ДИТ

Реагирование на компьютерные атаки и инциденты субъектом КИИ

Валерий Комаров, начальник отдела обеспечения осведомленности, ДИТ Москвы

ДИТ

Порядок действия работников ЗОКИИ при компьютерных инцидентах

Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»

Методические рекомендации НКЦКИ по установлению причин и ликвидации последствий компьютерных инцидентов

Методические рекомендации НКЦКИ по разработке плана реагирования на компьютерные инциденты

Рекомендации ФСТЭК России по подготовке планов мероприятий, реализуемых субъектами критической информационной инфраструктуры Российской Федерации при установлении в отношении принадлежащих им объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак

ГОСТ Р 53131 — 2008 (ИСО/МЭК ТО 24762:2008) «Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий»

ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования

NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide «Руководство по обработке инцидентов компьютерной безопасности»

Проекты национальных стандартов ГОСТ Р:

- «Управление инцидентами, связанными с безопасностью информации. Руководство по планированию и подготовке к реагированию на инциденты»
- «Управление инцидентами, связанными с безопасностью информации. Руководство по реагированию на инциденты в сфере информационных и компьютерных технологий»
- «Управление инцидентами, связанными с безопасностью информации. Принципы менеджмента инцидентов»

Новые требования ФСБ России

Приказ ФСБ России от 07.07.2022 № 348 «О внесении изменений в Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом ФСБ России от 19 июня 2019 г. № 282»

Начало действия документа: 16.08.2022

Разработанный План утверждается руководителем субъекта критической информационной инфраструктуры (индивидуальным предпринимателем - субъектом критической информационной инфраструктуры), которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры.

Копия утвержденного Плана в срок **до 7 календарных дней** со дня утверждения направляется в НКЦКИ.

ДИТ

Типовое положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации)

14. Ответственное лицо с использованием нормативных правовых документов и методических материалов Федеральной службы безопасности Российской Федерации организует обнаружение, предупреждение и ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты с информационными ресурсами органа (организации), а также взаимодействие с Национальным координационным центром по компьютерным инцидентам одним (или несколькими) из следующих способов:

а) силами структурного подразделения, ответственного за обеспечение информационной безопасности, с заключением соглашения (издания совместного акта) о взаимодействии с Федеральной службой безопасности Российской Федерации (Национальным координационным центром по компьютерным инцидентам), включающего в том числе права и обязанности сторон, порядок проведения совместных мероприятий, регламент информационного обмена, порядок и сроки представления отчетности, порядок и формы контроля;

б) силами структурного подразделения, ответственного за обеспечение информационной безопасности, с его аккредитацией как центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

в) силами организаций, являющихся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

ДИТ

Компьютерный инцидент и инцидент ИБ

Заражение ВПО

В случае, когда ВПО было обнаружено и удалено средством антивирусной защиты, и при этом не привело к нарушению безопасности информации, обрабатываемой в информационном ресурсе или к нарушению и (или) прекращению функционирования информационного ресурса компьютерный инцидент не регистрируется, но при этом по решению организации такой факт может регистрироваться как инцидент ИБ

Несанкционированное изменение информации

В случае, когда изменение содержания произошло по отношению к информации, для которой не применялись требования к целостности по решению организации такой факт может регистрироваться как инцидент ИБ. Примером данной ситуации является повреждение файлов не относящихся к выполнению критических процессов или иных важных для организации процессов (например, файлов, содержащих тексты служебных записок, и прочих файлов, которые создают пользователи автоматизированных рабочих мест)

Несанкционированное разглашение информации

В случае, когда произошло разглашение информации, для которой организация не устанавливает требования по обеспечению ее конфиденциальности по решению организации такой факт может регистрироваться как инцидент ИБ

ДИТ

Реагирование/действия работников при обнаружении компьютерных инцидентов на значимом объекте КИИ

1. Документирование информации о компьютерных инцидентах (цифровых свидетельств), предпринятых действий по реагированию и последующих действий, выполненных в процессе деятельности по управлению компьютерными инцидентами

2. Взаимодействие между специалистами подразделения по управлению компьютерными инцидентами, специалистами смежных подразделений и подразделений, задействованных в деятельности по управлению компьютерными инцидентами, а также с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами и с иными внешними организациями

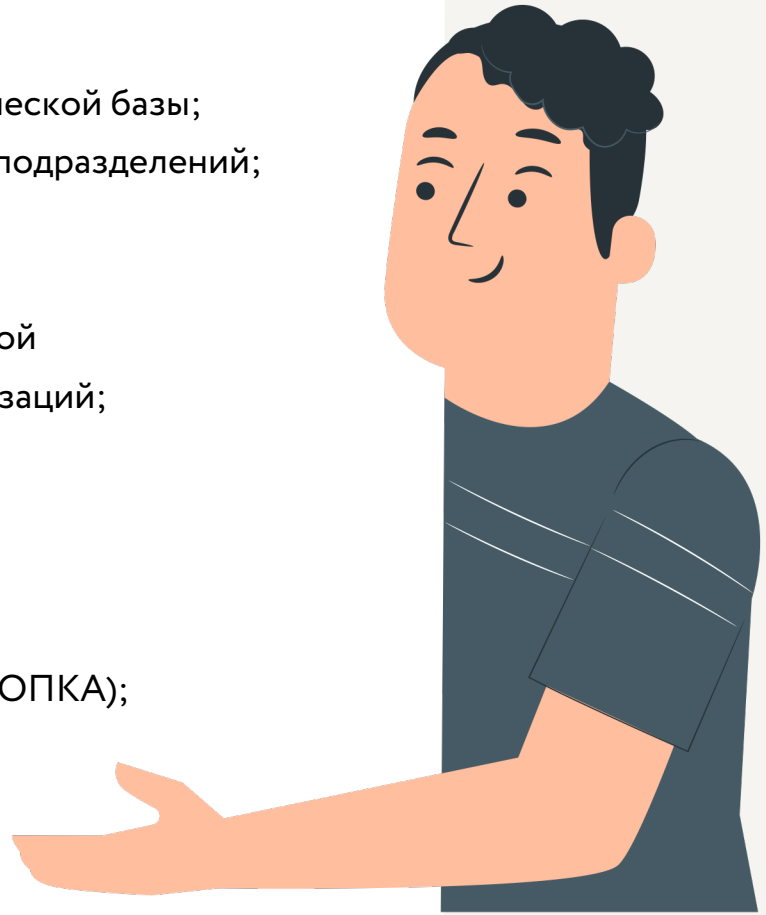
3. Уведомление руководства и других заинтересованных сторон о существенных (с высоким уровнем влияния) инцидентах

4. Обмен информацией с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами

Планируем действия при реагировании на компьютерный инцидент

Учитываем при разработке и актуализации Плана реагирования:

- Разработку, ведение и совершенствование нормативно-правовой и методической базы;
- Совершенствование организационно-штатной структуры задействованных подразделений;
- Оснащение подразделений специальной техникой и оборудованием;
- Поддержание готовности сил и средств к реагированию на инциденты ИБ;
- Обеспечение уровня профессиональной подготовки к действиям в аварийной обстановке руководителей и персонала организаций, привлекаемых организаций;
- Проведение учений и тренировок;
- Маркеры (вехи) для старта выполнения этапов плана;
- Приоритезация мероприятий;
- Научно-техническая поддержка принятия решений в условиях ликвидации аварии и чрезвычайной ситуации (НКЦКИ, ФСТЭК, Отраслевой центр ГосСОПКА);
- Оперативный обмен информацией и взаимодействие с правоохранительными органами и СМИ



Рекомендации по ликвидации последствий компьютерного инцидента

Основные цели

- Минимизировать последствия компьютерного инцидента, сохраняя непрерывность критических процессов;
- Обеспечить эффективное и своевременное восстановление работоспособности (штатного функционирования) информационных ресурсов;
- Повысить уровень обеспечения ИБ в организации и эффективность ведения деятельности по управлению компьютерными инцидентами

Этап локализации компьютерного инцидента представляет собой действия, направленные на определение и ограничение функционирования информационных ресурсов, на которых обнаружены признаки зарегистрированного компьютерного инцидента с целью предотвращения его дальнейшего распространения

Цель локализации компьютерного инцидента состоит в том, чтобы предотвратить следующие возможные действия злоумышленника:

- предотвратить нарушения конфиденциальности, целостности или доступности информации в следствие НСД;
- предотвратить несанкционированное вмешательство в работу информационного ресурса;
- предотвратить использование информационного ресурса для атаки на смежные ресурсы.

Выявление последствий компьютерного инцидента

Основные цели

- Выявление признаков негативного воздействия на элементы информационной инфраструктуры в результате компьютерного инцидента;
- Оценку негативного влияния компьютерного инцидента на информационные ресурсы, задействованные в компьютерном инциденте.

При оценке негативного воздействия на элементы информационной инфраструктуры в результате компьютерного инцидента должны оцениваться

- Трудозатраты, связанные с проведением мероприятий по реагированию на компьютерный инцидент;
- Время простоя функционирования информационных ресурсов;
- Вред, причиненный интересам лица, ответственного за эксплуатацию элемента информационной инфраструктуры, подверженного воздействию, пользователя (пользователей) элемента информационной инфраструктуры, подверженного воздействию, в том числе связанный с нарушением конфиденциальности, целостности и доступности сведений, обрабатываемых данным объектом;
- Вред, причиненный организации, в том числе репутационные потери, экономический ущерб и иной вред;
- Финансовые затраты на восстановление штатного функционирования информационных ресурсов.

ДИТ

Ликвидация последствий компьютерного инцидента

При недостаточной квалификации специалистов руководителем (его заместителем или ответственным за отработку компьютерного инцидента) должно приниматься решение о необходимости взаимодействия с организациями, осуществляющими координацию деятельности в части управления компьютерными инцидентами в целях получения необходимой технической помощи.

При проведении мероприятий по установлению причин возникновения компьютерного инцидента фиксируются

- Технические данные
- Результаты проводимых исследований носителей информации
- Результаты анализа технических данных
- Иная информация о компьютерном инциденте (цифровые свидетельства)

ДИТ

Установление причин компьютерных инцидентов

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

Проводится

- Анализ действий пользователей;
- Системный анализ;
- Сетевой анализ;
- Анализ программных и информационных объектов.

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

- Действия пользователей (администраторов), которые выполнялись с информационным ресурсом до и во время регистрации компьютерного инцидента (например, посещение веб-сайта, открытие сообщения электронной почты, открытие электронного документа, подключение носителя информации к СВТ, подключение СВТ к сетевой розетке);
- Сведения об игнорировании пользователем (администратором) появляющихся сообщений (о необходимости выполнить обновление ОС, ее перезагрузку, о необходимости ввести в определенные поля учетные данные пользователя, о выявленном потенциально вредоносном файле)

ДИТ

Всегда на связи!

mos.ru/dit