ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59711— 2022

Защита информации

УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

Организация деятельности по управлению компьютерными инцидентами

Издание официальное

Москва
Российский институт стандартизации
2022

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. № 1377-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 (www.rst.gov.ru)

Содержание

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 организации деятельности по управлению компьютерными инцидентами.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

Организация деятельности по управлению компьютерными инцидентами

Information protection.
Computer incidents management.
Organization of computer incidents management activities

Дата введения — 2023—02—01

1 Область применения

Настоящий стандарт определяет содержание этапов организации деятельности по управлению компьютерными инцидентами.

Настоящий стандарт предназначен как для субъектов 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.

Примечание — В настоящем стандарте «субъекты ГосСОПКА» названы «организациями».

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 56939 Защита информации. Разработка безопасного программного обеспечения. Общие требования

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

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 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.

Издание официальное

3 Термины и определения

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

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ГосСОПКА — Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

КИИ — критическая информационная инфраструктура;

СВТ — средство вычислительной техники.

5 Общие положения

Стадия «организация деятельности по управлению компьютерными инцидентами» в рамках деятельности по управлению компьютерными инцидентами состоит из следующих этапов:

- разработка политики управления компьютерными инцидентами;
- разработка плана реагирования на компьютерные инциденты;
- определение подразделения, ответственного за управление компьютерными инцидентами;
- организация взаимодействия с подразделениями внутри организации и с внешними организациями;
- материально-техническое оснащение подразделения, ответственного за управление компьютерными инцидентами;
- организация обучения и информирования в части управления компьютерными инцидентами;
- проведение тренировок по отработке мероприятий плана реагирования на компьютерные инциденты.

6 Разработка политики управления компьютерными инцидентами

6.1 Общие положения

В организации, планирующей ведение деятельности по управлению компьютерными инцидентами, должна быть разработана и внедрена политика управления компьютерными инцидентами, которая определяет общий порядок ведения деятельности по управлению компьютерными инцидентами, а также лиц, которые будут принимать участие в данной деятельности, их роли и обязанности.

К процессу разработки политики управления компьютерными инцидентами следует привлекать работников организации, которые могут принимать участие в деятельности по управлению компьютерными инцидентами.

Политика управления компьютерными инцидентами должна быть согласована или утверждена руководителем организации или уполномоченным им лицом.

6.2 Содержание политики управления компьютерными инцидентами

Политику управления компьютерными инцидентами следует разрабатывать как высокоуровневый документ.

В политике управления компьютерными инцидентами должны быть определены:

- цели ведения деятельности по управлению компьютерными инцидентами;
- информация о ресурсах, в отношении которых будет вестись деятельность по управлению компьютерными инцидентами (зона ответственности);
- общие сведения о том, что для организации является компьютерным инцидентом.

Примечания

1 К компьютерным инцидентам относят инциденты, характеризующиеся наличием факта нарушения и (или) прекращения функционирования информационных ресурсов субъектов ГосСОПКА, сети электросвязи, используемой для организации взаимодействия информационных ресурсов, и (или) нарушения безопасности обрабатываемой в информационном ресурсе субъектов ГосСОПКА информации, необходимой для обеспечения критических процессов (ее конфиденциальности, целостности или доступности), в том числе произошедших в результате ком-

пьютерной атаки. При этом под прекращением или нарушением функционирования информационных ресурсов понимают приведение 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.

2 Приведенные в политике сведения о том, что для организации является компьютерным инцидентом, в дальнейшем используются для разработки правил регистрации признаков возможного возникновения компьютерных инцидентов (правил, осуществляющих автоматизированный анализ и корреляцию событий безопасности и иных данных мониторинга) и при проведении проверки фактов возникновения компьютерных инцидентов с целью их подтверждения.

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

- высокоуровневый обзор или визуализация процесса управления компьютерными инцидентами в части стадий «обнаружение и регистрация компьютерных инцидентов» и «реагирование на компьютерные инциденты»;
- описание организационной структуры подразделения, ответственного за управление компьютерными инцидентами, в том числе ролей специалистов подразделения, их обязанностей и полномочий.

7 Разработка плана реагирования на компьютерные инциденты

7.1 Общие положения

План реагирования на компьютерные инциденты должен содержать подробные пошаговые инструкции к действиям, выполняемым на стадиях «обнаружение и регистрация компьютерных инцидентов» и «реагирование на компьютерные инциденты», с учетом организационной структуры организации, особенностей ее информационной инфраструктуры, применяемых программных и программно-технических средств, типов компьютерных инцидентов, их приоритетов и уровней влияния.

Примечания

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

Организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами, является Национальный координационный центр по компьютерным инцидентам.

2 Подход к определению уровней влияния и приоритетов компьютерных инцидентов приведен в приложениях А и Б.

3 План реагирования на компьютерные инциденты может включать различные приложения, например инструкции, регламенты и иные документы, в соответствии с которыми осуществляется деятельность по обнаружению, регистрации, принятию решений и действий, связанных с реагированием на компьютерные инциденты.

Разработку плана реагирования на компьютерные инциденты должен координировать руководитель подразделения, ответственного за управление компьютерными инцидентами, и она должна быть выполнена с учетом положений политики управления компьютерными инцидентами.

Для разработки плана реагирования на компьютерные инциденты должны привлекаться работники организации, которые могут принимать участие в деятельности по управлению компьютерными инцидентами.

Примечание — К процессу согласования плана могут быть привлечены иные лица, определенные руководителем организации или уполномоченным им лицом.

Разработанный план должен быть согласован с руководителем подразделения, ответственного за управление компьютерными инцидентами, и утвержден руководителем организации или уполномоченным им лицом и в порядке информирования представлен в организацию, осуществляющую координацию деятельности в части управления компьютерными инцидентами.

7.2 Содержание плана реагирования на компьютерные инциденты

План реагирования на компьютерные инциденты должен включать:

а) общие сведения, необходимые для обнаружения и регистрации компьютерных инцидентов и реагирования на них, включая:

1) технические характеристики и состав контролируемых информационных ресурсов организации;

2) перечень типов компьютерных инцидентов, которые в организации требуется обнаруживать и регистрировать с указанием их уровней влияния, приоритетов и конкретных способов обнаружения и регистрации.

Примечание — Перечень типов компьютерных инцидентов, которые в организации требуется обнаруживать и регистрировать, формируют на основании установленных в утвержденной политике управления компьютерными инцидентами сведений о том, что для организации является компьютерным инцидентом.

Также может быть предусмотрен дополнительный тип компьютерных инцидентов (например, «прочее»). Его цель состоит в том, чтобы обеспечить регистрацию компьютерных инцидентов, не соответствующих ни одному из определенных ранее типов компьютерных инцидентов;

3) порядок формирования состава рабочих групп реагирования на компьютерные инциденты.

Примечание — Состав рабочих групп реагирования на компьютерные инциденты может зависеть:

- от информационного ресурса, в котором зарегистрирован компьютерный инцидент (в составе рабочей группы реагирования на компьютерные инциденты должны быть специалисты подразделений, ответственных за эксплуатацию информационного ресурса, на котором произошел компьютерный инцидент, так как только эти специалисты обладают правами доступа к информационному ресурсу, позволяющими выполнять все необходимые действия по реагированию на компьютерный инцидент);
- территориального расположения информационного ресурса (реагирование на компьютерные инциденты, произошедшие на территориально удаленных объектах, целесообразно проводить с привлечением специалистов, находящихся на этих объектах);
- типа компьютерного инцидента (при реагировании на определенные типы компьютерных инцидентов может возникать необходимость привлечения специалистов, обладающих определенными экспертными знаниями и (или) умениями);

4) перечень лиц, привлекаемых к реагированию на компьютерные инциденты, а также их функции и обязанности;

5) порядок осуществления доступа к информации о ходе реагирования на компьютерный инцидент и к данным мониторинга, на основании которых он зарегистрирован, работников организации, входящих в состав рабочей группы реагирования на компьютерные инциденты.

Примечание — Совместное использование информации о ходе реагирования на компьютерный инцидент и данных мониторинга, на основании которых он зарегистрирован, всеми участниками процесса по реагированию на компьютерный инцидент обеспечит повышение эффективности реагирования;

6) установленные сроки выполнения этапов реагирования на компьютерные инциденты.

Примечание — Сроки выполнения этапов реагирования на компьютерные инциденты устанавливают с учетом их уровней влияния;

7) порядок принятия решения о необходимости привлечения к реагированию на компьютерный инцидент организации, осуществляющей координацию деятельности по управлению компьютерными инцидентами.

Примечания

1 На основании данного порядка специалист, ответственный за реагирование на компьютерный инцидент (руководитель рабочей группы реагирования на компьютерные инциденты), будет понимать, при каких обстоятельствах требуется привлечение организации, осуществляющей координацию деятельности по управлению компьютерными инцидентами. Например, это может потребоваться, когда компьютерный инцидент не может быть взят под контроль или ожидается, что он будет иметь критические последствия для организации.

2 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.

3 Компьютерный инцидент считается «находящимся под контролем», если удалось принять меры, которые позволили предотвратить вовлечение в инцидент новых элементов информационной инфраструктуры и увеличение масштаба негативных последствий;

8) порядок регистрации действий, выполняемых на стадии «реагирование на компьютерные инциденты».

Примечание — Порядок регистрации действий, выполняемых на стадии «реагирование на компьютерные инциденты» должен предусматривать регистрацию всех действий, выполняемых на каждом этапе стадии «реагирование на компьютерный инцидент», так как после закрытия компьютерного инцидента данная информация может быть полезной для приобретения и накопления опыта, который может использоваться для предотвращения повторного возникновения компьютерных инцидентов и повышения эффективности процедур реагирования на компьютерные инциденты;

9) порядок проведения мероприятий по реагированию на компьютерные инциденты совместно с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

Примечание — Подпункты 7 и 9 пункта а) «Общие сведения, необходимые для обнаружения и регистрации компьютерных инцидентов и реагирования на них» не являются обязательными для включения в план реагирования на компьютерные инциденты. При включении данных пунктов в план проект плана, до его утверждения, должен быть представлен в федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования ГосСОПКА;

б) порядок обнаружения и регистрации компьютерных инцидентов, включая:

1) перечень и описание правил регистрации признаков возможного возникновения компьютерных инцидентов.

Примечание — Описание правила регистрации признаков возможного возникновения компьютерного инцидента должно содержать перечень событий безопасности и иных данных мониторинга, а также связей между ними и дополнительных условий, на основании которых принимают решение о регистрации такого признака;

2) порядок приема специалистами подразделения, ответственного за управление компьютерными инцидентами, сведений об обнаруженных признаках возможного возникновения компьютерных инцидентов от работников организации;

3) порядок проведения проверки фактов возникновения компьютерных инцидентов;

4) формы карточек компьютерных инцидентов, которые формируют при регистрации компьютерных инцидентов разных типов.

Примечание — В формах карточек должны быть определены поля, которые заполняются автоматическим способом, и поля, которые заполняют специалисты, входящие в состав рабочих групп реагирования на компьютерные инциденты;

5) перечень и формы отчетов, формируемых на стадиях «обнаружение и регистрация компьютерных инцидентов» и «реагирование на компьютерные инциденты».

Примечание — В рамках деятельности по управлению компьютерными инцидентами могут быть сформированы различные статистические отчеты по зарегистрированным компьютерным инцидентам, отчеты с показателями эффективности работы рабочих групп реагирования на компьютерные инциденты, сводные отчеты о результатах деятельности по реагированию на компьютерные инциденты за различные периоды времени и иные отчеты, состав которых должен быть определен в плане;

в) порядок реагирования на компьютерные инциденты, включая:

1) порядок определения вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;

2) порядок локализации компьютерных инцидентов.

Примечание — При локализации компьютерного инцидента применяют меры, направленные на ограничение функционирования информационных ресурсов, на которых обнаружены признаки зарегистрированного компьютерного инцидента, с целью предотвращения его дальнейшего распространения. Примерами таких мер являются отключение СВТ, на которых обнаружены признаки компьютерных инцидентов, от локальной вычислительной сети, отключение служб или процессов, уязвимости которых используются для распространения вредоносного программного обеспечения, блокирование потоков информации на межсетевых экранах. Меры, принимаемые при локализации компьютерных инцидентов, определяют для установленных в плане реагирования на компьютерные инциденты типов компьютерных инцидентов;

3) ситуации, при которых требуется прекратить действия по реагированию на компьютерный инцидент.

Примечание — К таким ситуациям могут относиться случаи, при которых действия по реагированию на компьютерный инцидент, например, связанные с приостановкой или прекращением функционирования информационного ресурса, могут негативно влиять на критические процессы организации. Для каждой из таких ситуаций должна быть предусмотрена необходимость привлечения руководства организации, экспертных организаций, организации, осуществляющей координацию деятельности в части управления компьютерными инцидентами, иных лиц и (или) организаций для определения и (или) выполнения дальнейших действий по реагированию на компьютерный инцидент;

4) порядок контроля процесса реагирования на компьютерные инциденты со стороны специалистов, ответственных за реагирование на компьютерные инциденты (руководителей рабочих групп реагирования на компьютерные инциденты).

Примечание — Контроль предусматривает отслеживание сроков реагирования на компьютерные инциденты и проверку результатов реагирования на компьютерные инциденты для принятия решения об их закрытии или возврате на один из предыдущих этапов реагирования. Если в ходе контроля реагирования на компьютерные инциденты установлено, что имеются проблемы по локализации и ликвидации последствий компьютерного инцидента, и предполагается, что он будет оказывать серьезные негативные воздействия на критические процессы организации, то целесообразно направить обращение в организацию, осуществляющую координацию деятельности в части управления компьютерными инцидентами, об оказании содействия в реагировании на компьютерный инцидент;

5) порядок действий в процессе выявления и ликвидации последствий компьютерных инцидентов;

6) порядок закрытия компьютерных инцидентов;

7) порядок фиксации материалов, связанных с возникновением компьютерных инцидентов, и установления причин и условий их возникновения.

7.3 Применение плана реагирования на компьютерные инциденты

К деталям плана реагирования на компьютерные инциденты должны иметь доступ только специалисты подразделения, ответственного за управление компьютерными инцидентами. Для других работников организации, привлекаемых к реагированию на компьютерные инциденты, на основании плана реагирования на компьютерные инциденты необходимо разрабатывать отдельные инструкции, определяющие их функции и задачи в рамках реагирования на компьютерные инциденты, которые должны содержать только касающиеся соответствующих работников сведения. Например, такими задачами могут быть:

- отключение информационного ресурса в целом, его отдельного сегмента, сервиса или элемента информационной инфраструктуры (отдельное СВТ, входящее в состав комплекса программно-технических средств), вовлеченного в компьютерный инцидент, при локализации компьютерного инцидента;
- мониторинг состояния информационного ресурса в целом, его отдельного сегмента, сервиса или элемента информационной инфраструктуры, вовлеченного в компьютерный инцидент, при локализации компьютерного инцидента;
- определение перечня удаленных или поврежденных в результате компьютерного инцидента объектов при выявлении последствий компьютерных инцидентов;
- фиксация материалов, связанных с возникновением компьютерного инцидента (цифровых свидетельств);
- восстановление информационного ресурса в целом, его отдельного сегмента, сервиса или элемента информационной инфраструктуры, вовлеченного в компьютерный инцидент из резервных копий (как способа восстановления работоспособности), или выполнение иных процедур восстановления;
- передача информации о компьютерных инцидентах специалистам смежных подразделений, а также внешним организациям, в том числе в организацию, осуществляющую координацию деятельности в части управления компьютерными инцидентами.

Каждому работнику организации, привлекаемому к реагированию на компьютерные инциденты, могут быть определены одна или несколько ролей в рамках деятельности по реагированию на компьютерные инциденты.

В процессе реагирования на компьютерные инциденты работникам организации, привлекаемым к реагированию на компьютерные инциденты, необходимо предоставлять доступ к информации, полу-

ченной по результатам реагирования на компьютерные инциденты, только в случае необходимости и только в необходимом объеме.

7.4 Обработка информации ограниченного доступа

Отчетные материалы, формируемые в ходе деятельности по управлению компьютерными инцидентами, могут содержать информацию ограниченного доступа, поэтому при ведении деятельности по управлению компьютерными инцидентами важно обеспечить защиту такой информации.

Если в ходе деятельности по управлению компьютерными инцидентами используются данные мониторинга, получаемые из информационных ресурсов, защита которых осуществляется в соответствии с законодательством Российской Федерации, то защита таких данных и результатов их обработки (карточки компьютерных инцидентов и иные отчеты) также должна осуществляться в соответствии с законодательством Российской Федерации.

Защита информации должна быть обеспечена и при организации взаимодействия с внешними организациями, в том числе с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

8 Определение подразделения, ответственного за управление компьютерными инцидентами

8.1 Подходы к определению подразделения, ответственного за управление компьютерными инцидентами

Одним из важнейших этапов организации деятельности по управлению компьютерными инцидентами является определение в организации соответствующего структурного подразделения, специалисты которого будут выполнять следующие задачи:

- обнаружение и регистрацию компьютерных инцидентов;
- организацию и контроль процессов реагирования на компьютерные инциденты с привлечением специалистов подразделений, ответственных за эксплуатацию информационных ресурсов, и (или) непосредственное выполнение действий по реагированию;
- анализ результатов деятельности по управлению компьютерными инцидентами с целью идентификации методов и способов обнаружения и реагирования на компьютерные инциденты, которые показали свою эффективность в отношении уже закрытых компьютерных инцидентов, предотвращения повторного возникновения компьютерных инцидентов и доработки (актуализации) документации в части управления компьютерными инцидентами.

Организация может определить ответственным за управление компьютерными инцидентами существующее штатное подразделение, ответственное за обеспечение безопасности информации и (или) за защиту информации (из состава подразделений (работников) по информационной безопасности организации, находящихся под общим руководством), создать новое подразделение (в составе подразделений (работников) по информационной безопасности организации, находящихся под общим руководством) или присоединиться к зоне ответственности внешнего подразделения, оказывающего услуги по управлению компьютерными инцидентами.

Эффективность деятельности подразделения, ответственного за управление компьютерными инцидентами, зависит от организованного взаимодействия со всеми подразделениями организации, участвующими в деятельности по управлению компьютерными инцидентами.

Подразделение, ответственное за управление компьютерными инцидентами, должно иметь соответствующие полномочия. Принципиально важно, чтобы все подразделения организации были уведомлены о полномочиях специалистов подразделения, ответственного за управление компьютерными инцидентами. Для этих целей в организации должны быть сформированы соответствующие приказы и (или) распоряжения руководителя организации или уполномоченного им лица.

Если для организации деятельности по управлению компьютерными инцидентами планируется создать новое подразделение, целесообразно, чтобы его организационная структура учитывала особенности его зоны ответственности. На рисунке 1 представлены примеры структуры подразделения, ответственного за управление компьютерными инцидентами.

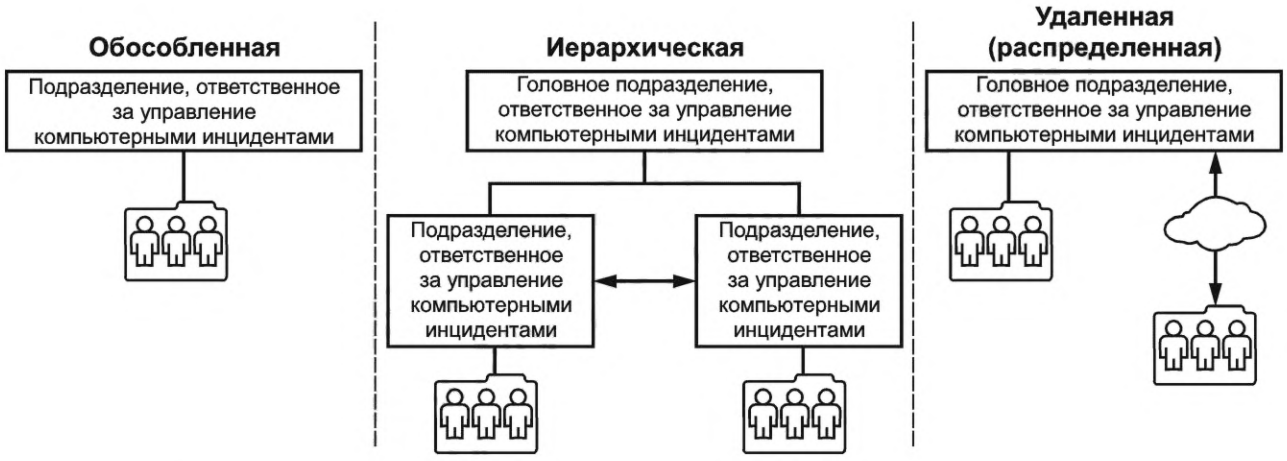

Рисунок 1 — Примеры структуры подразделения, ответственного за управление компьютерными инцидентами

Выделяют следующие типы структур подразделений, ответственных за управление компьютерными инцидентами:

- обособленная;
- иерархическая;
- удаленная (распределенная).

Обособленная структура подразделения, ответственного за управление компьютерными инцидентами, не предусматривает наличие подчиненных подразделений. Такой тип структуры обычно подходит подразделениям, которые ведут деятельность по управлению компьютерными инцидентами в рамках одной зоны ответственности.

Иерархическая структура подразделения, ответственного за управление компьютерными инцидентами, предусматривает наличие нескольких подразделений, подчиненных головному подразделению. Такой тип структуры обычно подходит подразделениям, которые ведут деятельность по управлению компьютерными инцидентами в интересах одной организации, имеющей филиалы, или в зону ответственности которых входят информационные ресурсы, принадлежащие другим организациям.

Удаленная (распределенная) структура подразделения, ответственного за управление компьютерными инцидентами, предусматривает удаленную деятельность по управлению компьютерными инцидентами. Такой тип структуры обычно подходит подразделениям, которые ведут деятельность по управлению компьютерными инцидентами на удаленных объектах или в зону ответственности которых входят информационные ресурсы, принадлежащие другим организациям. При таком типе структуры подразделение, ответственное за управление компьютерными инцидентами, привлекает для реагирования на компьютерные инциденты специалистов подразделений, ответственных за эксплуатацию информационных ресурсов на этих удаленных объектах.

Организация может присоединиться (может быть включена) к зоне ответственности субъекта ГосСОПКА, оказывающего услуги по управлению компьютерными инцидентами, на основании договора или соглашения (например, в рамках функционирования ГосСОПКА в соответствии с законодательством Российской Федерации).

Сфера деятельности организации, а также характеристики и масштаб ее информационных ресурсов влияют на состав (объем) и формы оказания требуемых услуг по управлению компьютерными инцидентами.

8.2 Виды деятельности подразделения, ответственного за управление компьютерными инцидентами

Основными видами деятельности подразделения, ответственного за управление компьютерными инцидентами, должны являться (но не ограничиваться ими):

а) в рамках задачи обнаружения и регистрации компьютерных инцидентов:

1) эксплуатация средств, предназначенных для обнаружения и регистрации компьютерных инцидентов;

2) разработка правил регистрации признаков возможного возникновения компьютерных инцидентов;

3) регистрация признаков возможного возникновения компьютерных инцидентов по информации, поступившей от работников организации;

4) проведение проверки фактов возникновения компьютерных инцидентов;

б) в рамках задачи организации и контроля процессов реагирования на компьютерные инциденты с привлечением специалистов подразделений, ответственных за эксплуатацию информационных ресурсов, и (или) непосредственного выполнения действий по реагированию:

1) эксплуатация средств, предназначенных для реагирования на компьютерные инциденты;

2) формирование состава рабочих групп реагирования на компьютерные инциденты;

3) выполнение действий по реагированию на компьютерные инциденты в рамках рабочих групп реагирования на компьютерные инциденты;

4) контроль выполнения процедур реагирования на компьютерные инциденты, в том числе фиксации материалов, связанных с возникновением компьютерных инцидентов и установлением причин и условий их возникновения;

5) взаимодействие с внешними организациями в рамках деятельности по управлению компьютерными инцидентами, в том числе с организацией, осуществляющей координацию деятельности по управлению компьютерными инцидентами;

в) в рамках задачи анализа 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.

Примечание — Некоторые из вышеперечисленных обязанностей могут быть возложены на иные подразделения организации, участвующие в деятельности по управлению компьютерными инцидентами.

8.3 Роли и распределение функций между специалистами подразделения, ответственного за управление компьютерными инцидентами

При определении подразделения, ответственного за управление компьютерными инцидентами, должны быть определены роли специалистов данного подразделения. При определении ролей специалистов необходимо учитывать, что в составе подразделения должны быть специалисты, в обязанности которых будут входить:

- разработка правил регистрации признаков возможного возникновения компьютерных инцидентов;
- прием сообщений от работников организации об обнаруженных ими признаках возможного возникновения компьютерных инцидентов;
- участие в реагировании на компьютерные инциденты;
- разработка и (или) доработка (актуализация) документации в части управления компьютерными инцидентами;
- обслуживание программных и программно-технических средств, используемых в деятельности по управлению компьютерными инцидентами.

Некоторые функции, возложенные на подразделение, ответственное за управление компьютерными инцидентами, могут быть распределены (переданы) специалистам смежных подразделений. Пример такого распределения представлен в таблице 1.

Таблица 1 — Пример распределения функций, возложенных на подразделение, ответственное за управление компьютерными инцидентами, между специалистами смежных подразделений

Должность	Функции
Инженер подразделения технической поддержки	- прием и обработка информации о компьютерных инцидентах от средств управления событиями информационной безопасности, средств управления инцидентами, работников организации; - внесение дополнительной информации в карточки компьютерных инцидентов
Инженер отдела информационной безопасности/инженер отдела информационных технологий/системный администратор	- реагирование на компьютерные инциденты; - взаимодействия с внешними организациями, в том числе с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами; - эксплуатация и мониторинг средств обнаружения компьютерных атак, средств управления событиями информационной безопасности, средств управления инцидентами, средств для предупреждения компьютерных атак, средств обмена информацией
Методист (разработчик технической документации)	- оказание помощи в разработке и улучшении (актуализации) документов в части управления компьютерными инцидентами; - оказание помощи в разработке рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов; - разработка учебных материалов в части управления компьютерными инцидентами

8.4 Требования к знаниям и навыкам специалистов подразделения, ответственного за управление компьютерными инцидентами

Эффективность деятельности по управлению компьютерными инцидентами зависит от квалификации специалистов, которые могут быть привлечены к реагированию на компьютерные инциденты.

Специалистам подразделения, ответственного за управление компьютерными инцидентами, необходимо обладать следующими знаниями и навыками:

- знаниями актуальных проблем безопасности локальных вычислительных сетей, включая тактики и техники проведения компьютерных атак;
- знаниями практик обеспечения безопасности системного администрирования, таких как управление обновлениями, безопасная настройка, резервное копирование и аварийное восстановление;
- знаниями основ криптографической защиты информации (алгоритмы шифрования): цифровые подписи, сетевые протоколы, такие как SSL/TLS;
- знаниями общих сетевых протоколов, таких как Ethernet (IEEE 802.3), WiFi (IEEE 802.11) IPv4, IPv6, ICMP, UDP, TCP;
- знаниями общих протоколов сетевых приложений, таких как DNS, SMTP, HTTP (S);
- навыками сбора информации о компьютерных инцидентах (цифровых свидетельств), обратного инжиниринга;
- навыками реагирования на компьютерные инциденты;
- знаниями в области разработки безопасного программного обеспечения (в частности, в соответствии с ГОСТ Р 56939 и иными стандартами в указанной области), функционального и объектно-ориентированного программирования, системной архитектуры СВТ.

Примечание — Необходимый объем знаний определяют с учетом роли специалиста, участвующего в деятельности по управлению компьютерными инцидентами, и его должностных обязанностей.

Дополнительные знания и навыки, необходимые для реагирования на компьютерные инциденты, должны быть определены с учетом технологий, используемых в организации.

Руководитель подразделения, ответственного за управление компьютерными инцидентами, должен обеспечить своевременное выявление потребностей в получении специалистами подразделения дополнительных знаний и навыков, необходимых для эффективного реагирования на компьютерные инциденты.

Несмотря на то, что подразделение, ответственное за управление компьютерными инцидентами, является основным участником деятельности по управлению компьютерными инцидентами, не требуется, чтобы всеми знаниями и навыками обязательно обладали специалисты этого подразделения. Редко используемые экспертные знания и навыки могут иметь отдельные лица или группы лиц как внутри организации, так и за ее пределами, к которым специалисты подразделения, ответственного за управление компьютерными инцидентами, могут обратиться за помощью во время реагирования на компьютерный инцидент.

В организации рекомендуется вести реестр, который будет отражать текущие знания, навыки и умения работников, которые могут быть привлечены к деятельности по реагированию на компьютерные инциденты. Такой реестр может содержать следующую информацию:

- какие работники могут быть привлечены к реагированию на компьютерные инциденты;
- какими знаниями, навыками и умениями обладают эти работники;
- являются ли эти работники внутренними или внешними по отношению к организации.

9 Организация взаимодействия с подразделениями внутри организации и с внешними организациями

9.1 Взаимодействие с подразделениями внутри организации

В организации должно быть организовано взаимодействие подразделения, ответственного за управление компьютерными инцидентами, со смежными подразделениями, также участвующими в деятельности по управлению компьютерными инцидентами. Должны быть определены способы взаимодействия, правила и процедуры, в рамках которых такое взаимодействие будет реализовано.

Подразделение, ответственное за управление компьютерными инцидентами, в ходе своей деятельности может взаимодействовать со следующими группами специалистов:

- специалистами подразделения, ответственного за эксплуатацию информационных ресурсов.

Примечание — В организации должен быть регламентирован порядок взаимодействия подразделения, ответственного за управление компьютерными инцидентами, со специалистами подразделения, ответственного за эксплуатацию информационных ресурсов, включая разделение функций и полномочий между данными подразделениями и действий в случае возникновения компьютерного инцидента;

- специалистами юридического подразделения.

Примечание — Специалисты юридического подразделения должны предоставлять рекомендации и консультации по вопросам соблюдения требований законодательства в ходе деятельности по управлению компьютерными инцидентами, например не ущемляются ли права работников организации при осуществлении фиксации материалов, связанных с возникновением компьютерных инцидентов (цифровых свидетельств), необходимых для установления причин и условий их возникновения;

- специалистами отдела кадров.

Примечание — Специалисты отдела кадров должны принимать участие в разработке процедур увольнения работников организации, уличенных в действиях, которые привели к компьютерному инциденту;

- специалистами отдела по связям с общественностью.

Примечание — Специалисты отдела по связям с общественностью должны быть готовы обрабатывать любые запросы средств массовой информации и оказывать содействие в разработке политик и процедур раскрытия информации;

- специалистами подразделений обеспечения безопасности организации.

Примечание — Специалисты подразделения, ответственного за управление компьютерными инцидентами, должны информировать специалистов подразделений обеспечения безопасности организации о зарегистрированных компьютерных инцидентах с целью совместного реагирования на компьютерные инциденты, а также для организации взаимодействия с правоохранительными органами (при необходимости).

Подразделение, ответственное за управление компьютерными инцидентами, должно нести ответственность за выполнение действий по реагированию на компьютерные инциденты, и, следовательно, его специалисты должны обладать определенными полномочиями для выполнения действий, которые необходимы для осуществления указанной деятельности. При этом действия, которые могут иметь не-

гативное воздействие на критические процессы организации, должны быть согласованы с руководителем организации или уполномоченным им лицом.

9.2 Взаимодействие с внешними организациями

В организации должен быть организован порядок взаимодействия с внешними организациями (для каждой организации отдельно) по вопросам, связанным с деятельностью по управлению компьютерными инцидентами.

Взаимодействие с внешними организациями следует осуществлять в соответствии с положениями, политиками, регламентами или другими документами, утвержденными в организации.

В рамках функционирования ГосСОПКА организация должна осуществлять взаимодействие с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

При необходимости возможно взаимодействие с другими заинтересованными организациями в части управления компьютерными инцидентами в случае их возникновения.

Примечание — Организациям рекомендуется взаимодействовать с различными сообществами и группами, работающими в части управления компьютерными инцидентами, с целью повышения осведомленности, навыков и квалификации. Обмен информацией с партнерами на стадии «обнаружение и регистрация компьютерных инцидентов» может повысить эффективность реагирования и минимизировать последствия компьютерных инцидентов. Поскольку компьютерные инциденты могут затрагивать одновременно несколько организаций, такой обмен информацией считается важным и продуктивным. При наличии возможностей целесообразно организовать автоматизированный обмен информацией о компьютерных инцидентах, чтобы увеличить скорость обнаружения новых компьютерных инцидентов посредством коллективной деятельности по управлению компьютерными инцидентами. Примером такого взаимодействия может служить взаимодействие субъектов ГосСОПКА с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

Взаимодействие в части управления компьютерными инцидентами также может осуществляться (но не ограничиваться):

- с подразделениями, ответственными за управление компьютерными инцидентами внешних организаций;
- с организациями, которым предоставляют услуги по управлению компьютерными инцидентами (клиент, заказчики);
- с поставщиками услуг, включая техническую поддержку, предоставление каналов связи, и другими организациями;
- с правоохранительными органами;
- с организациями, предоставляющими юридические услуги;
- со средствами массовой информации.

10 Материально-техническое оснащение подразделения, ответственного за управление компьютерными инцидентами

10.1 Общие положения

Для обеспечения своевременного и эффективного обнаружения, регистрации и реагирования на компьютерные инциденты в организации должны быть внедрены соответствующие программные и программно-технические средства.

Организация должна обеспечить, чтобы автоматизированные средства, используемые для управления компьютерными инцидентами, в совокупности осуществляли поддержку, как минимум, следующей деятельности:

- сбор информации о событиях безопасности и иных данных мониторинга, а также регистрация с использованием собранных данных, компьютерных инцидентов.

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

- сбор и обработка сведений, необходимых для формирования рекомендаций по предотвращению компьютерных инцидентов и (или) снижению опасности их последствий.

Примечание — К таким сведениям относятся сведения о показателе доверия (репутации) сетевых адресов, доменных имен, серверов электронной почты, серверов доменных имен, сведения об известных уязвимостях используемого программного обеспечения, сведения о компьютерных сетях, состоящих из управляемых с использованием вредоносного программного обеспечения СВТ, включая сведения об их управляющих серверах;

- организация и контроль процессов реагирования на компьютерные инциденты, в том числе оповещение специалистов смежных подразделений, участвующих в деятельности по управлению компьютерными инцидентами;
- организация взаимодействия (обмена информацией) с внешними организациями;
- обеспечение защиты собранных данных мониторинга, результатов их обработки, а также результатов реагирования на компьютерные инциденты;
- обеспечение резервного копирования;
- подготовка данных для обмена информацией о компьютерных инцидентах с внешними организациями, в том числе с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

10.2 Примеры программных и программно-технических средств, обеспечивающих деятельность по управлению компьютерными инцидентами

В состав программных и программно-технических средств, обеспечивающих деятельность подразделения, ответственного за управление компьютерными инцидентами, могут входить как средства для автоматизации деятельности по управлению компьютерными инцидентами, так и средства, являющиеся источниками событий безопасности.

К средствам, обеспечивающим деятельность подразделения, ответственного за управление компьютерными инцидентами, могут относиться:

- средства управления событиями информационной безопасности;
- средства для предупреждения компьютерных атак;
- средства управления инцидентами;
- средства обмена информацией;
- средства криптографической защиты информации;
- средства анализа программного обеспечения, сетевого трафика, а также электронных образов носителей информации;
- средства обнаружения компьютерных атак (система обнаружения вторжений);
- межсетевые экраны;
- антивирусные средства;
- средства резервного копирования и восстановления информации;
- средства доверенной загрузки;
- средства контроля съемных машинных носителей информации;
- средства контроля подключения устройств;
- средства анализа защищенности;
- средства защиты от несанкционированного доступа;
- средства контроля целостности;
- замкнутая среда предварительного выполнения программ.

11 Организация обучения и информирования в части управления компьютерными инцидентами

В рамках обучения и информирования в области информационной безопасности работников организации целесообразно предусматривать получение знаний в области управления компьютерными инцидентами.

Для специалистов подразделения, ответственного за управление компьютерными инцидентами, а также специалистов смежных подразделений, участвующих в деятельности по управлению компьютерными инцидентами, должен быть разработан отдельный план обучения. Каждой группе специалистов, участвующих в деятельности по управлению компьютерными инцидентами, может потребоваться разный уровень подготовки в зависимости от выполняемых ими задач в соответствии с планом реагирования на компьютерные инциденты.

В процессе проведения обучения (инструктажей, курсов и т.п.) до специалистов, участвующих в деятельности по управлению компьютерными инцидентами, должна быть доведена следующая информация:

- порядок выполнения действий, предусмотренных планом реагирования на компьютерные инциденты;
- порядок ведения (составления) отчетности;
- перечень полномочий и ограничений в рамках деятельности по управлению компьютерными инцидентами.

Обучение должно сопровождаться конкретными упражнениями и тестированием для специалистов подразделения, ответственного за управление компьютерными инцидентами, а также специалистов смежных подразделений, участвующих в деятельности по управлению компьютерными инцидентами.

В дальнейшем на регулярной основе должны быть проведены инструктажи.

12 Проведение тренировок по отработке мероприятий плана реагирования на компьютерные инциденты

В ходе деятельности по управлению компьютерными инцидентами должны быть запланированы и проведены на регулярной основе тренировки по отработке мероприятий плана реагирования на компьютерные инциденты с целью выявления потенциальных недостатков и проблем, которые могут возникнуть в рамках данной деятельности. Тренировки должны предусматривать как моделирование различных сценариев, которые могут варьироваться от серьезных (сложных) компьютерных инцидентов, основанных на реалистичных имитациях компьютерных атак, сбоев или неисправностей, так и проведение теоретических занятий. Формат сценариев может зависеть от заранее определенных целей тренировки. В тренировках должны принимать участие как специалисты подразделения, ответственного за управление компьютерными инцидентами, так и специалисты смежных подразделений, участвующих в деятельности по управлению компьютерными инцидентами.

Все участники тренировок должны быть проинформированы о том, что они имеют дело с действиями, имитирующими компьютерный инцидент. Данная информация необходима для того, чтобы исключить действия по реагированию, приводящие к негативным последствиям для критических процессов организации.

Примечание — Для проведения тренировок могут быть применены тестовые системы, в которых могут быть имитированы компьютерные атаки и (или) особенности контролируемых информационных ресурсов. Такие тестовые системы также могут быть использованы для тестирования программных и программно-технических средств, обеспечивающих деятельность по управлению компьютерными инцидентами.

Информирование участников может не осуществляться в случае проведения тренировок в контролируемых условиях, препятствующих влиянию тренировок на критические процессы организации.

Тренировки могут быть проведены в форме:

- обсуждения (дискуссии);
- командных тренингов;
- практического занятия;
- смешанной (использование всех трех форм).

Выбор формы тренировки зависит от цели, которую планируется достичь, а также от наличия времени и ресурсов.

Тренировка преследует следующие основные цели:

- подтверждение применимости на практике плана реагирования на компьютерные инциденты и выявление потенциальных недостатков;
- проверка готовности специалистов, участвующих в деятельности по управлению компьютерными инцидентами, к выполнению мероприятий плана реагирования на компьютерные инциденты;
- тестирование существующих процессов и процедур реагирования на компьютерные инциденты.

При разработке организацией плана реагирования на компьютерные инциденты или его актуализации проводят тренировки для проверки его применимости. После введения плана реагирования на компьютерные инциденты в действие проводят тренировки для проверки готовности специалистов подразделения, ответственного за управление компьютерными инцидентами, и специалистов смежных подразделений, участвующих в деятельности по управлению компьютерными инцидентами. После того

как существующие процессы и процедуры отработаны, должны быть проведены периодические тренировки для подтверждения актуальности плана реагирования на компьютерные инциденты.

В таблице 2 представлены формы тренировок и цели, для которых они могут быть проведены.

Таблица 2 — Формы тренировок и цели

Цель проведения тренировки	Форма проведения тренировки
Подтверждение применимости на практике плана реагирования на компьютерные инциденты и выявление потенциальных недостатков	обсуждения (дискуссии); командные тренинги
Проверка готовности специалистов, участвующих в деятельности по управлению компьютерными инцидентами, к выполнению мероприятий плана реагирования на компьютерные инциденты	обсуждения (дискуссии); командные тренинги; практические занятия
Тестирование существующих процессов и процедур реагирования на компьютерные инциденты	командные тренинги; практические занятия

При планировании тренировок необходимо учитывать следующие вопросы:

- проводится ли тренировка в рамках одной организации или будут участвовать внешние организации;
- специалисты каких подразделений организации будут участвовать в тренировках.

Для успешного проведения тренировок необходимо выполнить ряд задач, основные из которых представлены ниже:

- краткое ознакомление участников с целями проведения тренировок;
- распределение ролей и обязанностей между участниками;
- обеспечение сопровождения участников в процессе тренировок;
- предоставление временных ресурсов, необходимых для проведения тренировок, в том числе для проведения анализа результатов тренировок;
- разработка отчетных материалов по результатам проведения тренировок и их доведение до всех участников тренировок.

Приложение А
(обязательное)

Подход к определению уровней влияния компьютерных инцидентов

В приложении А приведено описание подхода к определению уровней влияния компьютерных инцидентов.

Представленный подход может быть уточнен в соответствии с потребностями организации, ведущей деятельность по управлению компьютерными инцидентами.

А.1 Общие положения

Подход к определению уровней влияния компьютерных инцидентов основан на следующих критериях:

- ущерб в социальной сфере;
- ущерб в политической сфере;
- экономический ущерб;
- ущерб в экологической сфере;
- ущерб для обеспечения обороны страны, безопасности государства и правопорядка.

Все перечисленные критерии определены с учетом [1] и должны быть в обязательном порядке учтены субъектами КИИ. Данные критерии подлежат уточнению в случае внесения изменений в вышеуказанное постановление. Организации, не являющиеся субъектами КИИ, могут формировать свои критерии по примеру критериев, устанавливаемых для субъектов КИИ.

В зависимости от сферы деятельности организации не все критерии будут подходить для определения уровня влияния компьютерных инцидентов по отношению к ее информационным ресурсам. В таких случаях используются только те критерии, которые подходят для конкретной организации и ее информационных ресурсов. Чтобы понять, какие критерии подходят для конкретных информационных ресурсов организации, рекомендуется использовать результаты категорирования объектов КИИ.

Подход также предусматривает возможность использования дополнительных критериев, которые не определены в настоящем стандарте. Порядок применения дополнительных критериев определен в А.7.

По каждому критерию установлено не более четырех уровней влияния:

- критический;
- высокий;
- средний;
- низкий.

Итоговый уровень влияния компьютерного инцидента оценивается как максимальный уровень влияния среди определенных по разным критериям. Например, если для одного компьютерного инцидента по критерию «экономический ущерб» определен уровень влияния средний, а по критерию «ущерб в социальной сфере» для этого компьютерного инцидента определен уровень влияния высокий, то для данного компьютерного инцидента устанавливается высокий уровень влияния.

А.2 Ущерб в социальной сфере

Ущерб в социальной сфере классифицируют по четырем уровням влияния: критический, высокий, средний, и низкий.

Критический социальный ущерб будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с причинением ущерба жизни людей и (или) причинением ущерба здоровью 500 человек или более, и (или) прекращением или нарушением функционирования объектов обеспечения жизнедеятельности на территории более одного субъекта Российской Федерации или на территории города федерального значения, и (или) нарушением условий жизнедеятельности 5 000 человек или более, и (или) прекращением или нарушением функционирования объектов транспортной инфраструктуры на территории более одного субъекта Российской Федерации или на территории города федерального значения, и (или) недоступностью транспортных услуг для 5 000 человек или более, и (или) недоступностью сети связи для 5 000 человек или более, и (или) отсутствием доступа к государственной услуге, максимальное время недоступности которой не может превышать 6 ч.

Высокий социальный ущерб будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с причинением ущерба здоровью от 50 до 500 человек и (или) прекращением или нарушением функционирования объектов обеспечения жизнедеятельности на территории более одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения (но не за пределами территории одного субъекта Российской Федерации или территории города федерального значения), и (или) нарушением условий жизнедеятельности от 1 000 до 5 000 человек, и (или) прекращением или нарушением функционирования объектов транспортной инфраструктуры на территории более одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения (но не за пределами территории одного субъекта Российской Федерации или территории города федерального значения), и (или) недоступностью транспортных услуг от 1 000 до 5 000 человек или

более, и (или) недоступностью сети связи от 1 000 до 5 000 человек, и (или) отсутствием доступа к государственной услуге, максимальное время недоступности которой не может превышать от 6 до 12 ч.

Средний социальный ущерб будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с причинением ущерба здоровью от 1 до 50 человек и (или) прекращением или нарушением функционирования объектов обеспечения жизнедеятельности в одном муниципальном образовании (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения, и (или) нарушением условий жизнедеятельности от 2 до 1 000 человек и (или) прекращением или нарушением функционирования объектов транспортной инфраструктуры на территории одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения, и (или) недоступностью транспортных услуг от 2 до 1 000 человек, и (или) недоступностью сети связи от 2 до 1 000 человек, и (или) отсутствием доступа к государственной услуге, максимальное время недоступности которой не может превышать от 12 до 24 ч.

Низкий социальный ущерб будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с прекращением или нарушением функционирования объектов обеспечения жизнедеятельности и (или) прекращением или нарушением функционирования объектов транспортной инфраструктуры и (или) недоступностью транспортных услуг, и (или) недоступностью сети связи, и (или) отсутствием доступа к государственной услуге, которые не подпадают под критерии других уровней (критический, высокий, средний).

А.3 Ущерб в политической сфере

Ущерб в политической сфере классифицируют по трем уровням влияния: критический, высокий и средний.

Критический ущерб в политической сфере будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с прекращением или нарушением функционирования Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного суда Российской Федерации, Конституционного суда Российской Федерации.

Высокий ущерб в политической сфере будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с прекращением или нарушением функционирования федерального органа государственной власти.

Средний ущерб в политической сфере будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с прекращением или нарушением функционирования органа государственной власти субъекта Российской Федерации или города федерального значения.

А.4 Экономический ущерб

Экономический ущерб, вызванный компьютерными инцидентами, определяют с учетом тяжести последствий сбоя или полного прекращения деятельности из-за выхода из строя программного, технического или программно-технического оборудования информационного ресурса. Размер потерь (ущерба) может зависеть от затрат на восстановление штатной деятельности организации и других последствий компьютерных инцидентов, включая потерю прибыли и/или упущенные возможности. Экономический ущерб является единственным из рассмотренных в настоящем стандарте критериев, который могут использовать не только субъекты КИИ, но и организации, не относящиеся к субъектам КИИ. Этот подход классифицирует потери (ущерб) по четырем уровням влияния: критический, высокий, средний и низкий.

Критерии отнесения компьютерных инцидентов к указанным уровням, которые используют как субъекты КИИ, так и организации, не относящиеся к субъектам КИИ, представлены ниже.

Критический экономический ущерб для организации будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с прекращением деятельности организации на длительный период времени или полным прекращением деятельности и (или) с ущербом, выраженным в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности более чем на 20 % от годового объема доходов, усредненного за прошедший 5-летний период.

Высокий экономический ущерб для организации будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с прекращением деятельности организации на короткий период времени или остановкой отдельных видов деятельности и/или с ущербом, выраженным в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности от 10 до 20 % от годового объема доходов, усредненного за прошедший 5-летний период;

Средний экономический ущерб для организации будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с ущербом, выраженным в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности от 1 до 10 % от годового объема доходов, усредненного за прошедший 5-летний период.

Низкий экономический ущерб для организации будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с ущербом, выраженным в снижении уровня дохода, которое не подпадает под критерии других уровней (критический, высокий, средний).

При этом организации, не относящиеся к субъектам КИИ, могут устанавливать и иные критерии отнесения компьютерных инцидентов к указанным уровням.

Для субъектов КИИ должны дополнительно учитываться следующие критерии отнесения компьютерных инцидентов к указанным уровням экономического ущерба.

а) Критический экономический ущерб будет означать возможность возникновения в результате компьютерного инцидента любого из следующих негативных последствий:

1) возникновение ущерба бюджетам Российской Федерации, связанного со снижением выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом КИИ более чем на 0,1 % прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период;

2) прекращение или нарушение более 120 млн совершаемых в течение одного дня операций (на основе прогнозных значений), проводимых клиентами по банковским счетам и (или) без открытия банковского счета и (или) осуществляемых субъектом КИИ, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка.

б) Высокий экономический ущерб будет означать возможность возникновения в результате компьютерного инцидента любого из следующих негативных последствий:

1) возникновение ущерба бюджетам Российской Федерации, связанного со снижением выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом КИИ на 0,05 — 0,1 % прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период;

2) прекращение или нарушение от 70 до 120 млн совершаемых в течение одного дня операций (на основе прогнозных значений), проводимых клиентами по банковским счетам и (или) без открытия банковского счета и (или) осуществляемых субъектом КИИ, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка.

в) Средний экономический ущерб будет означать возможность возникновения в результате компьютерного инцидента любого из следующих негативных последствий:

1) возникновение ущерба бюджетам Российской Федерации, связанного со снижением выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом КИИ на 0,001 — 0,05 % прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период;

2) прекращение или нарушение от 3 до 70 млн совершаемых в течение одного дня операций (на основе прогнозных значений), проводимых клиентами по банковским счетам и (или) без открытия банковского счета и (или) осуществляемых субъектом КИИ, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка.

г) Низкий экономический ущерб будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, приводящих к ущербу бюджетам Российской Федерации, связанному со снижением выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом КИИ, и (или) приводящих к прекращению или нарушению операций, проводимых клиентами по банковским счетам и (или) без открытия банковского счета и (или) осуществляемых субъектом КИИ, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, которые не подпадают под критерии других уровней (критический, высокий, средний).

А.5 Ущерб в экологической сфере

Ущерб в экологической сфере классифицируют по четырем уровням влияния: критический, высокий, средний и низкий.

Критический ущерб в экологической сфере будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с вредными воздействиями на окружающую среду на территории, выходящей за пределы одного субъекта Российской Федерации или города федерального значения, и (или) вредными воздействиями на 5 000 человек и более.

Высокий ущерб в экологической сфере будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с вредными воздействиями на окружающую среду на территории, выходящей за пределы одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения, и (или) вредными воздействиями на 1 000—5 000 человек.

Средний ущерб в экологической сфере будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с вредными воздействиями на окружающую среду на тер-

ритории в пределах территории одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения и (или) вредными воздействиями на 2—1 000 человек.

Низкий ущерб в экологической сфере будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с вредными воздействиями на окружающую среду и (или) вредными воздействиями на людей, не подпадающих под критерии других уровней (критический, высокий, средний).

А.6 Ущерб для обеспечения обороны страны, безопасности государства и правопорядка

Ущерб для обеспечения обороны страны, безопасности государства и правопорядка классифицируют по трем уровням влияния: критический, высокий, средний.

Критический ущерб для обеспечения обороны страны, безопасности государства и правопорядка будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с прекращением или нарушением функционирования пункта управления государством или ситуационного центра Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного суда Российской Федерации, Конституционного суда Российской Федерации и (или) снижением объемов продукции (работ, услуг) в рамках государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом КИИ, в заданный период времени более чем на 15 %, и (или) увеличением времени выпуска продукции (работ, услуг) заданного объема в рамках государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом КИИ, более чем на 40 %, и (или) прекращением или нарушением функционирования (невыполнением установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, для которой определено максимально допустимое время недоступности пользователю до 1 ч.

Высокий ущерб для обеспечения обороны страны, безопасности государства и правопорядка будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с прекращением или нарушением функционирования пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации и (или) со снижением объемов продукции (работ, услуг) в рамках государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом КИИ, в заданный период времени на 10—15 %, и (или) увеличением времени выпуска продукции (работ, услуг) заданного объема в рамках государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом КИИ, на 10—40 %, и (или) прекращением или нарушением функционирования (невыполнением установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, для которой определено максимально допустимое время недоступности пользователю от 1 до 2 ч.

Средний ущерб для обеспечения обороны страны, безопасности государства и правопорядка будет означать возможность возникновения в результате компьютерного инцидента негативных последствий, связанных с прекращением или нарушением функционирования пункта управления или ситуационного центра органа государственной власти субъекта Российской Федерации или города федерального значения, и (или) со снижением объемов продукции (работ, услуг) в рамках государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом КИИ, в заданный период времени до 10 %, и (или) увеличением времени выпуска продукции (работ, услуг) заданного объема в рамках государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом КИИ, до 10 %, и (или) прекращением или нарушением функционирования (невыполнением установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, для которой определено максимально допустимое время недоступности пользователю от 2 до 4 ч.

А.7 Порядок применения дополнительных критериев

Организации могут формировать свои критерии по примеру критериев, установленных в А.2—А.6. Например, в организации могут быть установлены критерии, связанные с экономическим ущербом, выраженным в затратах на восстановление информационных ресурсов. Критерии должны быть определены не более чем по четырем уровням влияния: критический, высокий, средний, низкий. При этом допускается использовать меньшее количество уровней влияния. Например, если по определенному критерию не может быть низкого ущерба, допускается устанавливать уровни влияния: критический, высокий и средний. Бывают и другие ситуации, когда по определенному критерию не может быть критического ущерба, в таких случаях могут быть установлены уровни влияния: высокий, средний и низкий.

Приложение Б
(обязательное)

Подход к определению приоритетов компьютерных инцидентов и очередности реагирования на компьютерные инциденты

В приложении Б приведено описание подхода к определению приоритетов компьютерных инцидентов и очередности реагирования на компьютерные инциденты.

Представленный подход может быть уточнен в соответствии с потребностями организации, ведущей деятельность по управлению компьютерными инцидентами.

Б.1 Общие положения

Подход к определению приоритетов компьютерных инцидентов основан на использовании следующих характеристик регистрируемых компьютерных инцидентов:

- значимость элементов информационной инфраструктуры, на которых обнаружены признаки зарегистрированного компьютерного инцидента;
- масштаб компьютерного инцидента.

Подход к определению приоритетов компьютерных инцидентов также предусматривает возможность использования дополнительных критериев, которые не определены в настоящем стандарте.

По каждому критерию установлено не более трех приоритетов:

- высокий;
- средний;
- низкий.

Итоговый приоритет компьютерного инцидента оценивают как максимальный приоритет среди определенных по разным критериям. Например, если по критерию «значимость элементов информационной инфраструктуры» приоритет компьютерного инцидента определен как высокий, а по критерию «масштаб компьютерного инцидента» как средний, то итоговый приоритет компьютерного инцидента определяют как высокий.

Приоритеты не зависят от уровней влияния компьютерных инцидентов и могут использоваться совместно с ними для определения очередности отработки компьютерных инцидентов. Порядок определения очередности реагирования на компьютерные инциденты приведен в таблице Б.1.

Таблица Б.1 — Порядок определения очередности реагирования на компьютерные инциденты

Очередь реагирования	1-я	2-я	3-я	4-я	5-я	6-я	7-я	8-я	9-я
Уровень влияния компьютерного инцидента	Критический	Высокий	Высокий	Средний	Средний	Средний	Низкий	Низкий	Низкий
Приоритет компьютерного инцидента	Высокий	Высокий	Средний	Высокий	Средний	Низкий	Высокий	Средний	Низкий

Б.2 Значимость элементов информационной инфраструктуры

В соответствии с данным показателем приоритет компьютерного инцидента определяют в зависимости от значимости СВТ, на которых обнаружены признаки данного компьютерного инцидента. Значимость СВТ определяют в зависимости от функционирующих на данном СВТ сервисов, содержащейся на нем информации и (или) возможности распространения компьютерного инцидента на более значимые СВТ.

К высокому приоритету рекомендуется относить компьютерные инциденты, признаки которых обнаружены на СВТ, на которых функционируют сервисы, нарушение которых может привести к прекращению или нарушению самых критичных процессов организации либо компьютерные инциденты, признаки которых обнаружены на СВТ, на которых обрабатывается информация, необходимая для обеспечения самых критичных процессов организации.

К среднему приоритету рекомендуется относить компьютерные инциденты, признаки которых обнаружены на СВТ, с которых компьютерный инцидент наиболее быстро может распространиться на СВТ, на которых функционируют сервисы, нарушение которых может привести к прекращению или нарушению самых критичных про-

цессов организации, либо на СВТ, на которых обрабатывается информация, необходимая для обеспечения самых критичных процессов организации.

К низкому приоритету рекомендуется относить остальные компьютерные инциденты.

Примечание — Важно отличать приоритет от уровня влияния, так как уровень влияния определяется критичностью затронутого компьютерным инцидентом процесса, а при определении приоритета учитывают и другие критические процессы, функционирующие на тех же СВТ.

Б.3 Масштаб компьютерного инцидента

В соответствии с данным показателем приоритет компьютерного инцидента определяют в зависимости от количества СВТ, на которых обнаружены признаки зарегистрированного компьютерного инцидента.

К высокому приоритету рекомендуется относить компьютерные инциденты, признаки которых обнаружены на 30 % и более процентах СВТ.

К среднему приоритету рекомендуется относить компьютерные инциденты, признаки которых обнаружены на 10—30 % СВТ.

К низкому приоритету рекомендуется относить компьютерные инциденты, признаки которых обнаружены менее чем на 10 % СВТ.

Библиография

[1] Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

УДК 004.622:006.354 ОКС 35.020

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

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 30.11.2022. Подписано в печать 07.12.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,92.

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.
www.gostinfo.ru info@gostinfo.ru