ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59710— 2022

Защита информации

УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

Общие положения

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. № 1376-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 Стадии управления компьютерными инцидентами 5

Введение

С целью обеспечения защищенности информационных ресурсов Российской Федерации от компьютерных атак и штатного функционирования данных ресурсов в условиях возникновения компьютерных инцидентов, вызванных компьютерными атаками, создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

В рамках функционирования ГосСОПКА устанавливается единый структурированный подход к организации и ведению деятельности по управлению компьютерными инцидентами, взаимосвязанной с общей деятельностью по обеспечению информационной безопасности в целом, направленный на обеспечение эффективного реагирования на компьютерные инциденты. Такой подход предусматривает реализацию следующих стадий 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.

Принципы единого структурированного подхода к организации и ведению деятельности по управлению компьютерными инцидентами в рамках функционирования ГосСОПКА определены в следующих стандартах:

а) ГОСТ Р 59710 (настоящий стандарт) — определяет содержание следующих стадий управления компьютерными инцидентами:

1) организация деятельности по управлению компьютерными инцидентами;
2) обнаружение и регистрация компьютерных инцидентов;
3) реагирование на компьютерные инциденты;
4) анализ результатов деятельности по управлению компьютерными инцидентами;

б) ГОСТ Р 59711 — определяет содержание этапов организации деятельности по управлению компьютерными инцидентами, а именно:

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

в) ГОСТ Р 59712 — определяет содержание этапов, выполняемых на стадиях:

1) обнаружение и регистрация компьютерных инцидентов;
2) реагирование на компьютерные инциденты;
3) анализ результатов деятельности по управлению компьютерными инцидентами.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

Общие положения

Information protection. Computer incident management. General provisions

Дата введения — 2023—02—01

1 Область применения

Настоящий стандарт является основополагающим для серии стандартов по управлению компьютерными инцидентами в рамках функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА). В настоящем стандарте определено содержание стадий управления 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 (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 59711—2022 Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами

ГОСТ Р 59712 Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты

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 Общие положения

4.1 Общие принципы управления компьютерными инцидентами

Для обнаружения компьютерных инцидентов используют результаты проводимого в организации мониторинга информационной безопасности, в рамках которого осуществляется сбор информации о событиях безопасности и иных данных мониторинга, необходимых для поиска признаков возможного возникновения компьютерных инцидентов. Такие признаки представляют собой совокупность зарегистрированных событий безопасности и иных данных мониторинга, а также условий, при которых такая совокупность зарегистрированных событий безопасности и иных данных мониторинга может свидетельствовать о возможном возникновении компьютерного инцидента. Для сбора событий безопасности и иных данных мониторинга и последующего поиска признаков возможного возникновения компьютерных инцидентов, как правило, применяют средства управления событиями информационной безопасности. Такие средства позволяют осуществлять сбор, нормализацию, агрегацию событий безопасности и иных данных мониторинга и на основании настроенных правил (далее — правила регистрации признаков возможного возникновения компьютерных инцидентов) проводить автоматизированный анализ и корреляцию событий безопасности и иных данных мониторинга.

Примечания

1 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.

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

3 Некоторые данные мониторинга используют только как аналитические данные при формировании правил регистрации признаков возможного возникновения компьютерных инцидентов. К таким данным мониторинга, например, могут относиться данные об индикаторах компрометации. На основе данных об индикаторах компрометации можно сформировать новое правило, которое предусматривает анализ событий безопасности, ранее не использовавшихся в правилах регистрации признаков возможного возникновения компьютерных инцидентов. Другие данные мониторинга, в первую очередь данные о зарегистрированных событиях безопасности, используют непосредственно для обнаружения и регистрации компьютерных инцидентов как условия для правил регистрации признаков возможного возникновения компьютерных инцидентов.

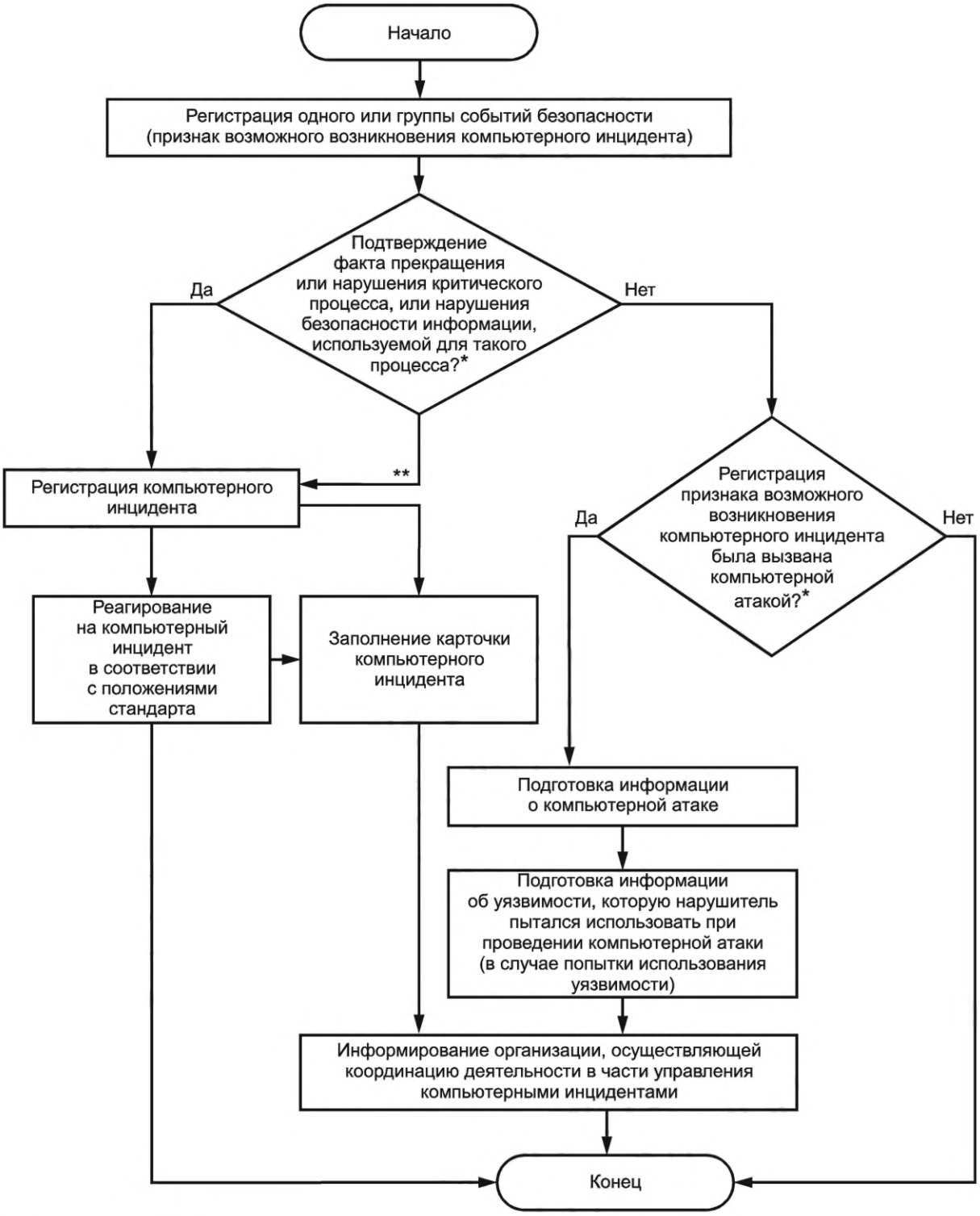
Для всех зарегистрированных признаков возможного возникновения компьютерных инцидентов необходимо проводить проверку факта их возникновения. Если в ходе проверки подтверждается факт возникновения компьютерного инцидента, то должна осуществляться его регистрация.

Если в ходе проверки не может быть однозначно подтверждено отсутствие факта возникновения компьютерного инцидента, то в этом случае также осуществляется его регистрация. При этом в ходе реагирования на компьютерный инцидент факт его возникновения может быть не подтвержден, что может являться основанием для его закрытия.

Если в ходе проверки подтверждается отсутствие факта возникновения компьютерного инцидента, то в этом случае он не регистрируется. При этом должна быть установлена причина регистрации признака возможного возникновения компьютерного инцидента. Если причиной регистрации признака возникновения компьютерного инцидента являлась компьютерная атака, организация, являющаяся субъектом ГосСОПКА, должна подготовить информацию о компьютерной атаке и уязвимости, которую злоумышленник пытался использовать при проведении этой компьютерной атаки и передать ее в организацию, осуществляющую координацию деятельности в части управления компьютерными инцидентами в виде карточки компьютерной атаки и карточки уязвимости.

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

На рисунке 1 представлен общий подход к обнаружению и регистрации компьютерных инцидентов, реагированию на них и информированию организации, осуществляющей координацию деятельности в части управления компьютерными инцидентами.



* Проверка факта возникновения компьютерного инцидента.

** Отсутствие факта возникновения компьютерного инцидента не может быть однозначно подтверждено.

Рисунок 1 — Общий подход к обнаружению и регистрации компьютерных инцидентов, реагированию на них и информированию организации, осуществляющей координацию деятельности в части управления компьютерными инцидентами

К компьютерным инцидентам относятся 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 компьютерной 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.

Субъекты ГосСОПКА, являющиеся субъектами критической информационной инфраструктуры, определяют критические процессы в соответствии с законодательством Российской Федерации. Иные субъекты ГосСОПКА определяют критические процессы установленным в организации порядком.

Для эффективного ведения деятельности по управлению компьютерными инцидентами в организации должны быть использованы не только средства управления событиями информационной безопасности, но и средства управления инцидентами, а также специализированные средства, предназначенные для обмена информацией о компьютерных атаках, компьютерных инцидентах и уязвимостях (средства обмена информацией).

Средства управления инцидентами должны обеспечивать автоматизацию процесса реагирования на компьютерные инциденты.

Средства обмена информацией следует использовать для взаимодействия с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами, и с иными внешними организациями.

Обмен информацией и взаимодействие с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами, и с иными внешними организациями значительно повышает эффективность управления компьютерными инцидентами, так как в некоторых случаях компьютерные инциденты не могут быть разрешены организацией самостоятельно (собственными силами) или могут выходить за пределы зоны ответственности одной организации.

4.2 Цели внедрения структурированного подхода к управлению компьютерными инцидентами

Использование структурированного подхода к управлению компьютерными инцидентами направлено на достижение следующих целей:

а) повышение эффективности реагирования на компьютерные инциденты

Повышению эффективности реагирования на компьютерные инциденты способствуют планирование и распределение ресурсов подразделений организации, участвующих в деятельности по управлению компьютерными инцидентами, а также возможность совместного использования информации о зарегистрированных компьютерных инцидентах специалистами подразделения, ответственного за управление компьютерными инцидентами, специалистами смежных подразделений, участвующих в деятельности по управлению компьютерными инцидентами, а также организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

Кроме того, управление компьютерными инцидентами предусматривает определение очередности реагирования на компьютерные инциденты с учетом их приоритетов и уровней влияния. Реагирование на компьютерные инциденты с учетом их приоритетов и уровней влияния позволяет исключить ситуации, в которых действия по реагированию проводят в режиме «быстрая реакция», когда компьютерные инциденты отрабатываются в порядке их регистрации, что может привести к несвоевременному реагированию на инциденты, оказывающие наибольшее негативное влияние на информационные ресурсы.

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

б) снижение негативного воздействия на процессы организации

Деятельность по управлению компьютерными инцидентами в первую очередь направлена на снижение уровня потенциальных негативных последствий от компьютерных инцидентов для процессов, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям в сфере обеспечения обороны страны,

безопасности государства и правопорядка, финансовым потерям или долгосрочным убыткам, возникающим из-за испорченной репутации и потери доверия к организации;

в) предотвращение компьютерных инцидентов

Анализ данных, связанных с компьютерными инцидентами, проводимый в рамках деятельности по управлению компьютерными инцидентами, направлен на выявление закономерностей и тенденций произошедших ранее компьютерных инцидентов, информация о которых может быть использована для приобретения и накопления опыта, а также при разработке рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов с целью предотвращения их повторного возникновения;

г) обеспечение повышения осведомленности (информирования) в области управления компьютерными инцидентами

Деятельность по управлению компьютерными инцидентами предусматривает информирование специалистов, участвующих в управлении компьютерными инцидентами, с учетом полученного опыта.

5 Стадии управления компьютерными инцидентами

5.1 Краткое описание

Для достижения целей, изложенных в 4.2, структурированный подход к организации и ведению деятельности по управлению компьютерными инцидентами включает в себя четыре стадии:

- организация деятельности по управлению компьютерными инцидентами;
- обнаружение и регистрация компьютерных инцидентов;
- реагирование на компьютерные инциденты (включая фиксацию материалов, связанных с возникновением компьютерных инцидентов и установление причин и условий возникновения компьютерных инцидентов);
- анализ результатов деятельности по управлению компьютерными инцидентами.

Высокоуровневое представление этих стадий показано на рисунке 2.



Рисунок 2 — Стадии управления компьютерными инцидентами

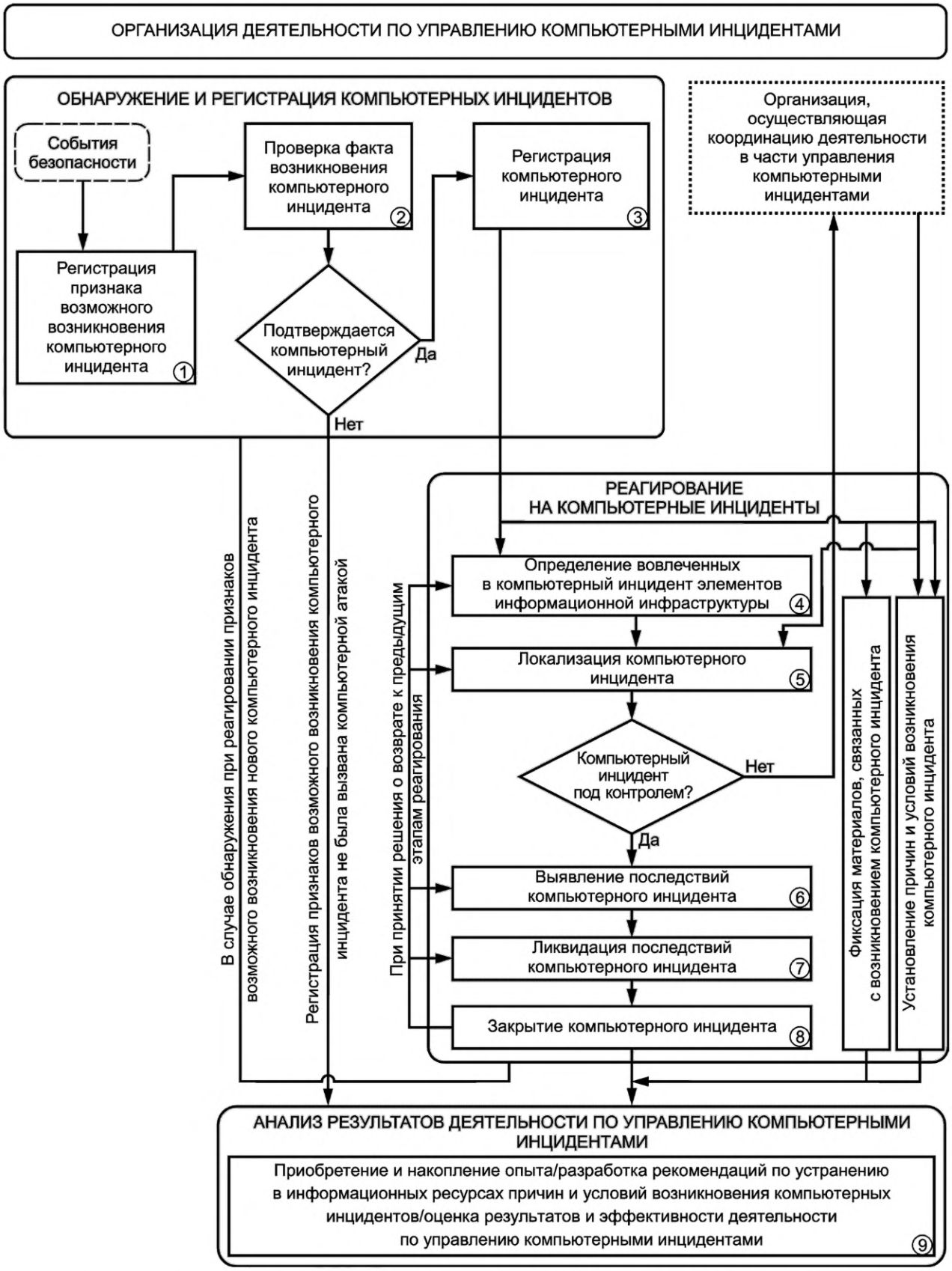


Рисунок 3 — Общий порядок ведения деятельности по управлению компьютерными инцидентами

Серия стандартов по управлению компьютерными инцидентами включает:

а) настоящий стандарт — охватывает все четыре стадии;

б) ГОСТ Р 59711 — охватывает стадию «организация деятельности по управлению компьютерными инцидентами»;

в) ГОСТ Р 59712 — охватывает стадии:

1) обнаружение и регистрация компьютерных инцидентов;

2) реагирование на компьютерные инциденты;

3) анализ результатов деятельности по управлению компьютерными инцидентами.

На рисунке 3 показан общий порядок ведения деятельности по управлению компьютерными инцидентами с детализацией стадий их управления.

5.2 Организация деятельности по управлению компьютерными инцидентами

Эффективное управление компьютерными инцидентами требует соответствующего планирования и подготовки. Для организации деятельности по управлению компьютерными инцидентами организация должна выполнить следующие мероприятия:

- разработать политику управления компьютерными инцидентами;
- разработать план реагирования на компьютерные инциденты;
- определить подразделение, ответственное за управление компьютерными инцидентами;
- организовать взаимодействие с подразделениями внутри организации и с внешними организациями;
- реализовать материально-техническое оснащение подразделения, ответственного за управление компьютерными инцидентами;
- организовать обучение и информирование в части управления компьютерными инцидентами;
- провести тренировки по отработке мероприятий плана реагирования на компьютерные инциденты.

5.3 Обнаружение и регистрация компьютерных инцидентов

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

Примечание — В состав собираемых данных помимо информации о зарегистрированных событиях безопасности, как правило, входят инвентаризационные данные, данные о сетевой активности, новостные ленты, касающиеся текущей политической, социальной или экономической деятельности (обстановки), которая может повлиять на активность, связанную с компьютерными инцидентами, информация о тенденциях, связанных с компьютерными инцидентами, о новых векторах атак и текущих индикаторах атак (индикаторах компрометации).

Стадия управления компьютерными инцидентами «обнаружение и регистрация компьютерных инцидентов» состоит из двух последовательных этапов:

- регистрация признаков возможного возникновения компьютерных инцидентов.

Примечания

1 Регистрация признаков возможного возникновения компьютерных инцидентов осуществляется как 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), так и автоматизированным способом (с использованием средства управления событиями информационной безопасности) на основе правил регистрации признаков возможного возникновения компьютерных инцидентов.

2 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.

При неавтоматизированном способе регистрации признака возможного возникновения компьютерных инцидентов специалист подразделения, ответственного за управление компьютерными инцидентами, самостоятельно регистрирует данный признак в средстве управления инцидентами (заполняет карточку признака возможного возникновения компьютерного инцидента);

- подтверждение компьютерных инцидентов.

Примечание — На этапе «подтверждение компьютерных инцидентов» проводится оценка 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 осуществляется сбор и внесение дополнительной информации. В случае подтверждения компьютерного инцидента осуществляется его регистрация и создание карточки 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.

5.4 Реагирование на компьютерные инциденты

Реагирование на компьютерные инциденты осуществляют специалисты подразделения, ответственного за управление компьютерными инцидентами, и специалисты смежных подразделений, участвующих в деятельности по управлению компьютерными инцидентами, входящие в состав рабочих групп реагирования на компьютерные инциденты.

В ходе реагирования на компьютерный инцидент должны быть выполнены следующие этапы:

- определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры.

Примечание — В карточке компьютерного инцидента может отсутствовать информация о полном множестве элементов информационной инфраструктуры, вовлеченных в компьютерный инцидент. Поэтому крайне важно до начала этапа «локализация компьютерного инцидента» определить полное множество элементов информационной инфраструктуры, вовлеченных в компьютерный инцидент и внести эту информацию в карточку компьютерного инцидента;

- локализация компьютерного инцидента.

Примечание — На этапе «локализация компьютерного инцидента» специалисты подразделения, ответственного за управление компьютерными инцидентами, должны определить, находится ли компьютерный инцидент под контролем. Если компьютерный инцидент находится под контролем, то выполняются последующие этапы реагирования. Если компьютерный инцидент не находится под контролем или ожидается, что он окажет серьезное воздействие на критические процессы (приведет к серьезным последствиям) организации, целесообразно направить обращения в организацию, осуществляющую координацию деятельности в части управления компьютерными инцидентами, об оказании содействия в реагировании на компьютерный инцидент.

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;

- выявление последствий компьютерного инцидента.

Примечание — На этапе «выявление последствий компьютерного инцидента» выполняются процедуры по выявлению признаков негативного воздействия компьютерного инцидента на информационные ресурсы;

- ликвидация последствий компьютерного инцидента.

Примечание — На этапе «ликвидация последствий компьютерных инцидентов» выполняются процедуры по восстановлению штатного функционирования информационных ресурсов и обрабатываемой им информации;

- закрытие компьютерного инцидента.

Примечания

1 На каждом из этапов стадии «реагирование на компьютерные инциденты» специалисты, ответственные за реагирование на компьютерные инциденты (руководители рабочих групп реагирования на компьютерные инциденты), должны осуществлять проверку качества и достаточности выполненных действий по реагированию на компьютерный инцидент и при необходимости создавать задания на доработку выполненных действий, а также принимать решение о возврате на предыдущий этап реагирования.

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.

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 привлече-

ния организации, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

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

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

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

Помимо перечисленных этапов реагирования организация должна решать следующие ключевые задачи:

- определение принципа очередности реагирования на компьютерные инциденты.

Примечание — Очередность реагирования на компьютерные инциденты должна определяться с учетом уровня их влияния и приоритетов;

- обеспечение документирования всех действий вовлеченных сторон и, в частности, специалистов подразделения, ответственного за управление компьютерными инцидентами, для последующего анализа и оценки;
- безопасное хранение зафиксированных материалов, связанных с возникновением компьютерных инцидентов (цифровых свидетельств), которые требуются для установления причин и условий возникновения компьютерных инцидентов;
- информирование о возникновении компьютерного инцидента и обмен информацией с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

Вся собранная информация, относящаяся к компьютерному инциденту, должна быть отражена в карточке компьютерного инцидента и быть максимально полной. Это позволяет качественно проводить анализ результатов деятельности по управлению компьютерными инцидентами.

5.5 Анализ результатов деятельности по управлению компьютерными инцидентами

Заключительная стадия управления компьютерными инцидентами «Анализ результатов деятельности по управлению компьютерными инцидентами» осуществляется после того, как компьютерный инцидент был закрыт. Данная стадия включает в себя следующие этапы:

- приобретение и накопление опыта по результатам управления компьютерными инцидентами.

Примечание — Приобретение и накопление опыта по результатам деятельности по управлению компьютерными инцидентами предусматривает идентификацию методов и способов обнаружения и реагирования на компьютерные инциденты, которые показали свою эффективность в отношении уже закрытых компьютерных инцидентов.

Идентифицированная информация может быть использована при доработке (актуализации) документации в части управления компьютерными инцидентами;

- разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов.

Примечание — Разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов осуществляется с целью предотвращения их повторного возникновения;

- оценка результатов и эффективности реагирования на компьютерные инциденты.

Примечание — Оценка результатов и эффективности реагирования на компьютерные инциденты предусматривает проведение анализа процессов, процедур, форматов отчетов и состава рабочих групп при реагировании на компьютерные инциденты и оценки их эффективности. Организация должна периодически проводить комплексную оценку результатов и эффективности реагирования на компьютерные инциденты.

На основе оценки результатов и эффективности реагирования на компьютерные инциденты осуществляется (при необходимости) доработка (актуализация) документации в части управления компьютерными инцидентами;

На стадии «анализ результатов деятельности по управлению компьютерными инцидентами» организация также должна решать следующие ключевые задачи:

- информирование и обмен результатами деятельности по управлению компьютерными инцидентами с заинтересованными организациями (при необходимости);
- определение состава информации о компьютерных инцидентах, связанных с ними векторах атак и уязвимостях, которая может быть передана организациям, с которыми осуществляется взаимодействие, в целях предотвращения возникновения таких же компьютерных инцидентов в их информационной инфраструктуре.

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 *М.В. Бучная*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 30.11.2022. Подписано в печать 02.12.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68.

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