ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59712— 2022

Защита информации

УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

Руководство по реагированию на компьютерные инциденты

Издание официальное

Москва
Российский институт стандартизации
2022

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным казенным учреждением «Войсковая часть 43753» (в/ч 43753), Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2022 г. № 1378-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2022

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Общие положения 2
5 Обнаружение и регистрация компьютерных инцидентов 2
6 Реагирование на компьютерные инциденты 5
7 Фиксация материалов, связанных с возникновением компьютерных инцидентов, и установление причин и условий их возникновения 11
8 Анализ результатов деятельности по управлению компьютерными инцидентами 12

Введение

Серия стандартов «Управление компьютерными инцидентами» определяет единый структурированный подход к организации и ведению деятельности по управлению компьютерными инцидентами в рамках функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

В соответствии с ГОСТ Р 59710 структурированный подход к организации и ведению деятельности по управлению компьютерными инцидентами предусматривает следующие стадии управления компьютерными инцидентами:

- организация деятельности по управлению компьютерными инцидентами;
- обнаружение и регистрация компьютерных инцидентов;
- реагирование на компьютерные инциденты;
- анализ результатов деятельности по управлению компьютерными инцидентами.

Настоящий стандарт определяет содержание этапов, выполняемых на следующих стадиях:

- обнаружение и регистрация компьютерных инцидентов;
- реагирование на компьютерные инциденты;
- анализ результатов деятельности по управлению компьютерными инцидентами.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

Руководство по реагированию на компьютерные инциденты

Information protection. Computer incident management.Guide to responding to computer incident

Дата введения — 2023—02—01

1 Область применения

Настоящий стандарт определяет содержание этапов, выполняемых на следующих стадиях управления компьютерными инцидентами:

- обнаружение и регистрация компьютерных инцидентов;
- реагирование на компьютерные инциденты;
- анализ результатов деятельности по управлению компьютерными инцидентами.

Настоящий стандарт предназначен как для субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), самостоятельно осуществляющих управление компьютерными инцидентами в отношении собственных информационных ресурсов, так и для субъектов ГосСОПКА, в зону ответственности которых входят информационные ресурсы, принадлежащие другим субъектам ГосСОПКА (далее — организации).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 59547 Защита информации. Мониторинг информационной безопасности. Общие положения

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

ГОСТ Р 59710 Защита информации. Управление компьютерными инцидентами. Общие положения

ГОСТ Р 59711—2022 Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется

Издание официальное

применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 59709 и ГОСТ Р 59547.

4 Общие положения

Настоящий стандарт определяет содержание трех стадий управления компьютерными инцидентами, которые включают в себя соответствующие этапы:

а) обнаружение и регистрация компьютерных инцидентов:

1) регистрация признаков возможного возникновения компьютерных инцидентов;

2) подтверждение компьютерных инцидентов;

б) реагирование на компьютерные инциденты:

1) определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;

2) локализация компьютерного инцидента;

3) выявление последствий компьютерного инцидента;

4) ликвидация последствий компьютерного инцидента;

5) закрытие компьютерного инцидента;

6) фиксация материалов, связанных с возникновением компьютерного инцидента;

7) установление причин и условий возникновения компьютерного инцидента;

в) анализ результатов деятельности по управлению компьютерными инцидентами:

1) приобретение и накопление опыта по результатам управления компьютерными инцидентами;

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

3) оценка результатов и эффективности реагирования на компьютерные инциденты.

5 Обнаружение и регистрация компьютерных инцидентов

5.1 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.

Примечание — Сбор информации о событиях безопасности и иных данных мониторинга, необходимых для обнаружения компьютерных инцидентов, осуществляется в соответствии с ГОСТ Р 59547.

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

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

5.2 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 работников организации).

Примечание — Понятие «признак возможного возникновения компьютерных инцидентов» применяют в связи с тем, что средства управления событиями информационной безопасности фиксируют возникновение ситуации, которая может свидетельствовать о возникновении компьютерного инцидента, а не сам факт его возникновения.

5.2.1 Регистрация признаков возможного возникновения компьютерных инцидентов автоматизированным способом

Регистрация признаков возможного возникновения компьютерных инцидентов автоматизированным способом осуществляется с использованием средства управления событиями информационной безопасности 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.

Примечание — Профиль функционирования формируется по результатам поведенческого анализа, который содержит набор атрибутов и их значений. Такие данные характеризуют работу конкретного приложения в среде функционирования в определенный промежуток времени.

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.

Примечание — Правила регистрации признаков возможного возникновения компьютерных инцидентов могут содержать условия отбора событий безопасности и иных данных мониторинга в виде отдельных логических операций, например конъюнкция («И»), дизъюнкция («ИЛИ»), отрицание («НЕ») и их комбинаций, критерии срабатывания правила, учитывающие количественные, временные и иные характеристики событий безопасности и иных данных мониторинга, а также результаты их сравнения («больше», «меньше», «равно» и иные). Правила регистрации признаков возможного возникновения компьютерных инцидентов также могут содержать операторы выполнения действий в зависимости от соответствия переменных (объектов, принимающих несколько значений) заданному условию, циклические и иные операторы, позволяющие повысить эффективность и точность описания критериев отбора событий безопасности и иных данных мониторинга.

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

При автоматизированном способе регистрации признака возможного возникновения компьютерных инцидентов информация о данном зарегистрированном признаке передается из средства управления событиями информационной безопасности в средство управления инцидентами, где на основании поступившей информации автоматически формируется карточка признака возможного возникновения компьютерного инцидента.

5.2.2 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 работников организации. Неавтоматизированная регистрация признаков возможного возникновения компьютерных инцидентов осуществляется в средстве управления инцидентами путем внесения в карточку признака возможного возникновения компьютерного инцидента необходимой информации.

5.3 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).

Примечания

1 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.

2 В рамках функционирования ГосСОПКА организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами, является Национальный координационный центр по компьютерным инцидентам.

Регистрируемые признаки возможного возникновения компьютерных инцидентов распределяются между специалистами, ответственными за реагирование на компьютерные инциденты (руководителями рабочих групп реагирования на компьютерные инциденты), в порядке очереди и/или с учетом предварительно определенных типов компьютерных инцидентов, и/или географического местоположения информационных ресурсов, в которых регистрируются признаки возможного возникновения компьютерных инцидентов.

Примечание — В рамках функционирования ГосСОПКА типы компьютерных инцидентов определяет организация, осуществляющая координацию деятельности в части управления компьютерными инцидентами.

Проверка факта возникновения компьютерного инцидента предусматривает выполнение следующих процедур:

а) анализ информации, содержащейся в карточке признака возможного возникновения компьютерного инцидента.

Примечание — При анализе информации, содержащейся в карточке признака возможного возникновения компьютерного инцидента, проводят оценку информации, связанной с событиями безопасности, на основании которых был зарегистрирован признак возможного возникновения компьютерных инцидентов, для определения характера влияния на информационные ресурсы с целью принятия решения о регистрации компьютерного инцидента. При необходимости осуществляют сбор и внесение дополнительной информации. В случае подтверждения компьютерного инцидента осуществляют его регистрацию и создают карточку компьютерного инцидента.

В рамках функционирования ГосСОПКА формат и содержание карточек компьютерных инцидентов, компьютерных атак и уязвимостей определяется организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами;

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

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

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

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

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

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

Примечание — 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);

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

Примечания

1 Регистрация компьютерного инцидента осуществляется, если в ходе проверки подтвержден факт возникновения компьютерного инцидента. При регистрации компьютерного инцидента следует создавать карточку компьютерного инцидента.

Регистрация компьютерного инцидента не осуществляется, если в ходе проверки установлено, что регистрация признака возможного возникновения компьютерного инцидента является ложной.

Если в ходе проверки было установлено, что причиной регистрации признака возможного возникновения компьютерного инцидента является компьютерная атака, в случаях, если компьютерный инцидент не регистрируется, то должна формироваться карточка компьютерной атаки и карточка уязвимости.

2 Приоритеты и уровни влияния компьютерного инцидента могут определяться вместе с регистрацией признака возможного возникновения компьютерного инцидента при срабатывании правила, но они должны подтверждаться специалистом, ответственным за реагирование на компьютерный инцидент (руководителем рабочей группы реагирования на компьютерные инциденты), и при необходимости уточняться.

Подход к определению уровней влияния и приоритетов компьютерных инцидентов приведен в приложениях А и Б ГОСТ Р 59711—2022.

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

Примечание — Назначение рабочих групп для реагирования на компьютерный инцидент может осуществляться автоматически средством управления инцидентами для каждого типа компьютерного инцидента или не автоматически специалистом, ответственным за реагирование на компьютерный инцидент (руководителем рабочей группы реагирования на компьютерные инциденты).

Одновременно с уведомлением специалистов, входящих в состав рабочей группы, назначенной для реагирования на зарегистрированный компьютерный инцидент, должно осуществляться уведомление организации, осуществляющей координацию деятельности в части управления компьютерными инцидентами, с направлением карточки компьютерного инцидента (в случае регистрации компьютерного инцидента) или карточек компьютерной атаки и уязвимости, которые могли быть использованы при проведении компьютерной атаки (если в ходе проверки признака возможного возникновения компьютерного инцидента было установлено, что причиной его регистрации является компьютерная атака, в случаях если компьютерный инцидент не регистрируется).

6 Реагирование на компьютерные инциденты

6.1 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.

Примечание — 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.

Описание этапов «фиксация материалов, связанных с возникновением компьютерного инцидента» и «установление причин и условий возникновения компьютерного инцидента» представлено в разделе 7.

6.2 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».

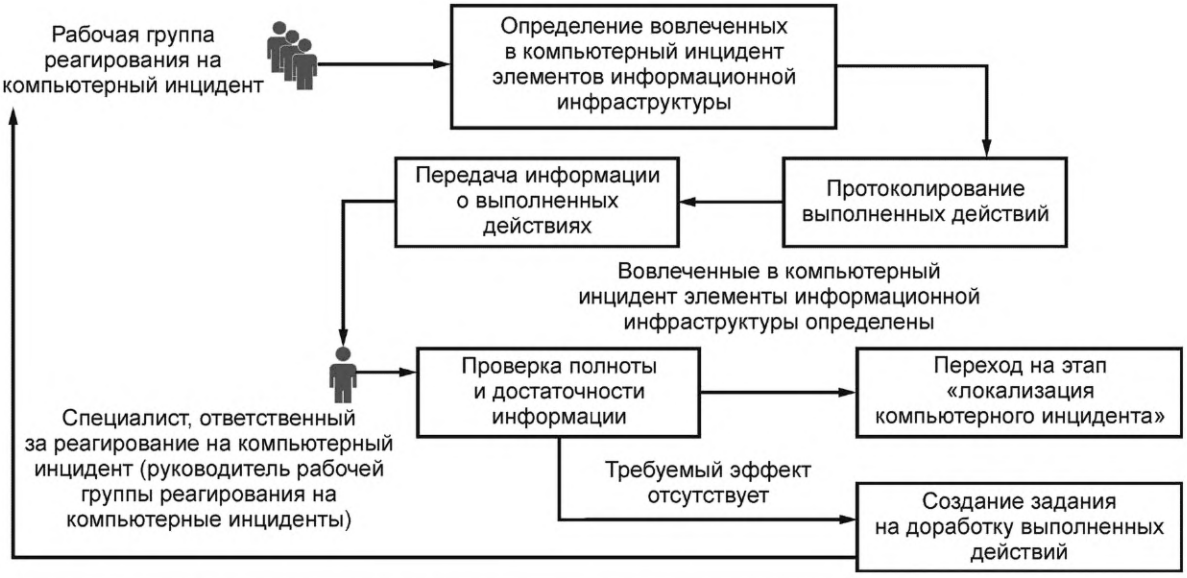

Рисунок 1 — Схема организационного процесса этапа «определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры»

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:

а) для получения доступа к файловой системе;

б) получения доступа к журналам регистрации событий безопасности:

1) операционной системы (ОС);

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

3) прикладного программного обеспечения (ПО);

в) сканирования файловой системы с целью выявления вредоносного ПО;

г) проведения инвентаризации;

д) проведения анализа уязвимостей;

е) оценки работоспособности и производительности элементов информационной инфраструктуры;

ж) получения информации из службы каталогов;

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

к) 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);

л) обнаружения компьютерных атак.

6.3 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».

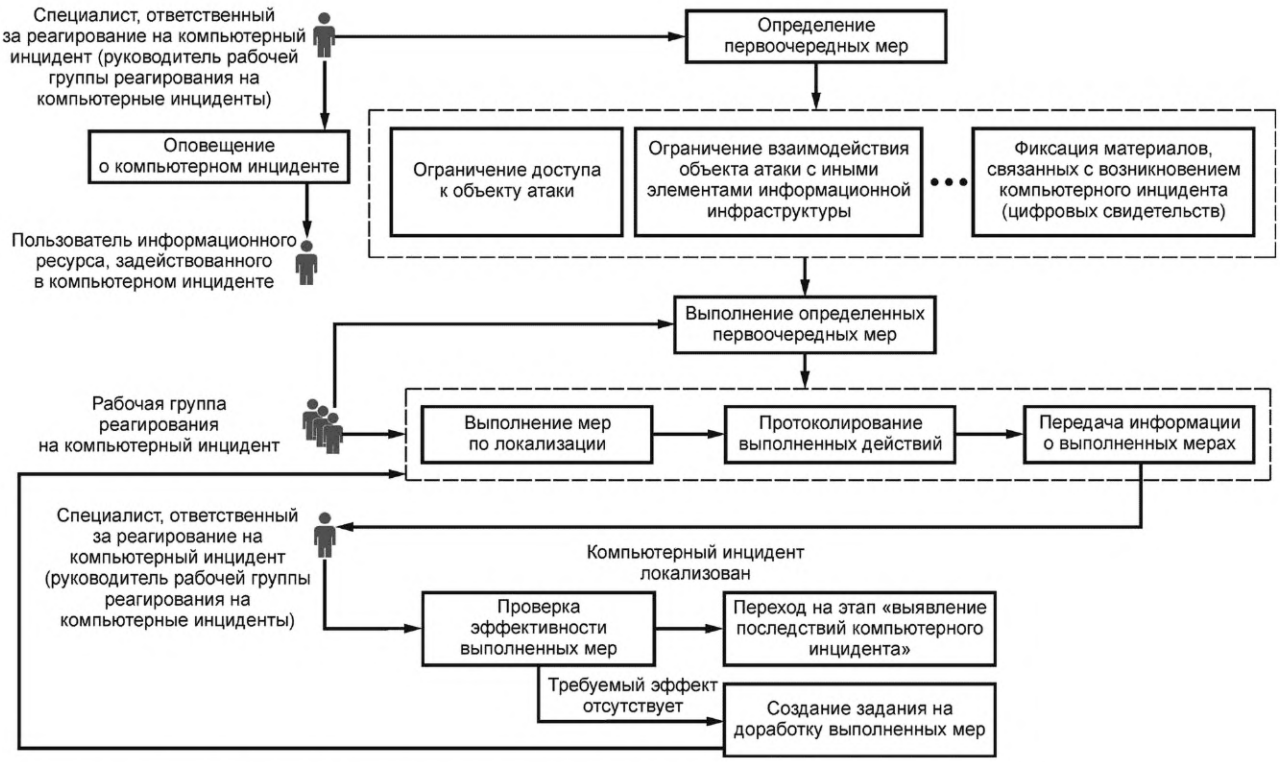

Рисунок 2 — Схема организационного процесса этапа «локализация компьютерного инцидента»

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

- применение блокировок (использование межсетевого экрана).

Примечание — 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).

Примечание — 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.

Примечание — 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.

Примечание — 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.

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

- отключение учетных записей пользователей.

Примечание — 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.

6.4 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;

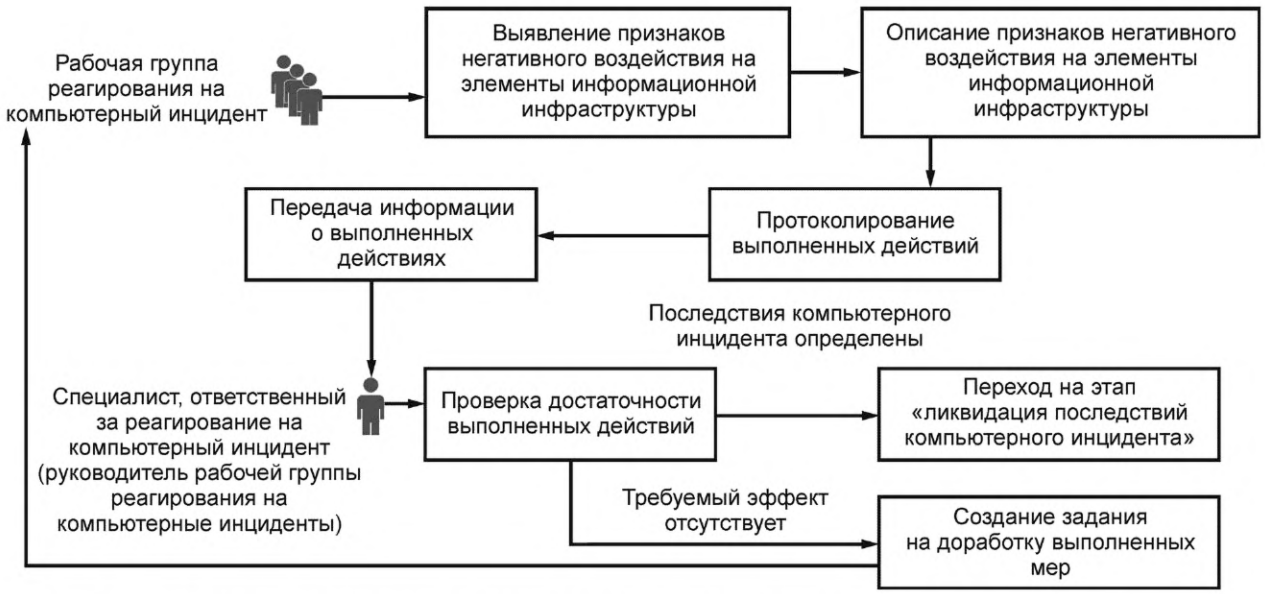

Рисунок 3 — Схема организационного процесса этапа «выявление последствий компьютерного инцидента»

- признаки нарушений функционирования сетевых служб, аномального использования системных ресурсов;
- другая информация, характерная для отдельных типов компьютерных инцидентов и компьютерных атак.

6.5 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».

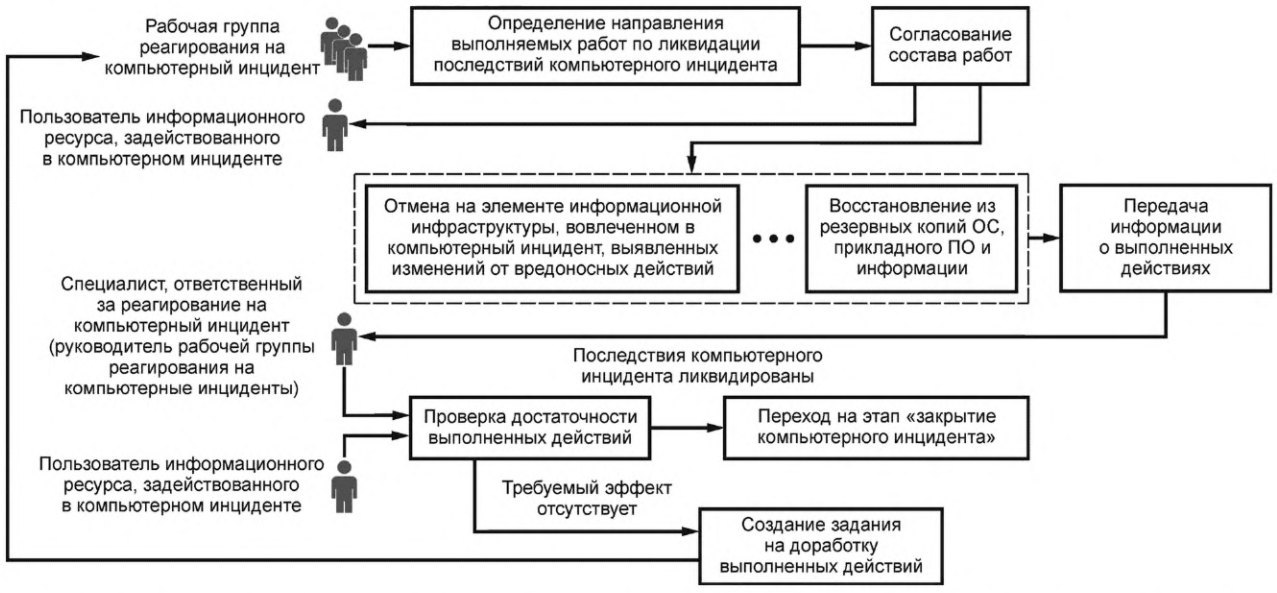

Рисунок 4 — Схема организационного процесса этапа «ликвидация последствий компьютерного инцидента»

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

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

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

в) смена аутентификационной информации скомпрометированных учетных записей пользователей:

1) на телекоммуникационном оборудовании;

2) средствах межсетевого экранирования;

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

г) внесение изменений в правила фильтрации межсетевых экранов;

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

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

ж) 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.

6.6 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.

Примечание — 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.

7 Фиксация материалов, связанных с возникновением компьютерных инцидентов, и установление причин и условий их возникновения

7.1 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.

7.2 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.

Примечание — Анализ действий пользователей является процессом изучения сведений, задокументированных в ходе опроса лица, взаимодействующего с элементом информационной инфраструктуры, вовлеченным в компьютерный инцидент в момент его возникновения.

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.

Примечание — Анализ ОС элемента информационной инфраструктуры является процессом изучения событий безопасности ОС, средств защиты информации и прикладного ПО, которые регистрировались до и во время возникновения компьютерного инцидента.

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.

Примечание — 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.

Примечание — Анализ сетевого трафика является процессом изучения сетевого трафика и информации о потоках сетевого трафика в отношении элементов информационной инфраструктуры, вовлеченных в компьютерный инцидент до, во время и после возникновения компьютерного инцидента.

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.

Примечание — Анализ программных и информационных объектов является процессом идентификации вредоносного программного кода в объектах файловой системы, в оперативной памяти средств вычислительной техники и в информационных объектах (веб-ссылки, программный код веб-страницы, карточные транзакции и иные структурированные конструкции данных), выявления в них связей с вредоносными ресурсами или ресурсами, предположительно используемыми злоумышленниками, а также определения принципа их работы.

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.

8 Анализ результатов деятельности по управлению компьютерными инцидентами

8.1 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.

8.2 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, том числе политику управления компьютерными инцидентами 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.

8.3 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.

8.4 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».

Примечание — 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.

УДК 004.622:006.354 ОКС 35.020

Ключевые слова: компьютерный инцидент, управление компьютерными инцидентами, регистрация компьютерного инцидента, реагирование на компьютерный инцидент

Редактор *Н.В. Таланова*
Технический редактор *В.Н. Прусакова*
Корректор *О.В. Лазарева*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 30.11.2022. Подписано в печать 08.12.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,12.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru