и ключевой информации; **20.** Выполнение операций со средствами криптографической защиты информации и ключевой информацией. **21.** Выделение и назначение ролей, в том числе ролей, связанных с обеспечением ИБ.