АДМИНИСТРАЦИЯ КАЧКАНАРСКОГО ГОРОДСКОГО ОКРУГА СВЕРДЛОВСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

29.09.2023 № 83

г. Качканар

Об информационной безопасности (защите информации) в Администрации Качканарского городского округа Свердловской области

Во исполнение федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в Администрации Качканарского городского округа Свердловской области:

1. Утвердить :

1) Положение об информационной безопасности (защите информации) Администрации Качканарского городского округа Свердловской области (Приложение 1);

2) Методическое руководство по организации технических мероприятий, направленных на проведение служебных проверок при возникновении компьютерных инцидентов (Приложение 2);

3) Формы отчета о событиях и инцидентах информационной безопасности (Приложение 3);

4) Состав постоянно действующей комиссии по информационной безопасности (защите информации) в Администрации Качканарского городского округа (Приложение 4);

5) Состав группы реагирования на инциденты информационной безопасности в Администрации Качканарского городского округа Свердловской области (Приложение 5);

6) Инструкцию пользователя Администрации Качканарского городского округа Свердловской области (Приложение 6);

7) Журнал регистрации пользователей Администрации Качканарского городского округа Свердловской области (Приложение 7).

Типография «Скиф», г. Качканар, ул. Свердлова, 7а.
Тел. 8-900-21-618-91. ИНН 6615072772880. Заказ 445 от 10.07.2023. т. 200 экз.

2. Опубликовать на официальном сайте Качканарского городского округа KGO66.RU в сети интернет:

1) Положение об информационной безопасности (защите информации) Администрации Качканарского городского округа Свердловской области (Приложение 1);

2) Инструкцию пользователя Администрации Качканарского городского округа Свердловской области (Приложение 6).

3. Ознакомить сотрудников Администрации Качканарского городского округа Свердловской области с:

1) Положением об информационной безопасности (защите информации) Администрации Качканарского городского округа Свердловской области (Приложение 1);

2) Инструкцией пользователя Администрации Качканарского городского округа Свердловской области (Приложение 6).

4. Назначить ответственным за организацию работы по информационной безопасности (защите информации) начальника отдела по организационной работе Администрации Качканарского городского округа Свердловской области.

5. Признать утратившим силу распоряжение Администрации Качканарского городского округа от 21.01.2010 № 2 «О защите информации в Администрации Качканарского городского округа».

6. Контроль за исполнением настоящего распоряжения возлагаю на заместителя главы Качканарского городского округа по социальным вопросам Качканарского городского округа Свердловской области.

Глава городского округа А.А. Ярославцев

Приложение 1.

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

Положение
об информационной безопасности (защите информации) Администрации Качканарского городского округа Свердловской области

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об информационной безопасности (защите информации) Администрации Качканарского городского округа Свердловской области (далее - Положение, Организация) разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- «ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (утвержден и введен в действие Приказом Росстандарта от 28.01.2014 № 3-ст);

- «ГОСТ Р 56545-2015. Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» (утвержден и введен в действие Приказом Росстандарта от 19.08.2015 № 1180-ст);

- «ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят и введен в действие Постановлением Госстандарта Российской Федерации от 09.02.1995 № 49);

- «ГОСТ Р 56938-2016. Национальный стандарт Российской Федерации. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» (утвержден и введен в действие Приказом Росстандарта от 01.06.2016 N 457-ст);

- «ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» (утв. Приказом Ростехрегулирования от 27.12.2007 № 513-ст);

- «ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» (утвержден и введен в действие Приказом Росстандарта от 01.12.2011 № 683-ст);

- и иными нормами действующего законодательства Российской Федерации.

1.2. Положение обязательно к исполнению всеми работниками Организации.

1.3. Положение подлежит применению по месту нахождения учреждения - адрес: Свердловская область, г.Качканар, ул.Сверлова, д. 8.

1.4. Сокращения Положения:

- ИС - информационные системы;
- СВТ - средства вычислительной техники;
- НСД - несанкционированный доступ;
- КСЗ - комплекс средств защиты;
- ЗИ - защита информации;
- ВВС - виртуальные вычислительные системы;
- ПРД - правила разграничения доступа;
- ГРИИБ - группа реагирования на инциденты информационной безопасности.

1.5. Подразделением, отвечающим за реализацию настоящего Положения, является отдел по организационной работе Администрации Качканарского городского округа Свердловской области (далее - Служба).

1.6. Информационная безопасность обеспечивается реализацией следующих мер:

1.6.1. Выполнение технических требований.

1.6.2. Идентификация уязвимостей.

1.6.3. Защита при использовании технологий виртуализации.

1.6.4. Применение системы менеджмента инцидентов информационной безопасности.

1.6.5. Создание структурных подразделений, обеспечивающих информационную безопасность.

1.6.6. Обучение работников Организации приемам информационной безопасности. Требование от работников их выполнения.

1.6.7. Использование КСЗ.

1.6.8. Мониторинг и проверка эксплуатации комплекса программных и технических средств и услуг.

1.6.9. Подготовка предложений по финансированию мероприятий по защите информации.

1.6.10. Оборудование помещений, предназначенных для размещения средств обработки информации ИС, системами инженерно-технического обеспечения (вентиляции, теплоснабжения, кондиционирования, охраны, сигнализации, пожаротушения, энергообеспечения) в соответствии с требованиями по защите информации.

1.6.11. Организация технического обслуживания и ремонта средств вычислительной техники, предназначенных для обработки информации ограниченного доступа, с учетом требований по защите информации.

II. ЗАЩИТА ИНФОРМАЦИИ

2.1. Защита информации в Организации представляет собой принятие правовых, организационных и технических мер, направленных:

1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2.2. Организация как обладатель информации и/или оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязана обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации;

8) документирование доказательств неправомерного доступа к компьютерной информации, создания, использования и распространения вредоносных компьютерных программ, нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, нарушения правил защиты информации, незаконной деятельности в области защиты информации, разглашения информации с ограниченным доступом, воспрепятствования уверенной работе сайтов в сети Интернет, нарушения требований законодательства о хранении документов и информации, содержащейся в информационных системах;

9) сопровождение исполнения заключенных Организацией договоров на закупку товаров, работ и услуг по темам развития и обеспечения защиты информации;

10) ведение реестра приобретенных средств защиты информации;

11) проведение служебных расследований по фактам нарушения требований защиты информации;

12) взаимодействие с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации по вопросам защиты информации в Организации;

13) обеспечение устойчивости и адаптивности ИС;

14) финансирование мероприятий по защите информации в Организации;

15) закупка товаров, работ и услуг, направленных на обеспечение защиты информации.

2.3. Информация, полученная работниками Организации при исполнении ими профессиональных обязанностей или самой Организацией при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица

федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

2.4. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

2.5. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия Организации или лица, предоставившего такую информацию о себе.

2.6. Порядок доступа к персональным данным граждан устанавливается Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных".

2.7. Документирование информации осуществляется в соответствии с установленными правилами делопроизводства.

2.8. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

2.9. Защита государственной тайны, коммерческой тайны, конфиденциальной информации обеспечивается в соответствии с федеральным законодательством и принятыми локальными нормативно-правовыми актами.

III. ВЫПОЛНЕНИЕ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ

3.1. Защищенность от НСД к информации при ее обработке СВТ характеризуется тем, что только надлежащим образом уполномоченные лица или процессы, инициированные ими, будут иметь доступ к ознакомлению, созданию, изменению или уничтожению информации.

3.2. Защищенность обеспечивается выполнением трех групп требований к средствам защиты, реализуемым в СВТ:

а) требования к разграничению доступа, предусматривающие то, что СВТ должны поддерживать непротиворечивые, однозначно определенные правила разграничения доступа;

б) требования к учету, предусматривающие то, что СВТ должны поддерживать регистрацию событий, имеющих отношение к защищенности информации;

в) требования к гарантиям, предусматривающие необходимость наличия в составе СВТ технических и программных механизмов, позволяющих получить гарантии того, что СВТ обеспечивают выполнение требований к разграничению доступа и к учету.

3.3. Согласование требований к техническим характеристикам объектов закупки и технических заданий в части обеспечения защиты информации на закупку Организацией товаров, работ и услуг, направленных на развитие и обеспечение функционирования ИС обязательно.

3.4. Подготовка и утверждение требований к техническим характеристикам объектов закупки и технических заданий на закупку Организацией товаров, работ и услуг, направленных на развитие и обеспечение защиты информации, выполняется отделом по организационной работе Администрации Качканарского городского округа Свердловской области.

3.5. Мониторинг и систематическая проверка эксплуатации комплекса программных и технических средств и услуг выполняется отделом по организационной работе Администрации Качканарского городского округа Свердловской области в течение всего срока их использования.

IV. ИДЕНТИФИКАЦИЯ УЯЗВИМОСТЕЙ

4.1. Для однозначной идентификации уязвимости их описание должно включать следующие

элементы:

- идентификатор уязвимости;

- наименование уязвимости;

- класс уязвимости;

- наименование программного обеспечения (ПО) и его версия.

4.2. Для анализа уязвимостей их описание должно включать:

- идентификатор типа недостатка;

- тип недостатка;

- место возникновения (проявления) уязвимости;

- способ (правило) обнаружения уязвимости;

- возможные меры по устранению уязвимости.

4.3. Дополнительная информация об уязвимости может включать:

- наименование операционной системы и тип аппаратной платформы;

- язык программирования ПО;

- служба (порт), которую(ый) используют для функционирования ПО;

- степень опасности уязвимости;

- краткое описание уязвимости;

- идентификаторы других систем описаний уязвимостей;

- дата выявления уязвимости;

- автор, опубликовавший информацию о выявленной уязвимости;

- критерии опасности уязвимости.

- описание реализуемой технологии обработки (передачи) информации;

- описание конфигурации ПО, определяемой параметрами установки;

- описание настроек ПО, при которых выявлена уязвимость;

- описание полномочий (прав доступа) к ИС, необходимых нарушителю для эксплуатации уязвимости;

- описание возможных угроз безопасности информации, реализация которых возможна при эксплуатации уязвимости;

- описание возможных последствий от эксплуатации уязвимости ИС;

- наименование организации, которая опубликовала информацию о выявленной уязвимости;

- дата опубликования уведомления о выявленной уязвимости, а также дата устранения уязвимости разработчиком ПО;

- другие сведения.

4.4. Уязвимости ИС по области происхождения подразделяются на следующие классы:

- уязвимости кода;

- уязвимости конфигурации;

- уязвимости архитектуры;

- организационные уязвимости;

- многофакторные уязвимости.

4.5. Уязвимости ИС по типам недостатков ИС подразделяются на следующие:

- недостатки, связанные с неправильной настройкой параметров ПО;

- недостатки, связанные с неполнотой проверки вводимых (входных) данных;

- недостатки, связанные с возможностью прослеживания пути доступа к каталогам;

- недостатки, связанные с возможностью перехода по ссылкам;

- недостатки, связанные с возможностью внедрения команд ОС;

- недостатки, связанные с межсайтовым скриптингом (выполнением сценариев);

- недостатки, связанные с внедрением интерпретируемых операторов языков программирования или разметки;

- недостатки, связанные с внедрением произвольного кода;

- недостатки, связанные с переполнением буфера памяти;

- недостатки, связанные с неконтролируемой форматной строкой;

- недостатки, связанные с вычислениями;

- недостатки, приводящие к утечке/раскрытию информации ограниченного доступа;

- недостатки, связанные с управлением полномочиями (учетными данными);

- недостатки, связанные с управлением разрешениями, привилегиями и доступом;

- недостатки, связанные с аутентификацией;

- недостатки, связанные с криптографическими преобразованиями (недостатки шифрования);

- недостатки, связанные с подменой межсайтовых запросов;

- недостатки, приводящие к "состоянию гонки";

- недостатки, связанные с управлением ресурсами;

- иные типы недостатков.

4.6. Уязвимости ИС по месту возникновения (проявления) подразделяются на следующие:

- уязвимости в общесистемном (общем) программном обеспечении.

- уязвимости в прикладном программном обеспечении.

- уязвимости в специальном программном обеспечении.

- уязвимости в технических средствах.

- уязвимости в портативных технических средствах.

- уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании.

- уязвимости в средствах защиты информации.

V. ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

5.1. Виртуализацию проводят в отношении:

- программ;

- вычислительных систем;

- систем хранения данных;

- вычислительных сетей;

- памяти;

- данных.

5.2. К основным объектам защиты при использовании технологий виртуализации относят:

- средства создания и управления виртуальной инфраструктурой (гипервизор I типа, гипервизор II типа, гипервизор системы хранения данных, консоль управления виртуальной инфраструктурой и др.);

- виртуальные вычислительные системы (ВВС, виртуальные сервера и др.);

- виртуальные системы хранения данных;

- виртуальные каналы передачи данных;

- отдельные виртуальные устройства обработки, хранения и передачи данных (виртуальные процессоры, виртуальные диски, виртуальную память, виртуальное активное и пассивное сетевое оборудование и др.);

- виртуальные средства защиты информации (ЗИ) и средства ЗИ, предназначенные для использования в среде виртуализации;

- периметр виртуальной инфраструктуры (задействованные при реализации технологий виртуализации центральные процессоры и их ядра, адресное пространство памяти, сетевые интерфейсы, порты подключения внешних устройств и др.).

5.3. Для защиты перечисленных объектов используют как виртуальные средства ЗИ и средства ЗИ, предназначенные для использования в среде виртуализации, являющиеся разновидностями средств ЗИ, так и другие виды средств ЗИ.

5.4. Угрозы безопасности, обусловленные использованием технологий виртуализации.

5.4.1. Использование технологий виртуализации создает предпосылки для появления угроз

безопасности, не характерных для информационных систем, построенных без использования технологий виртуализации. Общий перечень угроз, дополнительно могущих возникать при использовании технологий виртуализации, включает угрозы, описанные далее.

5.4.2. Угрозы атаки на активное и/или пассивное виртуальное и/или физическое сетевое оборудование из физической и/или виртуальной сети.

5.4.3. Данные угрозы появляются в связи с ограниченностью функциональных возможностей (наличием слабостей) активного и/или пассивного виртуального и/или физического сетевого оборудования, входящего в состав виртуальной инфраструктуры. На реализацию данных угроз прямое влияние оказывают: наличие уязвимостей программного и/или микропрограммного обеспечения указанного оборудования, наличие у него фиксированного сетевого адреса и другие параметры его настройки, возможность изменения алгоритма работы программного обеспечения (ПО) сетевого оборудования вредоносными программами.

5.4.4. Угрозы атаки на виртуальные каналы передачи. Данные угрозы связаны со слабостями технологий виртуализации, с помощью которых строят виртуальные каналы передачи данных (сетевых технологий виртуализации). Некорректное использование сетевых технологий виртуализации может обеспечивать возможность несанкционированного перехвата трафика сетевых узлов, недоступных с помощью других сетевых технологий.

5.5. Угрозы атаки на гипервизор из виртуальной машины и/или физической сети.

5.5.1. Слабость гипервизора, а также слабость программных средств и ограниченность функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности. Реализация данных угроз приводит к недоступности всей (если гипервизор один) или части (если используют несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры.

5.5.2. Наличие у гипервизоров сетевых программных интерфейсов, предназначенных для удаленного управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами, что позволяет злоумышленнику удаленно осуществлять несанкционированный доступ (НСД) к этим устройствам с помощью сетевых технологий из виртуальной и/или физической сети. Возможный ущерб может быть связан с доступностью данных виртуальных устройств.

5.5.3. Наличие у создаваемых ВВС сетевых адресов и возможность осуществления ими сетевого взаимодействия с другими субъектами как с помощью стандартных сетевых технологий, так и с помощью сетевых технологий виртуализации.

5.5.4. Атака на систему хранения данных из виртуальной и/или физической сети. Угрозы данного типа реализуются за счет слабостей применяемых технологий распределения информации по различным виртуальным устройствам хранения данных и/или виртуальным дискам, а также слабостей технологии единого виртуального дискового пространства. Указанные слабости связаны со сложностью алгоритмов обеспечения согласованности при реализации процессов распределения информации в рамках единого виртуального дискового пространства, а также взаимодействия с виртуальными и физическими каналами передачи данных для обеспечения работы в рамках одного дискового пространства.

5.5.5. Выход процесса за пределы виртуальной машины. Данная угроза связана с наличием слабостей ПО гипервизора, реализующего функцию изолированной программной среды для функционирующих в ней программ. В случае запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора, последний, как и запущенные в нем средства защиты, не способен выполнять функции безопасности в отношении программ, функционирующих в собственном гипервизоре.

5.5.6. Несанкционированный доступ к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение. Данная угроза связана с наличием слабостей ПО гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения программного кода не только защищаемой информации и обрабатывающих ее программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от НСД со стороны вредоносной программы, функционирующей внутри ВВС. В случае осуществления НСД со стороны вредоносной программы, функционирующей внутри ВВС, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной ВВС, вредоносная программа может не только нарушать целостность программного кода своей и/или других ВВС, функционирующих под управлением того же гипервизора, но и изменять параметры его (их) настройки.

5.5.7. Нарушение изоляции пользовательских данных внутри виртуальной машины. Данная угроза связана с наличием слабостей ПО гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри ВВС, от НСД со стороны вредоносного ПО, функционирующего вне ВВС. В результате реализации данной угрозы может быть нарушена безопасность пользовательских данных программ, функционирующих внутри ВВС.

5.5.8. Нарушение процедуры аутентификации субъектов виртуального информационного взаимодействия. Данная угроза связана с наличием множества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между ее уровнями. Реализуемость данной угрозы напрямую зависит от качества реализации как самих протоколов, так и механизмов их взаимодействия.

5.5.9. Перехват управления гипервизором. Угроза перехвата управления гипервизором связана с наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, с возможностью НСД к данной консоли. Возможный ущерб может быть связан с нарушением безопасности информационных, программных и вычислительных ресурсов, зарезервированных и управляемых гипервизором.

5.5.10. Перехват управления средой виртуализации. Угроза перехвата управления средой виртуализации связаны с наличием у консоли управления виртуальной инфраструктурой, реализуемой в рамках одной из ВВС, а также у управляемых с ее помощью гипервизоров программных интерфейсов взаимодействия с другими программами и, как следствие, с возможностью НСД к указанному ПО уровня управления. Возможный ущерб может быть связан с нарушением безопасности информационных, программных и вычислительных ресурсов виртуальной инфраструктуры.

5.5.11. Неконтролируемый рост числа виртуальных машин. Данная угроза связана с наличием ограниченности объема дискового пространства, выделенного под виртуальную инфраструктуру и слабостями технологий контроля процесса создания ВВС, в связи с чем возможно случайное или несанкционированное преднамеренное создание множества ВВС. В результате реализации данной угрозы может быть ограничена или нарушена доступность виртуальных ресурсов для конечных пользователей облачных услуг.

5.5.12. Неконтролируемый рост числа зарезервированных вычислительных ресурсов. Данная угроза связана со слабостями ПО уровня управления виртуальной инфраструктурой, обеспечивающего выделение компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти). Реализация данной угрозы возможна за счет НСД к указанному ПО и из-за ошибок в его коде.

5.5.13. Нарушение технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин. Данная угроза связана с отсутствием в ПО

виртуализации защитных механизмов, предотвращающих НСД к образам ВВС. В результате реализации данной угрозы может быть нарушена конфиденциальность обрабатываемой с помощью данных ВВС защищаемой информации, целостность программ, установленных на ВВС, а также доступность ресурсов данных ВВС.

5.5.14. Несанкционированный доступ к хранимой в виртуальном пространстве защищаемой информации. В связи с применением множества технологий виртуализации, предназначенных для работы с данными (распределение данных внутри виртуальных и логических дисков, распределение данных между такими дисками, распределение данных между физическими и виртуальными накопителями единого дискового пространства, выделение областей дискового пространства в виде отдельных дисков и др.), практически все файлы хранятся в виде множества отдельных сегментов. Следовательно, в подавляющем большинстве случаев последовательное чтение данных с отдельно взятого носителя не позволяет нарушать конфиденциальность защищаемой информации, хранимой в системах хранения данных. В связи с этим меры по обеспечению конфиденциальности информации, хранящейся на отдельных накопителях, практически не применяют.

5.5.15. Ошибки обновления гипервизора. Данная угроза связана с зависимостью функционирования каждого виртуального устройства и каждого виртуализированного субъекта доступа, а также всей виртуальной инфраструктуры (или ее части, если используют более одного гипервизора) от работоспособности гипервизора. Некорректно обновленный гипервизор может привести к дискредитации функционирующих на его основе защитных механизмов, предотвращающих НСД к образам ВВС. Возможный ущерб может быть связан с нарушением конфиденциальности обрабатываемой с помощью данных ВВС защищаемой информации, целостности программ и доступности ресурсов данных ВВС.

Примечание. Ошибками обновления гипервизора являются:

- сбои в процессе его обновления;

- обновления, в ходе которых внедряются новые ошибки в код гипервизора;

- обновления, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования;

- другие инциденты безопасности информации, происходящие в процессе обновления гипервизора.

5.6. Особенности защиты информации при использовании технологий виртуализации.

5.6.1. Защита информации, обрабатываемой в информационной системе (ИС), построенных с использованием технологий виртуализации, обеспечивается выполнением требований к мерам ЗИ. В целом меры ЗИ аналогичны мерам, применяемым в ИС, не использующих технологию виртуализации. Далее приведены специфические меры ЗИ, дополнительно применяемые при использовании технологий виртуализации.

5.6.2. Меры ЗИ разделены на несколько групп в зависимости от объекта защиты.

5.6.3. Меры ЗИ следует выбирать с учетом угроз безопасности, особенностей использования объектов защиты и действующего законодательства в области ЗИ.

5.6.4. Мерами защиты средств создания и управления виртуальной инфраструктурой являются:

- автоматическое изменение маршрутов передачи сетевых пакетов между компонентами виртуальной инфраструктуры внутри гипервизора;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не

прошедших процедуру аутентификации;

- выявление, анализ и блокирование внутри виртуальной инфраструктуры скрытых каналов передачи информации в обход реализованных мер ЗИ или внутри разрешенных сетевых протоколов;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к консолям управления параметрами аппаратного обеспечения;

- контроль ввода (вывода) информации в/из виртуальную(ой) инфраструктуру(ы);

- контроль ввода (вывода) информации в/из ИС;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти хостовой операционной системы;

- контроль доступа субъектов доступа к средствам конфигурирования виртуального аппаратного обеспечения;

- контроль доступа субъектов доступа к средствам конфигурирования гипервизора и ВВС;

- контроль доступа субъектов доступа к средствам конфигурирования хостовой и/или гостевых операционных систем;

- контроль запуска гипервизора и ВВС на основе заданных критериев обеспечения безопасности объектов защиты (режим запуска, тип используемого носителя и т.д.);

- контроль запуска хостовой и/или гостевых операционных систем на основе заданных критериев обеспечения безопасности объектов защиты (режим запуска, тип используемого носителя и т.д.);

- контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях хостовой операционной системы, по следующим характеристикам: составу, объему и др.;

- контроль работоспособности дублирующих ключевых компонентов аппаратного обеспечения ИС;

- контроль работоспособности дублирующих ключевых компонентов виртуальной инфраструктуры;

- контроль целостности компонентов, критически важных для функционирования гипервизора и ВВС;

- контроль целостности компонентов, критически важных для функционирования хостовой и гостевых операционных систем;

- контроль целостности микропрограммного обеспечения аппаратной части ИС;

- мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения;

- обеспечение возможности наследования установленных на уровне управления прав доступа субъектов доступа к объектам доступа на уровне виртуализации и оборудования;

- обеспечение изоляции различных потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры хостовой операционной системы;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры хостовой операционной системы;

- предотвращение задержки или прерывания выполнения в виртуальной инфраструктуре процессов с высоким приоритетом со стороны процессов с низким приоритетом;

- предотвращение задержки или прерывания выполнения процессов ВВС с высоким приоритетом со стороны процессов ВВС с низким приоритетом;

- применение индивидуальных прав доступа к объектам доступа субъектов доступа для одного или совокупности компонентов виртуальной инфраструктуры;

- проверка наличия вредоносных программ в загрузочных областях машинных носителей информации, подключенных к ИС;

- проверка наличия вредоносных программ в микропрограммном обеспечении физического и виртуального аппаратного обеспечения;

- проверка наличия вредоносных программ в файлах конфигурации гипервизора и/или ВВС;

- проверка наличия вредоносных программ в файлах конфигурации хостовой и гостевых операционных системах;

- проверка наличия вредоносных программ в файлах-образах виртуализованного ПО и ВВС, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем;

- проверка оперативной памяти и файловой системы гипервизора и/или ВВС на наличие вредоносных программ;

- проверка оперативной памяти и файловой системы хостовой и/или гостевых операционных систем на наличие вредоносных программ;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в гипервизоре и/или ВВС;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в хостовой и/или гостевых операционных системах;

- регистрация и учет запуска (завершения) работы компонентов виртуальной инфраструктуры;

- регистрация входа (выхода) субъектов доступа в/из гипервизор(а) и/или ВВС;

- регистрация входа (выхода) субъектов доступа в/из хостовую(ой) и/или гостевых операционных систем;

- регистрация запуска (завершения работы) гипервизора и/или ВВС, программ и процессов в гипервизоре и/или ВВС;

- регистрация запуска (завершения работы) хостовой и/или гостевых операционных систем, программ и процессов в хостовой и/или гостевых операционных системах;

- регистрация и учет изменений в составе программной и аппаратной части ИС во время ее функционирования и/или в период ее аппаратного отключения;

- регистрация изменений правил доступа к виртуальному аппаратному обеспечению;

- регистрация изменений состава и конфигурации виртуального аппаратного обеспечения;

- регистрация изменений состава и конфигурации ВВС;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в гипервизоре и/или ВВС;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в хостовой и/или гостевых операционных системах;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в гипервизоре и/или ВВС;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в хостовой и/или гостевых операционных системах;

- резервирование пропускной способности канала связи для обеспечения стабильного взаимодействия между компонентами виртуальной инфраструктуры внутри гипервизора;

- резервное копирование защищаемой информации в гипервизоре и/или ВВС, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование защищаемой информации в хостовой и/или гостевых операционных системах, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование физического и/или виртуального дискового пространства, используемого для хранения журналов событий гипервизора и/или ВВС;

- своевременное обнаружение отказов компонентов виртуальной инфраструктуры;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- стирание остаточной информации, образующейся после удаления данных, обрабатываемых в виртуальной инфраструктуре, содержащих информацию ограниченного доступа;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в гипервизоре и/или ВВС;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в хостовой и/или гостевых операционных системах;

- стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуализованного ПО и виртуального аппаратного обеспечения;

- управление доступом к аппаратному обеспечению ИС, контроль подключения (отключения) машинных носителей информации;

- управление запуском (обращениями) компонентов ПО, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов ПО;

- управление установкой (инсталляцией) компонентов ПО, входящего в состав виртуальной инфраструктуры, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов ПО;

- установка (инсталляция) только разрешенного к использованию в виртуальной инфраструктуре ПО и/или его компонентов;

- фильтрация сетевого трафика между компонентами виртуальной инфраструктуры и внешними сетями хостовой операционной системы, в том числе сетями общего пользования;

- фильтрация сетевого трафика от/к каждой гостевой операционной системы(е).

5.6.5. Мерами защиты виртуальных вычислительных систем являются:

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти хостовой операционной системы;

- контроль доступа субъектов доступа к средствам конфигурирования гипервизора и ВВС;

- контроль доступа субъектов доступа к средствам конфигурирования хостовой и/или гостевых операционных систем;

- контроль доступа субъектов доступа к файлам-образам виртуализованного ПО и ВВС, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- контроль запуска гипервизора и ВВС на основе заданных критериев обеспечения безопасности объектов защиты (режима запуска, типа используемого носителя и т.д.);

- контроль запуска хостовой и/или гостевых операционных систем на основе заданных критериев обеспечения безопасности объектов защиты (режима запуска, типа используемого носителя и т.д.);

- контроль целостности компонентов, критически важных для функционирования гипервизора и ВВС;

- контроль целостности компонентов, критически важных для функционирования хостовой и гостевых операционных систем;

- контроль целостности файлов, содержащих настройки виртуализованного ПО и ВВС;

- контроль целостности файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- предотвращение задержки или прерывания выполнения процессов ВВС с высоким приоритетом со стороны процессов ВВС с низким приоритетом;

- проверка наличия вредоносных программ в микропрограммном обеспечении физического и виртуального аппаратного обеспечения;

- проверка наличия вредоносных программ в файлах конфигурации гипервизора и/или ВВС;

- проверка наличия вредоносных программ в файлах конфигурации хостовой и гостевых операционных системах;

- проверка наличия вредоносных программ в файлах-образах виртуализованного ПО и ВВС, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем;

- проверка оперативной памяти и файловой системы гипервизора и/или ВВС на наличие вредоносных программ;

- проверка оперативной памяти и файловой системы хостовой и/или гостевых операционных систем на наличие вредоносных программ;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в гипервизоре и/или ВВС;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в хостовой и/или гостевых операционных системах;

- регистрация входа (выхода) субъектов доступа в/из гипервизор(а) и/или ВВС;

- регистрация входа (выхода) субъектов доступа в/из хостовой и/или гостевых операционных системах (систем);

- регистрация запуска (завершения работы) гипервизора и/или ВВС, программ и процессов в гипервизоре и/или ВВС;

- регистрация запуска (завершения работы) хостовой и/или гостевых операционных систем, программ и процессов в хостовой и/или гостевых операционных системах;

- регистрация изменений прав доступа к файлам-образам виртуализованного ПО и ВВС, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- регистрация изменений правил доступа к виртуальному аппаратному обеспечению;

- регистрация изменений состава и конфигурации ВВС;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в гипервизоре и/или ВВС;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в хостовой и/или гостевых операционных системах;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в гипервизоре и/или ВВС;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в хостовой и/или гостевых операционных системах;

- резервное копирование защищаемой информации в гипервизоре и/или ВВС, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование защищаемой информации в хостовой и/или гостевых операционных системах, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- резервное копирование физического и/или виртуального дискового пространства, используемого для хранения журналов событий гипервизора и/или ВВС;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в гипервизоре и/или ВВС;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в хостовой и/или гостевых операционных системах;

- стирание остаточной информации, образующейся после удаления файлов-образов ВВС, в которых обрабатывалась информация ограниченного доступа;

- установка (инсталляция) только разрешенного к использованию в виртуальной инфраструктуре ПО и/или его компонентов;

- фильтрация сетевого трафика от/к каждой гостевой операционной системы(е);

- шифрование файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем, содержащих информацию ограниченного доступа.

5.6.6. Мерами защиты виртуальных систем хранения данных являются:

- автоматическое восстановление работоспособности системы хранения данных, подключенной к виртуальной инфраструктуре, в случае отказа одного или нескольких ее компонентов;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- контроль ввода (вывода) информации в/из систему(ы) хранения данных, входящей в состав

виртуальной инфраструктуры;

- контроль доступа субъектов доступа к средствам конфигурирования системы хранения данных, входящей в состав виртуальной инфраструктуры;

- контроль доступа субъектов доступа к файлам-образам виртуализованного ПО и ВВС, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- контроль работоспособности (изношенности) машинных носителей информации, подключенных к виртуальной инфраструктуре, переход на дублирующие при необходимости;

- контроль целостности данных, хранимых на машинных носителях информации, подключенных к виртуальной инфраструктуре;

- контроль целостности файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- обеспечение доверенных (защищенных) канала, маршрута передачи данных в/из систему(ы) хранения данных, входящую(ей) в состав виртуальной инфраструктуры;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

- проверка наличия вредоносных программ в операционной среде гипервизора системы хранения данных;

- проверка наличия вредоносных программ в файлах-образах виртуализованного ПО и ВВС, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем;

- разделение данных в зависимости от уровня конфиденциальности обрабатываемой информации между компонентами системы хранения данных, отдельными машинными носителями информации, входящими в состав виртуальной инфраструктуры, логическими дисками или между папками файлов;

- размещение системы хранения данных в защищенном сегменте информационной системы;

- регистрация изменений прав доступа к информации, хранящейся в системе хранения данных, входящей в состав виртуальной инфраструктуры;

- регистрация изменений прав доступа к файлам-образам виртуализованного ПО и ВВС, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- регистрация изменений правил доступа к виртуальному и физическому аппаратному обеспечению системы хранения данных;

- регистрация изменений состава и конфигурации виртуального и физического аппаратного обеспечения системы хранения данных;

- резервное копирование файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- управление доступом к аппаратному обеспечению системы хранения данных, контроль подключения (отключения) машинных носителей информации к/от виртуальной инфраструктуре(ы);

- шифрование файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем, содержащих информацию ограниченного доступа.

5.6.7. Мерами защиты виртуальных каналов передачи данных являются:

- автоматическое восстановление работоспособности системы хранения данных, подключенной к виртуальной инфраструктуре, в случае отказа одного или нескольких ее компонентов;

- автоматическое изменение маршрутов передачи сетевых пакетов между компонентами виртуальной инфраструктуры внутри гипервизора;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- выявление, анализ и блокирование внутри виртуальной инфраструктуры скрытых каналов передачи информации в обход реализованных мер ЗИ или внутри разрешенных сетевых протоколов;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях хостовой операционной системы, по следующим характеристикам: составу, объему и др.;

- мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения;

- обеспечение изоляции различных потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры хостовой операционной системы;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры хостовой операционной системы;

- передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией ограниченного доступа, обрабатываемой в виртуальной инфраструктуре, при обмене информацией с иными ИС;

- резервирование пропускной способности канала связи для обеспечения стабильного взаимодействия между компонентами виртуальной инфраструктуры внутри гипервизора;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- фильтрация сетевого трафика между компонентами виртуальной инфраструктуры и внешними сетями хостовой операционной системы, в том числе сетями общего пользования;

- фильтрация сетевого трафика от/к каждой гостевой операционной системы(е);

- шифрование информации ограниченного доступа, передаваемой по виртуальным и физическим каналам связи гипервизора;

- шифрование информации ограниченного доступа, передаваемой по виртуальным и физическим каналам связи хостовой операционной системы.

5.6.8. Мерами защиты виртуальных устройств обработки, хранения и передачи данных являются:

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- контроль доступа субъектов доступа к средствам конфигурирования виртуального аппаратного обеспечения;

- контроль доступа субъектов доступа к файлам-образам виртуализованного ПО и ВВС, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- контроль работоспособности дублирующих ключевых компонентов виртуальной инфраструктуры;

- контроль целостности файлов, содержащих настройки виртуализованного ПО и ВВС;

- мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения;

- обеспечение возможности наследования установленных на уровне управления прав доступа субъектов доступа к объектам доступа на уровни виртуализации и оборудования;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры хостовой операционной системы;

- применение индивидуальных прав доступа к объектам доступа субъектов доступа для одного или совокупности компонентов виртуальной инфраструктуры;

- проверка наличия вредоносных программ в микропрограммном обеспечении физического и виртуального аппаратного обеспечения;

- разделение физических ресурсов между компонентами виртуальной инфраструктуры в зависимости от уровня конфиденциальности обрабатываемой информации;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении;

- регистрация и учет запуска (завершения) работы компонентов виртуальной инфраструктуры;

- регистрация и учет изменений в составе программной и аппаратной части ИС во время ее

функционирования и/или в период ее аппаратного отключения;

- регистрация изменений правил доступа к виртуальному аппаратному обеспечению;

- регистрация изменений состава и конфигурации виртуального аппаратного обеспечения;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в гипервизоре и/или BBC;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в хостовой и/или гостевых операционных системах;

- резервное копирование защищаемой информации, хранимой на физических и виртуальных носителях информации;

- своевременное обнаружение отказов компонентов виртуальной инфраструктуры;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуализованного ПО и виртуального аппаратного обеспечения;

- управление доступом к аппаратному обеспечению ИС, контроль подключения (отключения) машинных носителей информации.

5.6.9. Мерами защиты виртуальных средств защиты информации и средств защиты информации, предназначенных для использования в среде виртуализации, являются:

- автоматическое восстановление всех функций средств ЗИ, входящих в состав ИС;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- обеспечение возможности наследования установленных на уровне управления прав доступа субъектов доступа к объектам доступа на уровни виртуализации и оборудования;

- обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами ЗИ (функциями безопасности средств ЗИ).

VI. МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Для эффективной реакции на инциденты ИБ Служба:

- разрабатывает и документирует политику менеджмента инцидентов ИБ, а также получает очевидную поддержку этой политики заинтересованными сторонами и, в особенности, высшего руководства;

- разрабатывает и в полном объеме документирует систему менеджмента инцидентов ИБ для поддержки политики менеджмента инцидентов ИБ. Формы, процедуры и инструменты поддержки обнаружения, оповещения, оценки и реагирования на инциденты ИБ, а также градации шкалы серьезности инцидентов отражаются в документации на конкретную систему - План реагирования

на инциденты ИБ;

- обновляет политику менеджмента ИБ и рисков на всех уровнях, то есть на корпоративном и для каждой системы, сервиса и сети отдельно с учетом системы менеджмента инцидентов ИБ;

- создает в Организации соответствующее структурное подразделение менеджмента инцидентов ИБ, то есть ГРИИБ, с заданными обязанностями и ответственностью персонала, способного адекватно реагировать на все известные типы инцидентов ИБ. В большинстве организаций ГРИИБ является группой, состоящей из специалистов по конкретным направлениям деятельности, например, при отражении атак вредоносной программы привлекают специалиста по инцидентам подобного типа;

- знакомит весь персонал Организации посредством инструктажей и (или) иными способами с существованием системы менеджмента инцидентов ИБ, ее преимуществами и с надлежащими способами сообщения о событиях ИБ. Проводит соответствующее обучение персонала, ответственного за управление системой менеджмента инцидентов ИБ, лиц, принимающих решения по определению того, являются ли события инцидентами, и лиц, исследующих инциденты;

- тестирует систему менеджмента инцидентов ИБ.

6.2. Применение системы менеджмента инцидентов информационной безопасности включает:

- обнаружение и оповещение о возникновении событий ИБ (человеком или автоматическими средствами);

- сбор информации, связанной с событиями ИБ, и оценка этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ;

- реагирование на инциденты ИБ:

- исключение несанкционированного доступа к информационным ресурсам;

- администрирование защиты (безопасности) информационных ресурсов;

- создание и выдача пользователям ИС ключей шифрования информации;

- проведение аттестационных испытаний объектов информатизации, обрабатывающих конфиденциальную информацию Организации;

- участие в подготовке организационно-распорядительных документов по обеспечению защиты информации;

- разграничение доступа к информационным ресурсам;

- проведение технического обслуживания и ремонт средств вычислительной техники, обрабатывающей информацию ограниченного доступа, с учетом требований по защите информации;

- немедленное реагирование на инциденты ИС;

- если инциденты ИБ находятся под контролем, выполнение менее срочных действий (например, способствующих полному восстановлению после катастрофы);

- если инциденты ИБ не находятся под контролем, выполнение "антикризисных" действий (например, вызов пожарной команды/аварийной службы/подразделения безопасности или инициирование выполнения плана непрерывности бизнеса);

- сообщить о наличии инцидентов ИБ и любые относящиеся к ним подробности персоналу Организации, а также персоналу сторонних организаций (что может включить в себя, по мере необходимости, распространение подробностей инцидента с целью дальнейшей оценки и (или) принятия решений);

- правовую экспертизу;

- надлежащую регистрацию всех действий и решений для последующего анализа;

- разрешение проблемы инцидентов.

6.3. После разрешения/закрытия инцидентов ИБ Служба организует осуществление следующих действий по анализу состояния ИБ:

- проведение дополнительной правовой экспертизы (при необходимости);

- изучение уроков, извлеченных из инцидентов ИБ;

- определение улучшений для внедрения защитных мер ИБ, полученных из уроков, извлеченных из одного или нескольких инцидентов ИБ;

- определение улучшений для системы менеджмента инцидентов ИБ в целом, учитывая уроки, извлеченные из результатов анализа качества предпринимаемого подхода (например, из анализа результативности процессов, процедур, форм отчета и (или) организации).

6.4. Процессы менеджмента инцидентов ИБ являются итеративными, с постоянным внесением улучшений с течением времени в ряд элементов ИБ. Эти улучшения предлагаются на основе данных об инцидентах ИБ и реагировании на них, а также данных о динамике тенденций. Этап "Улучшение" включает в себя:

- пересмотр имеющихся результатов анализа рисков ИБ и анализ менеджмента организации;

- улучшение системы менеджмента инцидентов ИБ и ее документации;

- инициирование улучшений в области безопасности, включая внедрение новых и (или) обновленных защитных мер ИБ.

6.5. Преимущества менеджмента объединяются в следующие группы:

6.5.1. Улучшение безопасности. Структурный процесс обнаружения, оповещения, оценки и менеджмента инцидентов и событий ИБ позволяет быстро идентифицировать любое событие или инцидент ИБ и реагировать на них, тем самым улучшая общую безопасность за счет быстрого определения и реализации правильного решения, а также обеспечивая средства предотвращения подобных инцидентов ИБ в будущем.

6.5.2. Снижение негативных воздействий на бизнес. Структурный подход к менеджменту инцидентов ИБ может способствовать снижению уровня негативных воздействий, связанных с инцидентами ИБ, на бизнес. Последствия этих воздействий могут включать в себя немедленные финансовые убытки, а также долговременные потери, возникающие от ущерба, нанесенного репутации и кредитоспособности организации.

6.5.3. Усиление внимания к предотвращению инцидентов. Использование структурного подхода к менеджменту инцидентов ИБ может способствовать усилению внимания к предотвращению инцидентов внутри организации. Анализ данных, связанных с инцидентами, позволяет определить модели и тенденции появления инцидентов, тем самым способствуя усилению внимания к предотвращению инцидентов и, следовательно, определению соответствующих действий по предотвращению возникновения инцидентов.

6.5.4. Усиление внимания к системе установления приоритетов и свидетельств. Структурный

подход к менеджменту инцидентов ИБ создает прочную основу для системы установления приоритетов при проведении расследований инцидентов ИБ.

6.5.5. Бюджет и ресурсы. Хорошо продуманный структурный подход к менеджменту инцидентов ИБ способствует обоснованию и упрощению распределения бюджетов и ресурсов внутри подразделений Организации. Выгоды самой системы менеджмента инцидентов ИБ:

- использование менее квалифицированного персонала для идентификации и фильтрации ложных сигналов тревоги;

- обеспечение лучшего руководства действиями квалифицированного персонала;

- привлечение квалифицированного персонала только для тех процессов, где требуются его навыки, и только на той стадии процесса, где его содействие необходимо.

6.5.6. Менеджмент и анализ рисков ИБ. Использование структурного подхода к менеджменту инцидентов ИБ способствует:

- сбору более качественных данных для идентификации и определения характеристик различных типов угроз и связанных с ними уязвимостей;

- предоставлению данных о частоте возникновения идентифицированных типов угроз.

Полученные данные о негативных последствиях инцидентов ИБ для бизнеса будут полезны для анализа этих последствий. Данные о частоте возникновения различных типов угроз намного повысят качество оценки угроз. Аналогично, данные об уязвимостях намного повысят качество будущих оценок уязвимостей.

Вышеупомянутые данные значительно улучшат результаты анализа менеджмента и анализа рисков ИБ.

6.5.7. Осведомленность в вопросах ИБ. Структурный подход к менеджменту инцидентов ИБ предоставляет узконаправленную информацию о программах обеспечения осведомленности в вопросах ИБ. Эта информация является источником реальных примеров, на которых можно показать, что инциденты ИБ действительно происходят именно в данной организации, а не где-либо еще. Таким образом можно продемонстрировать выгоды быстрого получения информации о решениях. Более того, подобная осведомленность в вопросах ИБ позволяет снизить вероятность ошибки, возникновения паники и (или) растерянности у людей в случае появления инцидента ИБ.

6.5.8. Входные данные для анализа политики ИБ. Информация, предоставляемая системой менеджмента инцидентов ИБ, может обеспечить ценные входные данные для анализа результативности и последующего улучшения политик ИБ (и другой документации, связанной с ИБ). Это относится к политикам и другой документации как на уровне организации, так и для отдельных систем, сервисов и сетей.

6.6. Обязательства руководства. Для принятия структурного подхода к менеджменту инцидентов ИБ жизненно необходима постоянная поддержка со стороны руководства. Персонал организации должен распознавать инциденты ИБ и знать свои действия при их возникновении, а также осознавать большие преимущества структурного подхода для организации. Однако этого может быть недостаточно при отсутствии поддержки со стороны руководства. Необходимо донести до руководства, что организация должна выполнять обязательства по обеспечению ресурсами и поддержке способности реагирования на инциденты.

6.7. Правовые и нормативные аспекты, в том числе:

- обеспечение адекватной защиты персональных данных и неприкосновенность персональной информации;

- лица, имеющие доступ к персональным данным, не должны лично знать тех людей, информация о которых изучается;

- лица с доступом к личным данным должны подписать соглашение об их неразглашении до того, как получат доступ к ним;

- персональные данные должны использоваться исключительно для тех целей, для которых они были получены, то есть для расследования инцидентов ИБ;

- соответствующее хранение записей;

- наличие защитных мер для обеспечения выполнения коммерческих договорных обязательств;

- правовые вопросы, связанные с политиками и процедурами;

- проверка на законность непризнания ответственности;

- включение в контракты со сторонним персоналом всех необходимых аспектов;

- соглашения о неразглашении конфиденциальной информации;

- исполнение требований правоприменяющих органов;

- ясность в вопросах ответственности;

- специальные нормативные требования;

- судебные преследования или внутренние дисциплинарные разбирательства. Для успешного судебного преследования или проведения дисциплинарных разбирательств внутри организации в отношении злоумышленников независимо от того, были ли эти атаки техническими или физическими, необходимо применять соответствующие меры защиты ИБ, включая доказуемо защищенные от внесения изменений журналы аудита. Для обеспечения успешного судебного преследования или проведения дисциплинарных разбирательств внутри организации в отношении злоумышленников независимо от того, были ли эти атаки техническими или физическими, необходимо собрать свидетельства для федеральных судов или других административных органов. Необходимо показать, что:

а) документация не подвергалась искажениям и является полной;

б) копии электронного свидетельства доказуемо идентичны оригиналам;

в) все системы ИТ, от которых были получены свидетельства, во время регистрации работали в штатном режиме;

- правовые аспекты, связанные с методами мониторинга;

- подготовка правил пользования информационными ресурсами и ознакомление с ними.

6.8. Эксплуатационная эффективность и качество. Эффективность эксплуатации и качество структурного подхода к менеджменту инцидентов ИБ зависит от ряда факторов, включающих в себя обязательность уведомления об инцидентах, качество уведомления, простоту использования, быстродействие и обучение. Некоторые из этих факторов связаны с обеспечением осведомленности пользователей о важности менеджмента инцидентов ИБ и их мотивированностью сообщать об инцидентах. Что касается быстродействия, то время, используемое на сообщение об инциденте ИБ, - не единственный фактор, важно также учитывать время, необходимое для обработки данных и распространения обработанной информации (особенно в случае с сигналами аварийности). Для минимизации задержек соответствующие программы обеспечения осведомленности и обучения пользователей должны дополняться

поддержкой по горячей линии, которая обеспечивается персоналом, осуществляющим менеджмент инцидентов ИБ.

6.9. Анонимность. Пользователи должны быть уверены, что информация об инцидентах ИБ, которую они сообщают, полностью защищена, а при необходимости обезличена, с тем чтобы ее невозможно было связать с их организацией или ее подразделением без их согласия. Система менеджмента инцидентов ИБ должна учитывать ситуации, когда важно обеспечить анонимность лица или организации, сообщающих о потенциальных инцидентах ИБ при особых обстоятельствах. У каждой организации должны быть положения, в которых четко разъяснялись бы важность сохранения анонимности или ее отсутствия для лиц и организаций, сообщающих о потенциальном инциденте ИБ. ГРИИБ может потребоваться дополнительная информация, не сообщенная изначально информирующим об инциденте лицом или организацией. Более того, важная информация об инциденте ИБ может быть получена от первого обнаружившего его лица.

6.10. Конфиденциальность. Во время обработки необходимо обеспечивать анонимность информации, или персонал должен подписать соглашение о конфиденциальности (неразглашении) при получении доступа к ней. Кроме того, система менеджмента инцидентов ИБ должна обеспечивать контроль за передачей сообщений об инцидентах сторонними организациями, включая СМИ, партнеров по бизнесу, потребителей, регулирующие организации и общественность.

6.11. Независимость деятельности ГРИИБ. Группа менеджмента инцидентов ИБ должна быть способна эффективно удовлетворять функциональные, финансовые, правовые и политические потребности конкретной организации и быть в состоянии соблюдать осторожность при управлении инцидентами ИБ. Деятельность группы менеджмента инцидентов ИБ должна также подвергаться независимому аудиту с целью проверки эффективности ее функционирования. Эффективным способом реализации независимости контроля является отделение цепочки сообщений о реагировании на инцидент ИБ от общего оперативного руководства и возложение на вышестоящего руководителя непосредственных обязанностей по управлению реагированием на инциденты. Финансирование работы группы, во избежание чрезмерного влияния на нее со стороны, также должно быть отдельным.

6.12. Политика менеджмента инцидентов информационной безопасности.

6.12.1. Назначение политики. Политика менеджмента инцидентов ИБ предназначена для всего персонала, имеющего авторизованный доступ к информационным системам организации и местам их расположения.

6.12.2. Лица, связанные с политикой менеджмента инцидентов информационной безопасности. Политика менеджмента инцидентов ИБ утверждается старшим должностным лицом организации с документально подтвержденными полномочиями, полученными от высшего руководства. Политика должна быть доступна для каждого сотрудника и подрядчика и доведена через инструктаж и обучение с целью обеспечения их осведомленности в области ИБ.

6.12.3. Содержание политики менеджмента инцидентов информационной безопасности.

Политика менеджмента инцидентов ИБ должна включать в себя следующие вопросы:

- значимость менеджмента инцидентов ИБ для организации, а также обязательства высшего руководства относительно поддержки менеджмента и его системы;

- общее представление об обнаружении событий ИБ, оповещении о них и сборе соответствующей информации, а также о путях использования этой информации для определения инцидентов ИБ. Это общее представление должно содержать перечень возможных событий ИБ, а также информацию о том, как сообщать о ней, что, где и кому сообщать, а также как обращаться с совершенно новыми событиями ИБ;

- общее представление об оценке инцидентов ИБ, включая перечень ответственных лиц,

необходимые для выполнения действия, уведомления об инцидентах и дальнейшие действия ответственных лиц;

- краткое изложение действий после подтверждения того, что событие ИБ является инцидентом ИБ. Эти действия представляют:

- немедленное реагирование;

- правовую экспертизу;

- передачу информации соответствующему персоналу или сторонним организациям;

- проверку, находится ли инцидент ИБ под контролем;

- дальнейшее реагирование;

- объявление "кризисной ситуации";

- определение критериев усиления реагирования на инциденты ИБ;

- определение ответственного за инцидент лица;

- ссылку на необходимость правильной регистрации всех действий для дальнейшего и непрерывного мониторинга с целью обеспечения защищенного хранения свидетельств в электронном виде на случай их востребования для судебного разбирательства или дисциплинарного расследования внутри организации;

- действия, следующие за разрешением инцидента ИБ, включая извлечение урока из инцидента и улучшение процесса, следующего за инцидентами ИБ;

- подробности места хранения документации о системе, включая процедуры хранения;

- общее представление о деятельности ГРИИБ, включающее в себя следующие вопросы:

организационную структуру ГРИИБ и весь основной персонал группы, включая лиц, ответственных:

- за краткое информирование высшего руководства об инцидентах;

- проведение расследований и другие действия персонала группы после объявления "кризисной ситуации";

- связь со сторонними организациями (при необходимости);

- положение о менеджменте ИБ, область деятельности ГРИИБ и полномочия, в рамках которых она будет ее осуществлять. Это положение должно включать в себя, как минимум, формулировку целевого назначения, определение области деятельности ГРИИБ и подробности об учредителе ГРИИБ и его полномочиях;

- формулировку целей ГРИИБ применительно к основной деятельности группы персонала. Для выполнения своих функций персонал должен участвовать в оценке инцидентов ИБ, реагировании на них и управлении ими, а также в их успешном разрешении. Для целей и назначения ГРИИБ требуется четкое и однозначное определение;

- определение сферы деятельности ГРИИБ. Обычно в сферу деятельности ГРИИБ организации входят все информационные системы, сервисы и сети организации. В некоторых случаях для организации может потребоваться сужение сферы действия ГРИИБ. При этом необходимо четко документировать, что входит и что не входит в сферу ее деятельности;

- личность учредителя ГРИИБ - старшего должностного лица (член правления, старший руководитель), который санкционирует действия ГРИИБ и устанавливает уровни полномочий, переданных ГРИИБ. Осведомленность об этом поможет всему персоналу организации понять предпосылки создания и структуру ГРИИБ, что является крайне важной информацией для формирования доверия к ГРИИБ. Следует отметить, что перед обнародованием подробностей о создании и структуре ГРИИБ необходимо проверить законность этого действия. В некоторых обстоятельствах раскрытие полномочий группы персонала может послужить причиной предъявления ей претензий по нарушению обязательств;

- общее представление о программе обеспечения осведомленности и обучения менеджменту инцидентов ИБ;

- перечень правовых и нормативных аспектов, предполагаемых к рассмотрению.

VII. СОЗДАНИЕ ГРУППЫ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Целью создания ГРИИБ является обеспечение организации соответствующим персоналом для оценки, реагирования на инциденты ИБ и извлечения уроков из них, а также необходимой координации, менеджмента, обратной связи и процесса передачи информации. Члены ГРИИБ могут участвовать в снижении физического и финансового ущерба, а также ущерба для репутации организации, связанного с инцидентами ИБ.

7.2. Состав и количество персонала, а также структура ГРИИБ должны соответствовать масштабу и структуре Организации. В организации ГРИИБ является отделом (или: внештатной группой, которая вправе привлекать сотрудников из различных подразделений Организации). ГРИИБ возглавляется одним из заместителей руководителя Организации.

7.3. Члены группы должны быть доступны для контакта так, чтобы их имена и имена лиц, их замещающих, а также подробности о контакте с ними были доступными внутри Организации. В документации системы менеджмента инцидентов ИБ должны быть четко указаны необходимые детали, включая любые документы по процедурам и формы отчетов, но не в положениях политики.

7.4. Руководитель ГРИИБ должен:

- иметь делегированные полномочия немедленного принятия решения о том, какие меры предпринять относительно инцидента;

- иметь отдельную линию для оповещения высшего руководства, которая должна быть изолирована от обычных бизнес-операций;

- обеспечивать необходимый уровень знаний и мастерства для всех членов ГРИИБ, а также поддержание этого уровня;

- поручать расследование каждого инцидента наиболее компетентному члену группы.

7.5. Руководитель ГРИИБ и члены группы обязаны и вправе предпринимать необходимые действия, адекватные инциденту ИБ. Действия, которые могут оказать неблагоприятное влияние на всю Организацию в отношении финансов или репутации, должны согласовываться с высшим руководством. О серьезных инцидентах ИБ руководитель ГРИИБ оповещает Главу Качканарского городского округа.

7.6. Процедуры общения со СМИ и ответственность за это общение также должны быть согласованы со старшим руководством, документированы и определять:

- представителя организации по работе со средствами массовой информации;

- метод взаимодействия подразделения организации с ГРИИБ.

7.7. Отношения со сторонними лицами и организациями.

7.7.1. К сторонним лицам и организациям относятся:

- сторонний вспомогательный персонал, работающий по контракту;

- ГРИИБ сторонних организаций;

- правоприменяющие организации;

- аварийные службы (например, пожарная бригада/отделение);

- соответствующие государственные организации;

- юридический персонал;

- официальные лица по связям с общественностью и (или) представителями средств массовой информации;

- партнеры по бизнесу;

- потребители;

- общественность.

7.7.2. Взаимодействие членов ГРИИБ со сторонними организациями и лицами допускается только по письменному распоряжению руководителя Организации.

7.8. Быстрое и эффективное реагирование на инциденты ИБ включает:

- получение, подготовку, тестирование технических и других средств поддержки и реагирования;

- доступ к актуальным деталям активов Организации и информацию по их связям с бизнес-функциями;

- доступ к документированной стратегии обеспечения непрерывности бизнеса и соответствующим планам;

- документированные и опубликованные процессы передачи информации;

- использование электронной базы данных событий/инцидентов ИБ и технических средств для быстрого пополнения и обновления базы данных, анализа ее информации и упрощения процессов реагирования (хотя общепризнано, что иногда сделанные вручную записи также оказываются востребованными и используются организацией);

- адекватные меры по обеспечению непрерывности бизнеса для базы данных событий/инцидентов ИБ.

VIII. ОБЕСПЕЧЕНИЕ ОСВЕДОМЛЕННОСТИ И ОБУЧЕНИЕ ПЕРСОНАЛА

8.1. Осведомленность и участие всего персонала Организации очень важны для обеспечения успеха менеджмента инцидентов ИБ. Программа обеспечения осведомленности и соответствующий материал должны быть доступны для всего персонала, включая новых служащих, пользователей сторонних организаций и подрядчиков.

8.1.1. Для группы обеспечения эксплуатации, для членов ГРИИБ, для персонала,

ответственного за ИБ, специальных администраторов разрабатываются специальные программы обучения.

8.1.2. Для каждой группы, непосредственно участвующей в менеджменте инцидентов, требуются различные уровни подготовки, зависящие от типа, частоты и значимости их взаимодействия с системой менеджмента инцидентов ИБ.

8.1.3. Инструктажи по обеспечению осведомленности должны включать в себя:

- основы работы системы менеджмента инцидентов ИБ, включая сферу ее действия и технологию работ по менеджменту инцидентов и событий ИБ;

- способы оповещения о событиях и инцидентах ИБ;

- защитные меры по обеспечению конфиденциальности источников (по необходимости);

- соглашения об уровнях сервиса системы;

- уведомление о результатах - на каких условиях будут информированы источники;

- любые ограничения, налагаемые соглашениями о неразглашении;

- полномочия организации менеджмента инцидентов ИБ и ее линия оповещения;

- кто и как получает отчеты от системы менеджмента инцидентов ИБ.

8.1.4. В программы ориентирования персонала или в общие корпоративные программы обеспечения осведомленности в вопросах ИБ включаются подробности обеспечения осведомленности о менеджменте инцидентов ИБ.

8.1.5. До ввода в эксплуатацию системы менеджмента инцидентов ИБ весь соответствующий персонал должен под роспись ознакомиться с процедурами обнаружения и оповещения о событиях ИБ.

8.1.6. Подготовка персонала должна сопровождаться специальными упражнениями и тестированием членов группы обеспечения эксплуатации и ГРИИБ, а также персонала, ответственного за ИБ, и специальных администраторов.

IX. ИСПОЛЬЗОВАНИЕ КСЗ

9.1. Использование КСЗ включает:

- обнаружение события ИБ и оповещение о нем одним из сотрудников персонала/клиентом организации или автоматически (например, сигналом тревоги от межсетевого экрана);

- сбор информации о событии ИБ и проведение первичной оценки персоналом группы обеспечения эксплуатации организации с целью определения, является ли событие инцидентом ИБ или ложным сигналом тревоги;

- проведение второй оценки ГРИИБ с целью подтвердить, что событие является инцидентом ИБ и, в положительном случае, инициировать немедленное реагирование, а также необходимость правовой экспертизы и действий по передаче информации;

- анализ, проводимый ГРИИБ с целью определить, находится ли инцидент под контролем:

- в положительном случае - инициация дальнейших мер реагирования и готовности всей системы для использования в процессе анализа последствий инцидента;

- при отрицательном ответе - инициация антикризисных действий с привлечением

соответствующего персонала, например руководителя и группы обеспечения непрерывности бизнеса организации;

- расширение области действия дальнейших оценок и (или) принятия решений, проводимое в течение всего этапа по требованию;

- обеспечение надлежащей регистрации всеми причастными лицами, в особенности членами ГРИИБ, всей деятельности для дальнейшего анализа;

- обеспечение сбора и защищенного хранения свидетельств в электронном виде и постоянного мониторинга защищенного хранения этих свидетельств на случай их востребованности для судебного преследования или внутреннего дисциплинарного разбирательства;

- поддержка режима контроля изменений, включая отслеживание инцидентов ИБ и обновления отчетов по инцидентам с тем, чтобы база данных событий/инцидентов ИБ постоянно соответствовала действительности.

9.2. Вся собранная информация, касающаяся событий или инцидентов ИБ, должна храниться в базе данных событий/инцидентов ИБ, управляемой ГРИИБ. Информация, сообщаемая в течение каждого процесса, должна быть как можно более полной в любое время, чтобы обеспечить наиболее прочную основу для оценок и принятия решений, а также для предпринимаемых действий.

9.3. После обнаружения события ИБ и сообщения о нем целями последующих процессов являются:

- распределение ответственности за деятельность, связанную с менеджментом инцидентов, через соответствующую иерархию персонала вместе с оценкой и принятием решений, а также за действия с привлечением персонала как связанного, так и не связанного с обеспечением безопасности;

- обеспечение формальных процедур для каждого оповещенного лица, включая анализ и корректировку сделанного сообщения, оценку ущерба и уведомление соответствующего персонала (действия каждого лица зависят от типа и опасности инцидента);

- использование рекомендаций для тщательного документирования событий ИБ, а позднее, если событие будет отнесено к инциденту ИБ, то и для последующих действий в отношении инцидента ИБ и обновления базы данных событий/инцидентов ИБ.

9.4. По обнаружению и оповещению о событиях ИБ, оценке и принятию решений (является ли событие инцидентом ИБ), реагированию на инциденты ИБ включают в себя:

- немедленное реагирование;

- анализ с целью определения, находится ли инцидент ИБ под контролем;

- последующие реагирования;

- антикризисные действия;

- правовую экспертизу;

- передачу информации;

- комментарий по вопросам расширения сферы менеджмента инцидентов ИБ;

- регистрацию деятельности.

9.5. События ИБ могут быть обнаружены непосредственно лицом или лицами, заметившими что-либо, вызывающее беспокойство и имеющее технический, физический или процедурный характер. Обнаружение может осуществляться, например, детекторами огня/дыма или с помощью охранной сигнализации путем передачи сигналов тревоги в заранее определенные места (для осуществления человеком определенных действий). Технические события ИБ могут обнаруживаться автоматически, например это могут быть сигналы тревоги, производимые устройствами анализа записей аудита, межсетевыми экранами, системами обнаружения вторжений, антивирусными программами, в каждом случае стимулируемые заранее установленными параметрами этих устройств.

9.5.1. Независимо от причины обнаружения события ИБ лицо, непосредственно обратившее внимание на нечто необычное или оповещенное автоматическими средствами, несет ответственность за инициирование процесса обнаружения и оповещения. Этим лицом может быть любой представитель персонала организации, работающий постоянно или по контракту. Этот представитель должен следовать процедурам и использовать форму отчета о событиях ИБ, определенную системой менеджмента инцидентов ИБ, с целью привлечения внимания прежде всего группы обеспечения эксплуатации и менеджмента. Следовательно, важно, чтобы весь персонал был ознакомлен с рекомендациями, относящимися к вопросу оповещения о возможных событиях ИБ, включая формы отчета, имел доступ к ним и знал сотрудников, которых необходимо оповещать о каждом случае появления события ИБ. Необходимо, чтобы весь персонал организации был по крайней мере осведомлен о форме отчета, что способствовало бы его пониманию системы менеджмента инцидентов ИБ.

9.5.2. Обработка конкретного события ИБ зависит от того, что оно собой представляет, а также от последствий и воздействий, к которым это событие может привести. Сотрудник, информирующий о событии ИБ, должен заполнить форму отчета так, чтобы в ней было как можно больше информации, доступной ему на тот момент. При необходимости он связывается со своим руководителем.

9.5.3. При заполнении формы отчета важна не только точность содержания, но и своевременность заполнения. Не следует задерживать представление формы отчета о событии ИБ по причине уточнения ее содержания.

9.5.4. При наличии проблем или при существовании мнения о наличии проблем с установленными по умолчанию механизмами электронного оповещения (например, электронной почтой), включая случаи атаки на систему и считывание формы отчета несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть нарочные, телефон, текстовые сообщения. Такие альтернативные средства должны использоваться на ранних стадиях расследования, когда становится очевидным, что событие ИБ будет переведено в категорию инцидента ИБ, особенно такого инцидента ИБ, который может считаться значительным.

9.6. Оценка и принятие решений по событиям/инцидентам.

9.6.1. Первая оценка и предварительное решение. В группе обеспечения эксплуатации системы менеджмента инцидентов ИБ принимающее лицо должно подтвердить получение заполненной формы отчета, ввести ее в базу данных событий/инцидентов ИБ и проанализировать данную форму отчета. Далее должностное лицо должно попытаться получить любые уточнения от сообщившего лица о событии ИБ и собрать требуемую дополнительную информацию, считающуюся доступной, как от сообщившего о событии лица, так и из любого другого места. Затем представитель группы обеспечения эксплуатации должен провести оценку для определения, подходит ли это событие под категорию инцидента ИБ или является ложным. Если событие ИБ определяется как ложное, необходимо заполнить форму отчета и передать в ГРИИБ для записи в базу данных и дальнейшего анализа, а также создать копии для сообщившего о событии лица и его/ее местного руководителя.

9.6.1.1. Информация и другие свидетельства, собранные на этом этапе, могут потребоваться в

будущем для дисциплинарного или судебного разбирательства. Лицо или лица, выполняющие задачи сбора и оценки информации, должны хорошо знать требования по сбору и сохранению свидетельств.

9.6.1.2. Дополнительно к дате (датам) и времени выполнения действий необходимо полностью документировать:

- проведенные мероприятия (включая использованные средства) и их цели;

- место хранения свидетельства наличия события;

- способ архивирования свидетельства (если оно уместно);

- способ верификации свидетельства (если оно уместно);

- детали хранения материалов и последующего доступа к ним.

9.6.1.3. Если событие ИБ определено как вероятный инцидент ИБ, а сотрудник группы обеспечения эксплуатации имеет соответствующий уровень компетентности, то проводится дальнейшая оценка. В результате могут потребоваться корректирующие действия, например идентификация дополнительных "аварийных" защитных мер и обращение за помощью в их реализации к соответствующему лицу. Событие ИБ может быть определено как инцидент ИБ, причем значительный (по шкале серьезности, принятой в организации), в этом случае необходимо проинформировать непосредственно руководителя ГРИИБ. Может потребоваться объявление "кризисной ситуации" и, как следствие, уведомление руководителя обеспечения непрерывности бизнеса о возможной активизации плана обеспечения непрерывности бизнеса с одновременным информированием руководителя ГРИИБ и вышестоящего руководства. Однако наиболее вероятна ситуация передачи инцидента ИБ непосредственно в ГРИИБ для дальнейшей оценки и выполнения соответствующих действий.

9.6.1.4. Каким бы ни был следующий шаг, сотрудник группы обеспечения эксплуатации должен заполнить форму отчета по возможности наиболее подробно. Отчет должен содержать информацию в описательном виде и, насколько это возможно, характеризовать:

- что представляет собой инцидент ИБ;

- что явилось его причиной, чем или кем он был вызван;

- на что он влияет или может повлиять;

- реальное или потенциальное воздействие инцидента ИБ на бизнес организации;

- указание на вероятную значительность или незначительность инцидента ИБ (по шкале серьезности, принятой в организации);

- как инцидент ИБ обрабатывался до этого времени.

9.6.1.5. При рассмотрении потенциального или фактического негативного воздействия инцидента на бизнес организации в результате несанкционированного раскрытия информации, несанкционированной модификации информации, отказа от имеющейся информации, недоступности информации и (или) сервиса, уничтожения информации и (или) сервиса в первую очередь необходимо определить, какое из перечисленных ниже последствий будет иметь инцидент ИБ.

Примерами последствий ИБ являются:

- финансовые убытки/прерывание бизнес-операций;

- ущерб коммерческим и экономическим интересам;

- ущерб информации, содержащей персональные данные;

- нарушение правовых и нормативных обязательств;

- сбои операций по менеджменту и бизнес-операций;

- утрата престижа организации.

9.6.1.6. Для категорий, отнесенных к инциденту ИБ, должны использоваться соответствующие рекомендации по категорированию потенциальных или фактических воздействий для внесения их в отчет по инцидентам ИБ.

9.6.1.7. Если инцидент ИБ был разрешен, то отчет должен содержать детали предпринятых защитных мер и извлеченных уроков (например, защитные меры, которые должны быть приняты для предотвращения повторного появления подобных инцидентов ИБ).

9.6.1.8. После наиболее подробного, по мере возможности, заполнения форма отчета должна быть представлена в ГРИИБ для ввода в базу данных инцидентов и событий ИБ и анализа в будущем.

9.6.1.9. Если расследование проводится больше недели, то должен быть составлен промежуточный отчет.

9.6.1.10. Важно, чтобы сотрудник группы обеспечения эксплуатации, оценивающий инцидент ИБ, основываясь на руководстве, содержащемся в документации системы менеджмента инцидентов ИБ, был осведомлен о том:

- когда и кому необходимо направлять материалы об инциденте;

- что при осуществлении всех действий, выполняемых группой обеспечения эксплуатации, необходимо выполнять документированные процедуры контроля изменений.

9.6.1.11. При наличии проблем или мнения о том, что существуют проблемы с установленными по умолчанию механизмами электронного оповещения (например электронной почтой), включая случаи атаки на информационную систему и считывание несанкционированными лицами формы отчета об инцидентах ИБ, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть: телефон, текстовые сообщения, а также курьеры. Такие альтернативные средства должны использоваться на ранних стадиях расследования, когда становится очевидным, что событие ИБ будет переведено в категорию инцидента ИБ, особенно такого инцидента ИБ, который может считаться "значительным".

9.6.2. Вторая оценка и подтверждение инцидента информационной безопасности. Вторая оценка и подтверждение инцидента ИБ или какое-либо другое решение относительно того, надо ли отнести событие ИБ к инциденту ИБ, должны входить в обязанности ГРИИБ. Принимающий отчеты сотрудник ГРИИБ должен:

- подтвердить получение формы отчета, заполненной по возможности наиболее подробно, группой обеспечения эксплуатации;

- ввести эту форму в базу данных событий/инцидентов ИБ;

- обратиться за уточнениями к группе обеспечения эксплуатации;

- проанализировать содержание отчетной формы;

- собрать дополнительную необходимую информацию о событии ИБ (если существует) от группы обеспечения эксплуатации, лица, заполнившего отчетную форму, или из какого-либо иного источника.

9.6.2.1. Если все еще остается какая-либо неопределенность относительно аутентичности инцидента ИБ или полноты полученной информации, то сотрудник ГРИИБ должен провести вторую оценку для определения реальности или ложности инцидента ИБ. Если инцидент ИБ определен как ложный, необходимо заполнить отчет о событии ИБ, добавить его в базу данных событий/инцидентов ИБ и передать руководителю ГРИИБ. Копии отчета необходимо передать группе обеспечения эксплуатации, лицу, сообщившему о событии, и его/ее местному руководителю.

9.6.2.2. Если инцидент ИБ определяется как реальный, то сотрудник ГРИИБ, при необходимости привлекая коллег, должен провести дальнейшую оценку. Целью оценки является максимально быстрое подтверждение:

- того, что представляет собой инцидент ИБ, что явилось его причиной, чем или кем был вызван, на что повлиял или мог повлиять, воздействие или потенциальное воздействие инцидента ИБ на бизнес организации, указание на вероятную значительность/незначительность инцидента (по шкале серьезности инцидентов, принятой в организации);

- предумышленной технической атаки нарушителя на некоторую информационную систему, сервис и (или) сеть, например:

глубины проникновения нарушителя в систему, сервис и (или) сеть и степень контроля, которой он обладает;

данных об информации, к которой получил доступ нарушитель, были ли они скопированы, изменены или удалены;

о том, какое программное обеспечение было скопировано, изменено или разрушено нарушителем;

в отношении предумышленной физической атаки нарушителя на любую информационную систему аппаратной части, сервиса и (или) на сеть и (или) на физическое месторасположение, например:

масштаба прямых и косвенных последствий нанесенного физического ущерба (при отсутствии физической защиты доступа);

прямых и косвенных последствий в отношении инцидентов ИБ, косвенно созданных действиями нарушителя (например, стал ли физический доступ возможным по причине пожара, является ли уязвимость информационной системы следствием неправильного функционирования программного обеспечения, линии связи или ошибки оператора);

- используемого до настоящего времени способа обработки инцидента ИБ.

9.6.2.3. При анализе потенциального или реального негативного воздействия инцидента ИБ на бизнес организации вследствие несанкционированного раскрытия информации, несанкционированной модификации информации, отказа от имеющейся информации, недоступности информации и (или) сервиса, разрушения информации и (или) сервиса необходимо подтвердить, какие последствия имели место вследствие данного инцидента. Примерами категорий последствий являются:

- финансовые убытки/разрушение бизнес-операций;

- ущерб коммерческим и экономическим интересам;

- ущерб для информации, содержащей персональные данные;

- нарушение правовых и нормативных обязательств;

- ущерб для менеджмента и бизнес-операций;

- утрата престижа организации.

9.6.2.4. Для отнесения потенциальных или фактических воздействий к той или иной категории необходимо использовать соответствующие рекомендации, которые относили бы их к инциденту ИБ и вносились в отчет по инцидентам ИБ.

9.7. Реагирование на инциденты.

9.7.1. Немедленное реагирование.

9.7.1.1. В большинстве случаев после подтверждения инцидента член ГРИИБ выполняет действия по немедленному реагированию относительно инцидента ИБ, регистрации подробностей в форме отчета об инциденте ИБ, введению в базу данных событий/инцидентов ИБ и уведомлению сотрудников организации о требуемых действиях на инцидент ИБ. Результатом данных действий может быть принятие аварийных защитных мер (например, отключение атакованной информационной системы, сервиса и (или) сети по предварительному соглашению с соответствующим руководством ИТ-подразделения и (или) бизнес-руководством) и (или) определение дополнительных постоянных защитных мер и уведомление сотрудников организации о принятии этих мер. Если аварийные защитные меры не применены, то нужно определить значительность инцидента ИБ по оценочной шкале, принятой в организации, и если инцидент ИБ достаточно значителен, то об этом необходимо непосредственно уведомить соответствующее вышестоящее руководство. Если очевидна необходимость объявления кризисной ситуации, руководитель, отвечающий за обеспечение непрерывности бизнеса, должен быть оповещен о возможной активизации плана обеспечения непрерывности бизнеса, причем необходимо проинформировать руководителя ГРИИБ и вышестоящее руководство.

9.7.1.2. Примерные действия по реагированию. Примером действий по немедленному реагированию в случае преднамеренной атаки на информационную систему, сервис и (или) сеть может быть то, что они остаются подключенными к Интернету и другим сетям с целью:

- обеспечения правильного функционирования критически важных бизнес-приложений;

- сбора наиболее полной информации о нарушителе при условии, если он не знает, что находится под наблюдением.

Однако при принятии решения по реагированию нужно учитывать следующие факторы:

- нарушитель может почувствовать, что находится под наблюдением, и предпринять действия, наносящие дальнейший ущерб атакованной системе, сервису и (или) сети и данным;

- нарушитель может разрушить информацию, которая способствует его отслеживанию.

9.7.1.2.1. Предотвращение повторного проявления инцидента обычно является более приоритетной задачей. В некоторых случаях необходимо учитывать то, что нарушитель выявил слабое место, которое должно быть устранено, а выгоды от выявления нарушителя не оправдывают затраченных на это усилий. Это особенно справедливо, если нарушитель на самом деле не является злоумышленником и не нанес большого или вообще не причинил никакого ущерба.

9.7.1.2.2. Что касается других инцидентов ИБ, кроме преднамеренной атаки, то их источник должен быть идентифицирован. Может потребоваться отключение информационной системы, сервиса и (или) сети или изоляция соответствующих их частей после получения предварительного согласия соответствующего руководства ИТ и (или) бизнес-руководителя на время внедрения защитных мер. Для этого может потребоваться больше времени, если уязвимое место для информационной системы, сервиса и (или) для сети окажется существенным или критически важным.

9.7.1.2.3. Другим действием по реагированию может быть активизация методов наблюдения. Это действие должно осуществляться на основе процедур, документированных для системы менеджмента инцидентов ИБ.

9.7.1.2.4. Информация, которая могла быть повреждена в результате инцидента ИБ, должна быть проверена членом ГРИИБ по резервным записям на предмет изменения, стирания или модификации информации. Может возникнуть необходимость проверки целостности журналов регистрации, поскольку злонамеренный нарушитель может подделать их с целью сокрытия следов проникновения.

9.7.1.3. Обновление информации об инцидентах. Независимо от последующих действий, сотрудник ГРИИБ должен обновить отчет об инциденте ИБ с максимальной детализацией, добавить его в базу данных событий/инцидентов ИБ, оповестив об этом руководителя ГРИИБ и (при необходимости) других лиц. Обновляют следующую информацию:

- о том, что представляет собой инцидент ИБ;

- о том, что явилось причиной, чем или кем он был вызван;

- на что воздействует или мог воздействовать;

- о фактическом или потенциальном воздействии инцидента ИБ на бизнес организации;

- об изменениях в указании на вероятную значительность или незначительность инцидента ИБ (по шкале серьезности, принятой в организации);

- о том, как он обрабатывался до этого времени.

9.7.1.3.1. Если инцидент ИБ разрешен, то отчет должен содержать подробности предпринятых защитных мер и извлеченных уроков (например, дополнительные защитные меры, которые следует предпринять для предотвращения повторного появления данного инцидента ИБ или подобных ему инцидентов ИБ). Обновленный отчет следует добавлять в базу данных событий/инцидентов ИБ и уведомлять руководителя ГРИИБ и других лиц по их требованию.

9.7.1.3.2. ГРИИБ отвечает за обеспечение безопасного хранения информации, относящейся к данному инциденту ИБ, с целью возможного проведения дальнейшей экспертизы и возможного использования судом в качестве доказательства. Например, для инцидента ИБ, ориентированного на ИТ, после первоначального обнаружения инцидента ИБ все непостоянные данные должны быть собраны до отключения пораженной системы ИТ, сервиса и (или) сети до проведения судебного расследования. Предназначенная для сбора информация содержит сведения о любых функционирующих процессах и хранится в памяти, кеше и регистрах. При этом необходимо:

- в зависимости от характера инцидента ИБ провести полное дублирование пораженной системы, сервиса и (или) сети на случай судебного разбирательства или резервное копирование журналов и важных файлов;

- собрать и проанализировать журналы соседних систем, сервисов и (или) сетей, например, маршрутизаторов и межсетевых экранов;

- всю собранную информацию хранить на носителях только для чтения;

- при выполнении дублирования на случай судебного разбирательства обеспечить присутствие не менее двух лиц для утверждения и подтверждения того, что все действия были выполнены согласно действующему нормативному законодательству;

- документировать и хранить вместе с исходными носителями спецификации и описания сервисных команд, которые используются для дублирования на случай судебного разбирательства.

9.7.1.3.3. Член ГРИИБ также является ответственным, если это возможно, во время обновления информации об инцидентах ИБ за возвращение в безопасное рабочее состояние пораженных устройств (имеющих или не имеющих отношение к ИТ) в интересах исключения атак на эти устройства.

9.7.1.4. Дополнительные действия. При определении членом ГРИИБ реальности инцидента ИБ его дополнительными действиями должны быть:

- проведение правовой экспертизы;

- информирование лиц, ответственных за передачу информации внутри организации и за ее пределами, о фактах и предложениях по информации, которую надо передать, в какой форме и кому.

9.7.1.4.1. После возможно наиболее подробного заполнения отчета об инциденте ИБ отчет вводится в базу данных событий/инцидентов ИБ и передается руководителю ГРИИБ.

9.7.1.4.2. Если время расследования превышает время, ранее согласованное внутри организации, то составляется промежуточный отчет.

9.7.1.4.3. Член ГРИИБ, оценивающий инцидент ИБ, на основании руководства, содержащегося в документации системы менеджмента инцидентов ИБ, должен знать:

- когда и кому необходимо направлять материалы;

- что при осуществлении любой деятельности ГРИИБ необходимо следовать документированным процедурам контроля за внесением изменений.

9.7.1.4.4. При наличии проблем или если считается, что существуют проблемы в отношении обычных средств связи (например, с электронной почтой), включая случаи, когда система, возможно, подвергается атаке и целесообразно сделать вывод, что инцидент ИБ является значительным и (или) была определена кризисная ситуация, то следует в первую очередь сообщить об инциденте ИБ ответственным лицам лично, по телефону или текстовым сообщением.

9.7.1.4.5. При необходимости руководитель ГРИИБ совместно с руководителем обеспечения безопасности ИБ организации и соответствующим руководителем организации (членом совета директоров) правления должны связаться со всеми отделами, которые вовлечены в инцидент ИБ как внутри организации, так и за ее пределами.

9.7.1.4.6. Для быстрой и эффективной организации связи необходимо заранее установить надежный метод передачи информации, не зависящий полностью от системы, сервиса или сети, на которые может воздействовать инцидент ИБ. Такие меры предосторожности могут включать в себя назначение резервных консультантов или представителей организации на случай отсутствия кого-либо из ее основных руководителей.

9.7.2. Контролируемость инцидента. После инициирования членом ГРИИБ немедленного реагирования соответствующей правовой экспертизы и действий по передаче информации необходимо срочно убедиться, находится ли инцидент ИБ под контролем. При необходимости член ГРИИБ может проконсультироваться с коллегами, руководителем ГРИИБ и (или) другими сотрудниками организации.

9.7.2.1. Если подтверждается, что инцидент ИБ находится под контролем, то член ГРИИБ должен перейти к другим дальнейшим необходимым действиям по реагированию, проведению правовой экспертизы и передаче информации с целью ликвидации инцидента ИБ и восстановления нормальной работы пораженной информационной системы.

9.7.2.2. Если не подтверждается, что инцидент ИБ находится под контролем, член ГРИИБ должен инициировать антикризисные действия.

9.7.3. Последующее реагирование. Определив, что инцидент ИБ находится под контролем и не является объектом антикризисной ситуации, член ГРИИБ должен определить необходимость и вероятные способы дальнейшего реагирования в отношении данного инцидента. Реагирование может включать в себя восстановление пораженных информационных систем(ы), сервисов(а) и (или) сетей(и) до нормального рабочего состояния. Затем член ГРИИБ должен занести детали в форму отчета об инциденте ИБ и базу данных событий/инцидентов ИБ, а также проинформировать об этом лиц, ответственных за завершение соответствующих действий. Подробности успешного завершения этих действий необходимо внести в форму отчета об инциденте ИБ и базу данных событий/инцидентов ИБ, а затем инцидент ИБ должен быть закрыт и соответствующий персонал должен быть проинформирован об этом.

9.7.3.1. Некоторые реагирования должны быть направлены на предотвращение повторения подобного ему инцидента ИБ. Например, если определено, что причиной инцидента ИБ является отказ аппаратурной части или программного обеспечения ИТ из-за отсутствия вставок в программу ("патчей"), то в этом случае необходимо немедленно связаться с поставщиком. Если причиной инцидента ИБ была известная уязвимость ИТ, то она должна быть устранена соответствующим обновлением защиты ИБ. Необходимо также решить любые проблемы, связанные с конфигурацией ИТ и выявленным инцидентом ИБ. Другими мерами уменьшения возможности повторения или появления такого инцидента ИБ или подобного ему инцидента могут быть изменение системных паролей и отключение неиспользуемых сервисов.

9.7.3.2. Другая область деятельности по реагированию на инцидент ИБ может включать в себя мониторинг системы, сервиса и (или) сети ИТ. Следом за оценкой инцидента ИБ может оказаться целесообразным ввести дополнительные защитные меры мониторинга для содействия в обнаружении необычных или подозрительных событий, которые могут оказаться признаками инцидентов ИБ. Такой мониторинг поможет также глубже раскрыть инцидент ИБ и идентифицировать другие системы ИТ, которые подверглись компрометации.

9.7.3.3. Может возникнуть необходимость в активизации специальных реагирований, документированных в соответствующем плане обеспечения непрерывности бизнес-процесса, которые можно применить к инцидентам ИБ как связанным, так и не связанным с ИТ. Специальные реагирования должны быть предусмотрены для всех аспектов бизнеса, связанных не только непосредственно с ИТ, но также с поддержкой ключевых функций бизнеса и последующего восстановления с помощью речевой сети связи и физических устройств.

9.7.3.4. Еще одной областью реагирования является восстановление пораженных информационных систем(ы), сервисов(а) и (или) сетей(и) до нормального рабочего состояния. Восстановление пораженных систем(ы), сервисов(а) и (или) сетей(и) до безопасного рабочего состояния может быть осуществлено применением "патчей" для известных уязвимостей или отключением скомпрометированных элементов. Если вследствие уничтожения журналов регистрации во время действия инцидента ИБ исчезает весь объем информации об инциденте ИБ, может потребоваться полная перестройка системы, сервиса и (или) сети. Также может потребоваться активизация части соответствующего плана непрерывности бизнеса.

9.7.3.5. Если инцидент ИБ, не связанный с ИТ, например, спровоцирован пожаром, наводнением или взрывом, то выполняются действия по восстановлению, документированные в соответствующем плане обеспечения непрерывности бизнеса.

9.7.4. Антикризисные действия. Может случиться так, что при определении ГРИИБ контролируется ли инцидент ИБ, группа придет к выводу, что инцидент ИБ не находится под контролем и должен обрабатываться в режиме антикризисных действий. В этом случае используется предварительно разработанный план (планы).

9.7.4.1. Лучшие варианты обработки всех возможных типов инцидентов ИБ, которые могут повлиять на доступность/разрушение и, в некоторой степени, на целостность информационной системы, должны быть определены в стратегии обеспечения непрерывности бизнеса организации. Эти варианты должны быть непосредственно связаны с приоритетами бизнеса организации и

соответствующими временными рамками восстановления бизнес-процессов и, следовательно, с максимально приемлемым временем простоя ИТ, речевой связи, персонала и размещения. В плане необходимо определить:

- предупреждающие, поддерживающие меры обеспечения непрерывности бизнеса и устойчивости к внешним изменениям;

- организационную структуру и обязанности, связанные с управлением планирования непрерывности бизнеса;

- структуру и основные положения плана (планов) обеспечения непрерывности бизнеса.

9.7.4.2. План (планы) обеспечения непрерывности бизнеса и защитные меры для поддержки активизации этого (этих) плана (планов), протестированных и признанных удовлетворительными, должны создать основу для ведения наиболее антикризисных действий, для которых они предназначены.

9.7.4.3. Другие типы возможных антикризисных действий включают в себя (но не ограничиваются) активизацией:

- средств пожаротушения и процедур эвакуации;

- средств предотвращения наводнения и процедур эвакуации;

- средств предотвращения взрыва бомбы и соответствующих процедур эвакуации;

- работы специалистов по расследованию фактов мошенничества в информационных системах;

- работы специалистов по расследованию технических атак.

9.7.5. Правовая экспертиза. Если в ходе предыдущей оценки была определена необходимость правовой экспертизы в целях доказательства значительного инцидента ИБ, правовую экспертизу проводит ГРИИБ. В целях проведения более подробной экспертизы конкретного инцидента ИБ необходимо применять следственные методы и средства, основанные на ИТ и поддерживаемые документированными процедурами, не используемые ранее в процессе менеджмента инцидентов ИБ. Такую экспертизу проводят структурным методом и определяют, что может использоваться в качестве доказательства при внутренних дисциплинарных разбирательствах или в ходе судебных процессов.

9.7.5.1. Для проведения правовой экспертизы могут использоваться технические (например, средства и методы аудита, средства восстановления свидетельств) и программные средства, защищенные служебные помещения, а также соответствующий персонал. Каждое действие правовой экспертизы должно быть полностью документировано, включая представление соответствующих фотографий, составление отчетов об анализе результатов аудита, проверку журналов восстановления данных. Квалификация лица или лиц, проводившего(их) правовую экспертизу, должна быть документирована так же, как результаты квалификационного тестирования. Необходимо также документировать любую другую информацию, способную продемонстрировать объективность и логический характер правовой экспертизы. Все записи о самих инцидентах ИБ, деятельности, связанной с правовой экспертизой этих инцидентов, и т.д., а также соответствующие носители информации должны храниться в физически защищенной среде и контролироваться соответствующими процедурами для предотвращения доступа к ним неавторизованных лиц с целью модификации записей. Средства правовой экспертизы, основанные на применении ИТ, должны точно соответствовать правовым нормам с целью исключения возможности оспаривания этого соответствия в судебном порядке и, в то же время, в них должны учитываться все текущие изменения в технологиях. В физической среде ГРИИБ необходимо создавать необходимые условия, гарантирующие неоспоримость обработки свидетельств. В любое время для обеспечения реагирования на инцидент ИБ число персонала должно быть достаточным.

9.7.5.2. Со временем, несомненно, возникнет необходимость разработки требований к анализу свидетельств в контексте многообразия инцидентов ИБ, включая мошенничество, кражу и акты вандализма. Следовательно, для содействия ГРИИБ потребуется большее число средств, основанных на ИТ, и вспомогательных процедур для раскрытия информации, скрытой в информационной системе, сервисе и (или) сети, включая информацию, которая на первый взгляд кажется стертой, зашифрованной или поврежденной. Эти средства должны учитывать все аспекты, связанные с известными типами инцидентов ИБ (разумеется, они должны быть документированы в процедурах ГРИИБ).

9.7.5.3. В современных условиях в правовую экспертизу часто включают сложные среды с сетевой структурой, в которых расследование распространяется на всю операционную среду, включая множество серверов (файловый сервер, серверы печати, связи, электронной почты и т.д.), а также средства удаленного доступа. Существует много инструментальных средств, включая средства поиска текстов, программное обеспечение формирования изображений и пакеты программ для правовой экспертизы. Главной целью процедур правовой экспертизы является сохранение свидетельств в неприкосновенности, их проверка на предмет противостояния любым оспариваниям в суде и проведение правовой экспертизы на точной копии исходных данных с тем, чтобы избежать сомнений в целостности исходных носителей в ходе аналитической работы.

9.7.5.4. Общий процесс правовой экспертизы должен охватывать следующие виды деятельности:

- обеспечение защиты целевой системы, сервиса и (или) сети в процессе проведения правовой экспертизы от превращения их в недоступные, изменения или от иной компрометации, включая введение вирусов, и обеспечение защиты от воздействий или минимальных воздействий на их нормальную работу;

- назначение приоритетов сбора доказательств, то есть рассмотрение их от наиболее до наименее изменчивых (что в значительной степени зависит от характера инцидента ИБ);

- идентификация всех необходимых файлов в предметной системе, сервисе и (или) сети, включая нормальные файлы, файлы, кажущиеся уничтоженными, но не являющиеся таковыми, файлы, защищенные паролем или иным образом, и зашифрованные файлы;

- восстановление как можно большего числа стертых файлов и других данных;

- раскрытие IP-адресов, имен хостов, сетевых маршрутов и информации Web-сайтов;

- извлечение содержимого скрытых, временных файлов и файлов подкачки, используемых как программное обеспечение операционной системы, так и как прикладное программное обеспечение;

- доступ к содержимому программного обеспечения защищенных или зашифрованных файлов (если это не запрещено законодательством);

- анализ всех возможно значимых данных, найденных в специальных (обычно недоступных) областях памяти на дисках;

- анализ времени доступа к файлу, его создания и изменения;

- анализ журналов регистрации системы/сервиса/сети и приложений;

- определение деятельности пользователей и (или) приложений в системе/сервисе/сети;

- анализ электронной почты на наличие исходной информации и ее содержания;

- проведение проверок целостности файлов с целью обнаружения файлов, содержащих "Троянского коня", и файлов, изначально отсутствовавших в системе;

- по возможности анализ физических доказательств ущерба имуществу, например отпечатков пальцев, результатов видеонаблюдения, журналов регистрации системы сигнализации, журналов регистрации доступа по пропускам и опроса свидетелей;

- обработка и хранение добытых потенциальных свидетельств так, чтобы избежать их повреждения, приведения в негодность и предотвращения просмотра конфиденциального материала несанкционированными лицами. Следует подчеркнуть, что сбор доказательств всегда должен проводиться в соответствии с правилами судопроизводства или слушания дела, для которых возможно представление данного доказательства;

- получение выводов о причинах инцидента ИБ, необходимых действиях и времени их выполнения с приведением свидетельств, включая список соответствующих файлов, включенных в приложение к главному отчету;

- обеспечение экспертной поддержки для любого дисциплинарного или правового действия (при необходимости).

Метод(ы) выполнения вышеуказанных действий должен(ны) документироваться в работе процедуры ГРИИБ.

X. ПРИМЕРЫ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРИЧИН ИХ ВОЗНИКНОВЕНИЯ

10.1. Инциденты ИБ могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами. Их последствиями могут быть такие события, как несанкционированные раскрытие или изменение информации, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение. Инциденты ИБ, о которых не было сообщено, но которые были определены как инциденты, расследовать невозможно и защитных мер для предотвращения повторного появления этих инцидентов применить нельзя. Важно заметить, что эти примеры не являются исчерпывающими.

10.2. Отказ в обслуживании. Отказ в обслуживании является обширной категорией инцидентов ИБ, имеющих одну общую черту. Подобные инциденты ИБ приводят к неспособности систем, сервисов или сетей продолжать функционирование с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям.

10.2.1. Существует два основных типа инцидентов ИБ, связанных с отказом в обслуживании, создаваемых техническими средствами: уничтожение ресурсов и истощение ресурсов. Некоторыми типичными примерами таких преднамеренных технических инцидентов ИБ "отказ в обслуживании" являются:

- зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;

- передача данных в непредусмотренном формате в систему, сервис или сеть в попытке разрушить или нарушить их нормальную работу;

- одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать их ресурсы (то есть замедление их работы, блокирование или разрушение).

10.2.2. Отказ в обслуживании в результате ошибки в конфигурации, допущенной оператором, или из-за несовместимости прикладного программного обеспечения.

10.2.3. Отказ в обслуживании инициированный намеренно с целью разрушения системы, сервиса и снижения производительности сети.

10.2.4. Многие преднамеренные технические инциденты типа "отказ в обслуживании" часто инициируются анонимно (то есть источник атаки неизвестен), поскольку злоумышленник обычно не получает информации об атакуемой сети или системе.

10.2.5. Инциденты ИБ "отказ в обслуживании", создаваемые нетехническими средствами и приводящие к утрате информации, сервиса и (или) устройств обработки информации, могут вызываться:

- нарушениями систем физической защиты, приводящими к хищениям, преднамеренному нанесению ущерба или разрушению оборудования;

- случайным нанесением ущерба аппаратуре и (или) ее местоположению от огня или воды/наводнения;

- экстремальными условиями окружающей среды, например высокой температурой (вследствие выхода из строя системы кондиционирования воздуха);

- неправильным функционированием или перегрузкой системы;

- неконтролируемыми изменениями в системе;

- неправильным функционированием программного или аппаратного обеспечения.

10.3. Сбор информации. Подобные инциденты ИБ предполагают проведение разведки с целью определения:

- наличия цели, получения представления об окружающей ее сетевой топологии и о том, с кем обычно эта цель связана обменом информации;

- потенциальных уязвимостей цели или непосредственно окружающей ее сетевой среды, которые можно использовать для атаки.

Типичными примерами атак, направленных на сбор информации техническими средствами, являются:

- сбрасывание записей DNS (системы доменных имен) для целевого домена Интернета (передача зоны DNS);

- отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;

- зондирование системы с целью идентификации (например, по контрольной сумме файлов) операционной системы хоста;

- сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов (например электронная почта, протокол FTP, сеть и т.д.) и версий программного обеспечения этих сервисов;

- сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов (горизонтальное сканирование).

10.3.1. В некоторых случаях технический сбор информации расширяется и переходит в несанкционированный доступ, если, злоумышленник при поиске уязвимости пытается получить несанкционированный доступ. Обычно это осуществляется автоматизированными средствами взлома, которые не только производят поиск уязвимости, но и автоматически пытаются использовать уязвимые системы, сервисы и (или) сети.

10.3.2. Инциденты, направленные на сбор информации, создаваемые нетехническими средствами, приводят:

- к прямому или косвенному раскрытию или модификации информации;

- хищению интеллектуальной собственности, хранимой в электронной форме;

- нарушению учета, например, при регистрации учетных записей;

- неправильному использованию информационных систем (например, с нарушением закона или политики организации).

Инциденты могут вызываться, например, следующими факторами:

- нарушениями физической защиты безопасности, приводящими к несанкционированному доступу к информации и хищению устройств хранения данных, содержащих значимые данные, например ключи шифрования;

- неудачно и (или) неправильно конфигурированными операционными системами по причине неконтролируемых изменений в системе или неправильным функционированием программного или аппаратного обеспечения, приводящим к тому, что персонал организации или посторонний персонал получает доступ к информации, не имея на это разрешения.

10.4. Несанкционированный доступ. Примеры несанкционированного доступа с помощью технических средств включают в себя:

- попытки извлечь файлы с паролями;

- атаки переполнения буфера с целью получения привилегированного (например, на уровне системного администратора) доступа к сети;

- использование уязвимостей протокола для перехвата соединения или ложного направления легитимных сетевых соединений;

- попытки расширить привилегии доступа к ресурсам или информации по сравнению с легитимно имеющимися у пользователя или администратора.

Инциденты несанкционированного доступа, создаваемые нетехническими средствами, которые приводят к прямому или косвенному раскрытию или модификации информации, нарушениям учета или неправильному использованию информационных систем, могут вызываться следующими факторами:

- разрушением устройств физической защиты с последующим несанкционированным доступом к информации;

- неудачной и (или) неправильной конфигурацией операционной системы вследствие неконтролируемых изменений в системе или неправильного функционирования программного или аппаратного обеспечения.

XI. РАЗРАБОТКА И ТЕСТИРОВАНИЕ КОМПЛЕКСА ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ, УСЛУГ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

11.1. После того как специализированная архитектура безопасности полностью документально оформлена и согласована, включая одобрение высшего руководства, должен быть разработан комплекс программных и технических средств и услуг по обеспечению безопасности, который должен быть реализован в экспериментальном режиме, тщательно протестирован, и должна быть проведена проверка его соответствия.

11.2. Общая проверка комплекса программных и технических средств и услуг на соответствие назначению должна проводиться в соответствии с документацией по стратегии тестирования, описывающей метод тестирования и позволяющей испытывать комплекс

программных и технических средств и услуг, и планом тестирования. В результате идентификации недостатков в ходе такого тестирования могут потребоваться внесение изменения и проведение любого необходимого повторного тестирования.

11.3. После того как тестирование на соответствие назначению успешно проведено и осуществлены какие-либо необходимые изменения, должна быть проведена проверка реализации на предмет соответствия документированной специализированной архитектуры безопасности необходимым мерам и средствам контроля и управления безопасностью, определенным в следующих документах:

- специализированная архитектура безопасности;

- политика сетевой безопасности;

- документы, связанные с SecOPs;

- политика (безопасности) доступа к услуге шлюза безопасности;

- план(ы) обеспечения непрерывности деятельности;

- условия обеспечения безопасности соединения (при необходимости).

11.4. Проверка соответствия комплекса программных и технических средств и услуг должна проводиться до начала фактического функционирования. Проверка комплекса программных и технических средств и услуг будет завершена, когда все недостатки идентифицированы, исправлены и признаны высшим руководством.

11.5. Проверка соответствия комплекса программных и технических средств и услуг должна включать в себя проведение тестирования безопасности по соответствующим национальным стандартам, стандартам организации (в отсутствие национальных стандартов) в соответствии с заранее разработанной стратегией тестирования безопасности и связанными с ней планами тестирования безопасности, точно определяющими, какое тестирование должно проводиться, с помощью чего, где и когда (примерный образец плана тестирования безопасности приведен в ИСО/МЭК 27033-2). Обычно тестирование должно сочетать в себе поиск уязвимостей и тестирование на проникновение. Перед началом любого такого тестирования необходимо проверить план тестирования с тем, чтобы обеспечить уверенность в проведении тестирования в полном соответствии с релевантными законодательством и инструкциями. При проведении этой проверки не следует забывать о том, что сеть может не ограничиваться одной страной, а распространяться на другие страны с различными законодательствами. После проведения тестирования в отчетах должны указываться особенности обнаруженных уязвимостей, необходимые меры по их устранению, и приоритет их принятия, а в приложении должно подтверждаться, что все согласованные меры по их устранению применены. Такие отчеты должны быть подписаны высшим руководством организации.

11.6. Когда все результаты будут признаны удовлетворительными, реализация должна быть одобрена и принята, включая одобрение высшего руководства организации.

XII. МОНИТОРИНГ И ПРОВЕРКА ЭКСПЛУАТАЦИИ КОМПЛЕКСА ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ И УСЛУГ

После начала эксплуатации должны проводиться действия по текущему мониторингу и проверке соответствия требованиям национальных стандартов, стандартов организации (при отсутствии национальных стандартов). Такие мероприятия должны проводиться ежегодно до появления новой основной версии (комплекса программных и технических средств и услуг), связанной со значительными изменениями потребностей деятельности организации, технологии, решений по обеспечению безопасности и т.д.

XIII. ОТВЕТСТВЕННОСТЬ

Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 2.

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

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

2023 г.

Оглавление

1. ВВЕДЕНИЕ

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

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

Данное Методическое руководство разработано в соответствии со следующими документами:

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

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

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

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

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

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

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

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

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

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

Цель и задачи Методического руководства:

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

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

– оперативное совершенствование системы защиты информации в Организации.

2. ТЕРМИНЫ И СОКРАЩЕНИЯ

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

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

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

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

Тип компьютерного инцидента: классификация разновидностей компьютерных инцидентов.

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

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

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

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

Тип компьютерной атаки: классификация разновидностей компьютерных атак.

3. СТРУКТУРА МЕТОДИЧЕСКОГО РУКОВОДСТВА

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

1. Обнаружение и регистрация компьютерных инцидентов:

1.1. Регистрация признаков возможного возникновения компьютерных инцидентов;

1.2. Подтверждение компьютерных инцидентов;

2. Реагирование на компьютерные инциденты:

2.1. Определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;

2.2. Локализация компьютерного инцидента;

2.3. Выявление последствий компьютерного инцидента;

2.4. Ликвидация последствий компьютерного инцидента;

2.5. Закрытие компьютерного инцидента;

2.6. Фиксация материалов, связанных с возникновением компьютерного инцидента;

2.7. Установление причин и условий возникновения компьютерного инцидента;

3. Анализ результатов деятельности по управлению компьютерными инцидентами:

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

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

3.3. Оценка результатов и эффективности реагирования на компьютерные инциденты.

4. ОБНАРУЖЕНИЕ И РЕГИСТРАЦИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

4.1. Общие положения

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

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

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

4.2. Регистрация признаков возможного возникновения компьютерных инцидентов

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

Информация об инцидентах ИБ может поступать по следующим каналам:

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

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

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

4.2.1. Регистрация признаков возможного возникновения компьютерных инцидентов автоматизированным способом

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

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

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

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

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

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

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

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

4.2.2. Регистрация признаков возможного возникновения компьютерных инцидентов неавтоматизированным способом

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

4.3. Подтверждение компьютерных инцидентов

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

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

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

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

– регистрация компьютерных инцидентов в случае их подтверждения;

– контроль выполнения этапов реагирования на компьютерные инциденты.

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

Проверка факта возникновения компьютерного инцидента предусматривает выполнение следующих процедур:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

5.1. Общие положения

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

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

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

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

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

5.2. Определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры

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

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

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

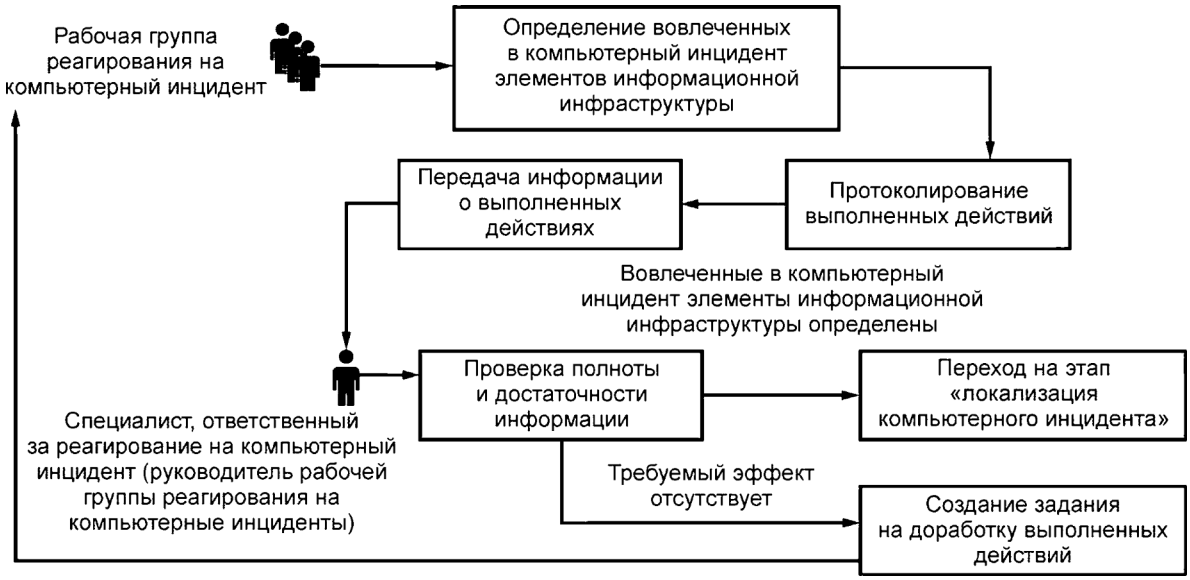

Рис. 1

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

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

1) для получения доступа к файловой системе;

2) получения доступа к журналам регистрации событий безопасности:

а) операционной системы (ОС);

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

в) прикладного программного обеспечения (ПО);

3) сканирования файловой системы с целью выявления вредоносного ПО;

4) проведения инвентаризации;

5) проведения анализа уязвимостей;

6) оценки работоспособности и производительности элементов информационной инфраструктуры;

7) получения информации из службы каталогов;

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

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

10) обнаружения компьютерных атак.

5.3. Локализация компьютерного инцидента

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

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

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

Схема организационного процесса этапа «локализация компьютерного инцидента»

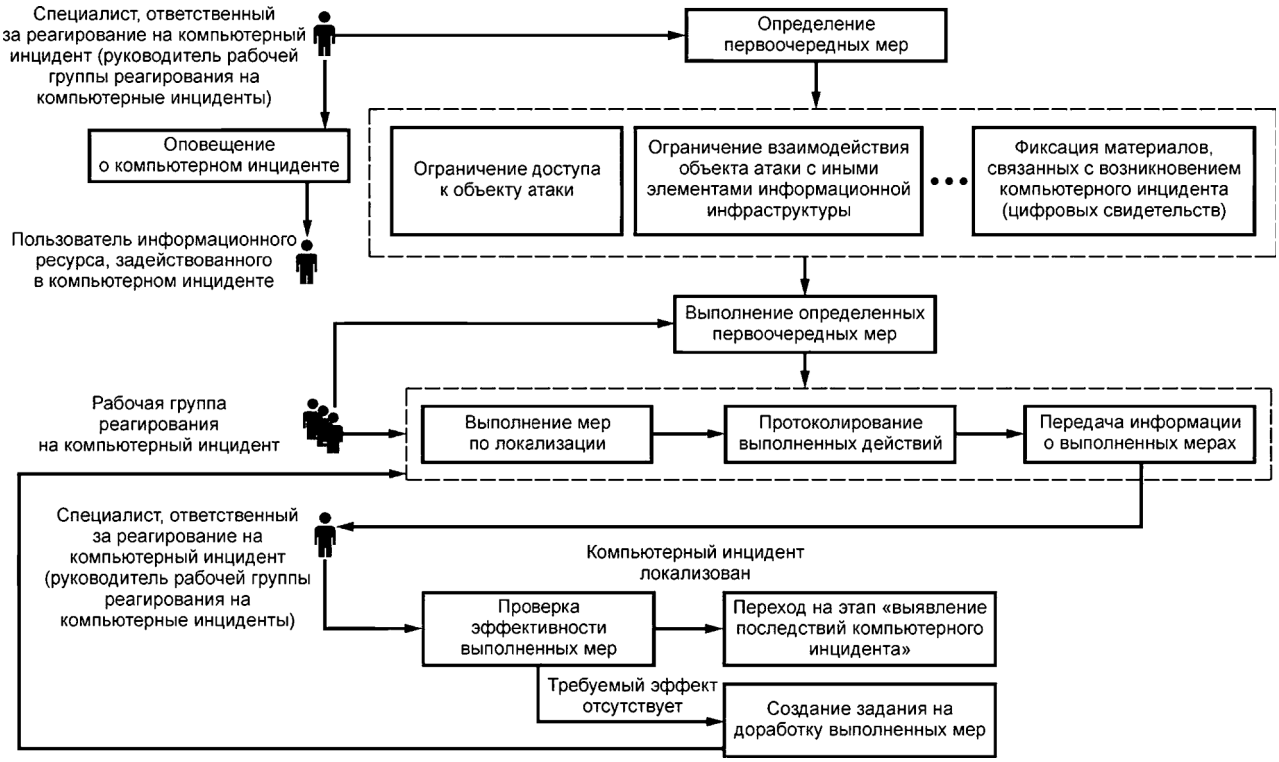

Рис. 2

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

– применение блокировок (использование межсетевого экрана).

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

– отключение (изоляция, исключение).

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

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

– выключение.

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

– изменения маршрутизации.

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

– отключение или блокирование процессов.

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

– отключение учетных записей пользователей.

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

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

5.4. Выявление последствий компьютерного инцидента

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

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

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

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

– нештатная сетевая активность элемента информационной инфраструктуры;

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

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

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

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

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

– признаки, идентифицирующие источник компьютерной атаки;

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

Схема организационного процесса этапа «выявление последствий компьютерного инцидента»

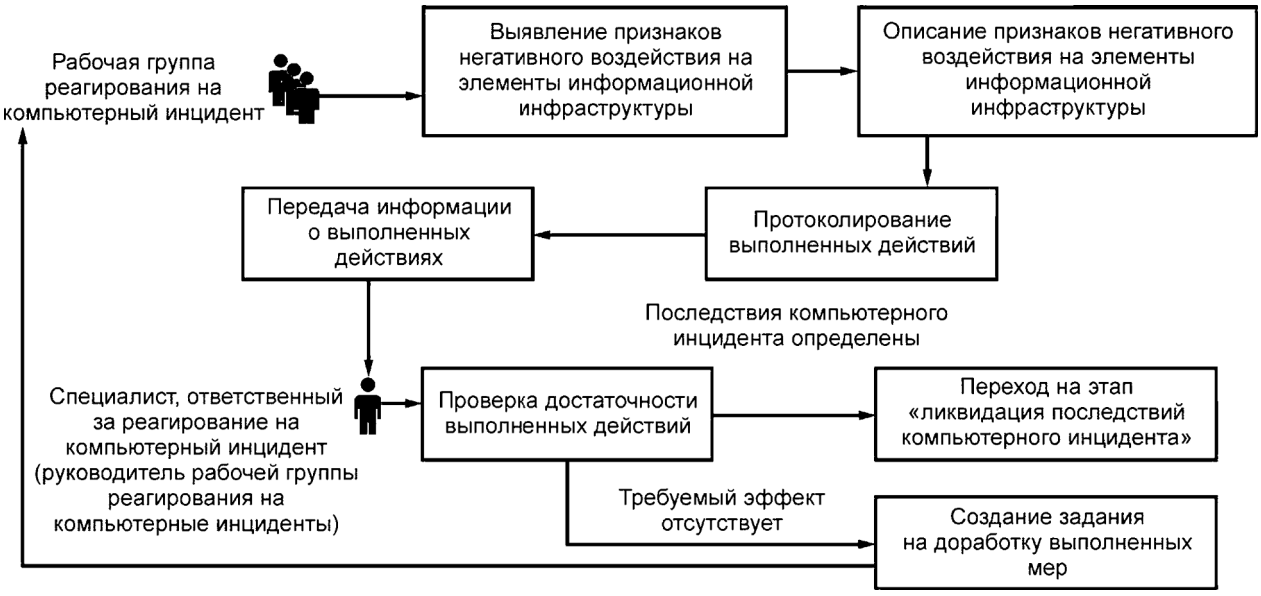

Рис. 3

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

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

5.5. Ликвидация последствий компьютерного инцидента

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

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

Схема организационного процесса этапа «ликвидация последствий компьютерного инцидента»

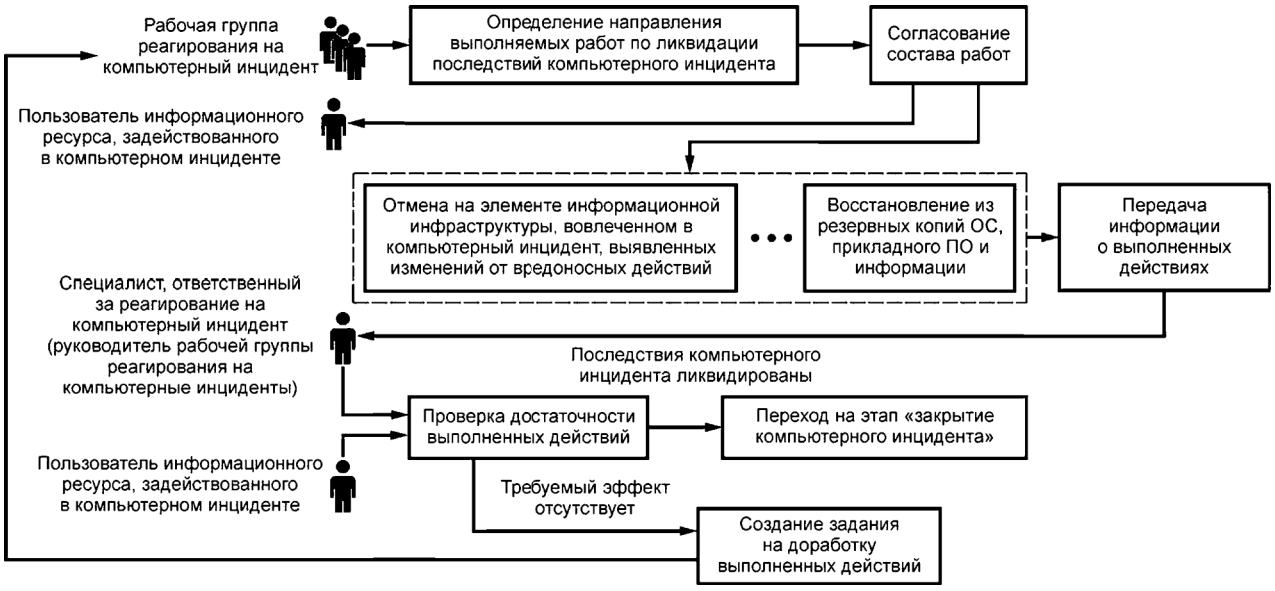

Рис. 4

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

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

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

3) смена аутентификационной информации скомпрометированных учетных записей пользователей:

а) на телекоммуникационном оборудовании;

б) средствах межсетевого экранирования;

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

4) внесение изменений в правила фильтрации межсетевых экранов;

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

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

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

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

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

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

– восстановление удаленных файлов, в том числе с использованием специальных

инструментальных средств;

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

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

– удаление вредоносного ПО;

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

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

– восстановление средств защиты информации, функционирующих в среде ОС;

– восстановление ОС в целом;

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

– настройка безопасной конфигурации ОС;

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

5.6. Закрытие компьютерного инцидента

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

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

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

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

6.1. Фиксация материалов, связанных с возникновением компьютерных инцидентов

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

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

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

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

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

– образцы вредоносного ПО;

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

– сообщения электронной почты;

– снимки состояния виртуальных машин.

6.2. Установление причин и условий возникновения компьютерных инцидентов

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

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

– анализ действий пользователей.

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

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

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

– анализ ОС элемента информационной инфраструктуры.

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

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

– информация о запущенных программных процессах;

– информация об установленных сетевых сессиях и открытых сетевых портах;

– реестр ОС (при наличии);

– информация об атрибутах объектов файловой системы;

– состав учетных записей пользователей и их прав;

– анализ защищенности.

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

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

– существующие результаты проведения мероприятий по анализу защищенности информационных ресурсов;

– сетевая конфигурация ОС, прикладного ПО;

– групповые политики безопасности ОС;

– функциональные параметры настроек прикладного ПО, служб ОС;

– состав установленных (неустановленных) актуальных обновлений безопасности

ОС, средств защиты информации и прикладного ПО;

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

– анализ сетевого трафика.

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

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

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

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

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

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

– анализ программных и информационных объектов.

Для анализа программных объектов допускается выполнять следующие процедуры:

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

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

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

7. АНАЛИЗ РЕЗУЛЬТАТОВ ДЕЯТЕЛЬНОСТИ ПО УПРАВЛЕНИЮ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

7.1. Общие положения

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

– приобретение и накопление опыта по результатам управления компьютерными инцидентами;

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

– оценка результатов и эффективности реагирования на компьютерные инциденты.

7.2. Приобретение и накопление опыта по результатам управления компьютерными инцидентами

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

Приобретение и накопление опыта по результатам управления компьютерными инцидентами позволяет:

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

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

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

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

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

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

– рекомендации по повышению защищенности информационных ресурсов от компьютерных атак;

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

7.4. Оценка результатов и эффективности реагирования на компьютерные инциденты

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

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

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

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

На рабочем совещании целесообразно обсудить следующие вопросы:

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

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

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

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

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

– среднее время проведения проверки признаков возможного возникновения компьютерных инцидентов;

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

– среднее время локализации компьютерных инцидентов;

– среднее время выявления последствий компьютерных инцидентов;

– среднее время ликвидации последствий компьютерных инцидентов;

– среднее время реагирования на компьютерные инциденты;

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

8. ОТВЕТСТВЕННОСТЬ

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

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

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

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

Таблица 1

ЖУРНАЛ
Регистрации инцидентов ИБ

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

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

Таблица 2

МИНИМАЛЬНЫЙ ПЕРЕЧЕНЬ ТИПОВ СОБЫТИЙ ИБ

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

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

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

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

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

Приложение 3.

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

Формы отчета о событиях и инцидентах информационной безопасности

Отчеты о событиях и инцидентах информационной безопасности

Рекомендации по заполнению

Назначением данной формы (формы отчета о событиях и инцидентах ИБ) является обеспечение информацией о событии информационной безопасности (далее - ИБ), а затем, если оно определено как инцидент ИБ, то и об инциденте ИБ, для определенных лиц.

Если подозревается, что событие ИБ развивается или уже свершилось, особенно событие, которое может привести к существенным потерям или ущербу собственности или репутации организации, то необходимо немедленно заполнить и передать форму отчета о событии ИБ в соответствии с процедурами, описанными в системе менеджмента инцидентов ИБ организации.

Представленная информация будет использована для инициирования соответствующего процесса оценки, которая определит, должно ли это событие категорироваться как инцидент ИБ и (в случае положительного ответа), какие корректирующие меры, необходимые для предотвращения или ограничения потерь или ущерба, следует предпринять. Поскольку процесс оценки по своему характеру является краткосрочным, то в данный момент необязательно заполнять все поля формы отчета.

Если сотрудник является членом группы обеспечения эксплуатации, анализирующим полностью/частично заполненные формы отчета, то он должен принять решение, надо ли отнести данное событие к категории инцидента ИБ. При положительном решении сотрудник должен внести в форму отчета об инциденте ИБ как можно больше информации и передать формы отчетов о событии и инциденте ИБ в группе реагирования на инциденты информационной безопасности (далее - ГРИИБ). Независимо от того, будет ли событие ИБ отнесено к категории инцидента ИБ, база данных событий/инцидентов ИБ должна быть обновлена.

Если сотрудник является сотрудником ГРИИБ, анализирующим формы отчетов о событиях и инцидентах ИБ, переданные членом группы обеспечения эксплуатации, то форма отчета об инциденте ИБ должна обновляться по ходу расследования и, соответственно, должна обновляться база данных событий/инцидентов ИБ.

При заполнении форм следует соблюдать следующие рекомендации:

- по возможности формы отчета должны заполняться и передаваться в электронном виде <1>. В случае, если существуют проблемы или считается, что существуют проблемы с принятыми по умолчанию механизмами электронного оповещения (например электронная почта), включая случаи, когда система может подвергаться атаке и формы отчета могут быть

прочитаны несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть телефон или текстовые сообщения, а также использование курьеров;

- следует представить информацию, основанную на фактах, в которой сотрудник уверен, не следует что-либо придумывать для того, чтобы заполнить все формы. Если сотрудник считает уместным включить иную информацию, которую не может подтвердить, следует указать, что это неподтвержденная информация, и причину убежденности в ее недостоверности;

- следует подробно указать, как можно связаться с сотрудником. Немедленно или спустя некоторое время может возникнуть необходимость контакта с ним для получения дальнейшей информации, касающейся Вашего отчета.

<1> Если возможно, то формы отчетов должны быть, например, на безопасной web-странице с привязкой к электронной базе данных событий инцидентов ИБ. В настоящее время основанная на бумажной технологии система является слишком медленно действующей и далеко не самой эффективной в эксплуатации.

Если позднее сотрудник обнаружит, что какая-либо представленная им информация неточна, неполна или ошибочна, то следует внести поправки в отчет и представить его повторно.

Отчет о событии информационной безопасности

Дата события
Номер события <1> _____ Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сообщающем лице

Фамилия _____ Адрес _____
Организация _____ _____
Телефон _____ Электронная почта _____
_____

Описание события ИБ

Описание события:
Что произошло
Как произошло
Почему произошло
Пораженные компоненты
Негативное воздействие на бизнес
Любые идентифицированные уязвимости

Подробности о событии ИБ

Дата и время наступления события
Дата и время обнаружения события
Дата и время сообщения о событии
Закончилось ли событие? (отметить в квадрате) Да ☐ Нет ☐
Если "да", то уточнить длительность события в днях/часах/минутах

<1> Номера событий назначаются руководителем ГРИИБ организации.

Отчет об инциденте информационной безопасности

Дата инцидента
Номер инцидента <1>: _____ Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сотруднике группы обеспечения эксплуатации

Фамилия _____ Адрес _____
Телефон _____ Электронная почта _____

Информация о сотруднике ГРИИБ

Фамилия _____ Адрес _____
Телефон _____ Электронная почта _____
_____

Описание инцидента ИБ

Дополнительное описание инцидента:
Что произошло
Как произошло
Почему произошло
Пораженные компоненты
Негативное воздействие на бизнес
Любые идентифицированные уязвимости

Подробности об инциденте ИБ

Дата и время возникновения инцидента
Дата и время обнаружения инцидента
Дата и время сообщения об инциденте
Закончился ли инцидент? (отметить в квадрате) Да ☐ Нет ☐
Если "Да", то уточнить длительность инцидента в днях/часах/минутах. Если "Нет", то уточнить, как долго он уже длится

<1> Номера инцидентов назначаются руководителем ГРИИБ организации и привязываются к номеру(ам) соответствующих событий.

Отчет об инциденте информационной безопасности

Тип инцидента ИБ

(Сделать отметку в одном из квадратов, затем заполнить ниже соответствующие поля)

Действительный ☐ Попытка ☐ Предполагаемый ☐

(Один из) Намеренная ☐ (указать типы угрозы)

- Хищение (TH) ☐
- Мошенничество (FR) ☐
- Саботаж/физический ущерб (SA) ☐
- Вредоносная программа (MC) ☐
- Хакерство/логическое проникновение (HA) ☐
- Неправильное использование ресурсов (MI) ☐
- Другой ущерб (OD) ☐

Определить:

(Один из) Случайная ☐ (указать типы угрозы)

- Отказ аппаратуры (HF) ☐
- Отказ ПО (SF) ☐
- Отказ системы связи (CF) ☐
- Пожар (HE) ☐
- Наводнение (FL) ☐
- Другие природные события (NE) ☐
- потеря значимых сервисов (LE) ☐
- недостаточное кадровое обеспечение (SS) ☐
- Другие случаи (OA) ☐

Определить:

(Один из) Ошибка ☐ (указать типы угрозы)

- Операционная ошибка (OE) ☐
- Ошибка в эксплуатации аппаратных средств (HE) ☐
- Ошибка в эксплуатации ПО (SE) ☐
- Ошибка пользователя (UE) ☐
- Ошибка проектирования (DE) ☐
- Другие случаи (включая ненамеренные ошибки) (OA) ☐

Определить:

Неизвестно ☐ (Если еще не установлен тип инцидента ИБ (намеренный, случайный, ошибка), то следует сделать отметку в квадрате "неизвестно" и, по возможности, указать тип угрозы, используя сокращения, приведенные выше)

Определить:

Отчет об инциденте информационной безопасности

Пораженные активы

Пораженные активы (при наличии) — (Дать описания активов, пораженных инцидентами ИБ или связанных с ним, включая (где требуются) серийные, лицензионные номера и номера версий)

Информация/данные _____
Аппаратные средства _____
Программное обеспечение _____
Средства связи _____
Документация _____

Негативное воздействие/влияние инцидента на бизнес

Сделать отметку в соответствующих квадратах для указанных ниже нарушений, затем в колонке "значимость" указать степень негативного воздействия на бизнес по шкале 1 - 10, используя следующие сокращения (указатели категорий): (FD) - финансовые убытки/разрушение бизнес-операций, (CE) - коммерческие и экономические интересы, (PI) - информация, содержащая персональные данные, (LR) - правовые и нормативные обязательства (это необходимо сравнить с английским оригиналом), (MO) - менеджмент и бизнес-операции, (LG) - потеря престижа (см. примеры в Приложении). Записать кодовые буквы в колонке "указатели", а если известны действительные издержки, - указать их в колонке "стоимость".

	Значимость	Указатели	Издержки
Нарушение конфиденциальности (то есть несанкционированное раскрытие)	☐		
Нарушение целостности (то есть несанкционированная модификация)	☐		
Нарушение доступности (то есть недоступность)	☐		
Нарушение неотказуемости	☐		
Уничтожение	☐		

Общие расходы на восстановление после инцидента ИБ

	Значимость	Указатели	Издержки
(Там, где возможно, необходимо указать общие расходы на восстановление после инцидента ИБ в целом по шкале 1 - 10 для "значимости" и в деньгах для "стоимости")			

Отчет об инциденте информационной безопасности

Разрешение инцидента

Дата начала расследования инцидента ИБ _____
Фамилия(ии) лица (лиц), проводившего(их) расследование инцидента _____
Дата завершения инцидента ИБ _____
Дата окончания воздействия _____
Дата завершения расследования инцидента ИБ _____
Место хранения отчета о расследовании _____

Причастные к инциденту лица/нарушители

(Один из) Лицо (PE) ☐ Легально учрежденная организация/учреждение (OI) ☐

Организованная группа (GR) ☐ Случайность (AC) ☐

Отсутствие нарушителя (NP)
Например, природные факторы, отказ оборудования, человеческий фактор ☐

Описание нарушителя
Действительная или предполагаемая мотивация

(Один из)
Криминальная/финансовая выгода (CG) ☐
Развлечение/хакерство (PH) ☐
Политика/терроризм (PT) ☐
Месть (RE) ☐
Другие мотивы (OM) ☐
Определить:

Действия, используемые для разрешения инцидента ИБ

(например, "никаких действий", "подручными средствами", "внутреннее расследование", "внешнее расследование с привлечением ...")

Действия, запланированные для разрешения инцидента

(включая возможные приведенные выше действия)

Прочие действия

(например, по-прежнему требуется проведение расследования, но другим персоналом)

Отчет об инциденте ИБ
Заключение

(Сделать отметку в одном из квадратов, является ли инцидент значительным или нет, и приложить краткое изложение обоснования этого заключения)

Значительный ☐ Незначительный ☐

(Указать любые другие заключения)

Оповещенные лица/субъекты

(Эта часть отчета заполняется соответствующим лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые действия. Обычно этим лицом является руководитель ИБ организации)

Руководитель службы ИБ ☐

Местный руководитель (уточнить, какого подразделения) ☐

Автор отчета ☐

Полиция ☐

Руководитель ГРИИБ ☐

Руководитель информационных систем ☐

Руководитель автора отчета ☐

Другие лица (например, справочная служба, отдел кадров, руководство, служба внутреннего аудита, регулятивный орган, сторонняя КСБР) ☐

Определить:

Привлеченные лица

Инициатор		Аналитик		Аналитик	
Подпись	_____	Подпись	_____	Подпись	_____
Фамилия	_____	Фамилия	_____	Фамилия	_____
Должность	_____	Должность	_____	Должность	_____
Дата	_____	Дата	_____	Дата	_____

Аналитик		Аналитик		Аналитик	
Подпись	_____	Подпись	_____	Подпись	_____
Фамилия	_____	Фамилия	_____	Фамилия	_____
Должность	_____	Должность	_____	Должность	_____
Дата	_____	Дата	_____	Дата	_____

Приложение
(справочное)

ПРИМЕРЫ ОБЩИХ РЕКОМЕНДАЦИЙ ПО ОЦЕНКЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.1. Введение

В настоящем приложении представлены примерные рекомендации по оценке и категорированию негативных последствий инцидентов ИБ, где каждая рекомендация имеет шкалу от 1 до 10 (1 - низкий, 10 - высокий). (На практике могут использоваться другие шкалы, например, с градацией от 1 до 5. Каждая организация должна использовать шкалу, наиболее подходящую для ее условий).

Перед изучением рекомендаций необходимо ознакомиться со следующими пояснениями:

- в некоторых из рекомендаций, представленных ниже, содержится примечание "Нет записи", для негативных последствий, приведенных для каждой градации инцидента ИБ (от 1 до 10) и идентичных для других шкал (например, с градацией от 1 до 5). Однако на некоторых градациях (по шкале от 1 до 10) для конкретных инцидентов ИБ считается, что из-за отсутствия больших различий в записях о последствиях инцидента ИБ на более низких градациях делать запись нецелесообразно и в этом случае делается примечание "Нет записи". Аналогично вышеизложенному, при более высоких градациях инцидента ИБ считается, что негативные последствия для них не могут быть серьезнее негативных последствий, показанных для самой высокой градации, и, следовательно, для этих градаций действует примечание "Нет записи". (Таким образом, было бы неправильно исключить указания с пометкой "Нет записи" и тем самым градацию шкалы);

- для приведенных рекомендаций, в которых применяются финансовые показатели, приведенные пределы колебаний кажутся несколько необычными. Перед использованием эти рекомендации должны быть дополнены нормированием колебаний курса валюты, наиболее подходящей для организации.

Таким образом, при использовании перечисляемых рекомендаций для расследования негативных последствий инцидента ИБ для бизнеса организации, являющихся следствием несанкционированного раскрытия информации, несанкционированного изменения информации, отказа от использованной информации, недоступности информации и (или) сервиса, уничтожения информации и (или) сервиса, в первую очередь необходимо определить, какая из нижеследующих категорий является соответствующей. Необходимо применять рекомендации по категорированию для определения реального негативного воздействия на бизнес-процессы ("значимость") с целью занесения в форму отчета об инциденте ИБ.

В.2. Финансовые убытки/нарушение хода бизнес-операций

Последствия несанкционированного раскрытия, модификации и искажения смысла переданной информации, а также недоступности и уничтожения такой информации могут привести к финансовым убыткам, например, в результате снижения цен на акции, мошенничества или разрыва контракта по причине бездействия или запоздалых действии в отношении этих последствий. Последствиями недоступности или уничтожения любой информации может быть также нарушение бизнес-процесса. На исправление ситуации и (или) восстановление бизнес-процесса после таких инцидентов ИБ потребуются время и усилия. Эти последствия в некоторых случаях могут быть значительными и должны обязательно приниматься во внимание. Для расчетов последствий необходимо, чтобы время восстановления вычислялось в единицах рабочего времени персонала и пересчитывалось в стоимость рабочего времени (финансовые затраты). Эти финансовые затраты должны быть вычислены, исходя из средней стоимости 1 чел.-мес по соответствующей градации/уровню, принятой/принятого внутри организации. Предлагается руководствоваться следующими рекомендациями:

1) результат в финансовых убытках/затратах x_1 или менее,

2) результат в финансовых убытках/затратах между x_1 и x_2;

3) результат в финансовых убытках/затратах между $x_2 + 1$ и x_3;

4) результат в финансовых убытках/затратах между $x_3 + 1$ и x_4;

5) результат в финансовых убытках/затратах между $x_4 + 1$ и x_5;

6) результат в финансовых убытках/затратах между $x_5 + 1$ и x_6;

7) результат в финансовых убытках/затратах между $x_6 + 1$ и x_7;

8) результат в финансовых убытках/затратах между $x_7 + 1$ и x_8;

9) результат в финансовых убытках/затратах более x_8;

10) организация выходит из бизнеса.

В.3. Коммерческие и экономические интересы

Коммерческая и экономическая информация нуждается в защите и оценивается с учетом ее значимости для конкурентов или по воздействию, которое оказывает ее компрометация на коммерческие интересы. Следует руководствоваться следующими рекомендациями по обеспечению защиты информации, представляющей интерес:

1) для конкурента, но не имеет коммерческой значимости (ценности);

2) для конкурента при значении параметра ценности информации, равном y_1 или менее (коммерческий оборот);

3) для конкурента при значении параметра ценности информации, находящегося в диапазоне $y_1 + 1$ и y_2 (оборот) или является причиной финансовых убытков, или потери заработка, или облегчает получение незаконной прибыли, или вызывает нарушение обязательств по поддержанию достоверности информации, поставляемой третьими сторонами;

4) для конкурента при значении параметра ценности информации, находящегося в диапазоне $y_2 + 1$ и y_3 (товарооборот);

5) для конкурента при значении параметра ценности информации, находящегося в диапазоне $y_3 + 1$ и y_4 (товарооборот);

6) для конкурента при значении параметра ценности информации более $y_4 + 1$ (оборот);

а также в случаях, когда:

7) нет записи <1>;

8) нет записи;

9) может существенно повлиять на коммерческие интересы или подорвать финансовое состояние организации;

10) нет записи.

<1> Термин "Нет записи" означает, что для этой градации последствий инцидента ИБ соответствующая запись отсутствует.

В.4. Информация, содержащая персональные данные

В местах хранения и обработки информации, содержащей персональные данные физических лиц, считают моральной и этически корректной, а при некоторых обстоятельствах юридически необходимой защиту этой информации от несанкционированного раскрытия, которое может привести в лучшем случае к созданию дискомфорта у юридического лица, а в худшем - к судебному преследованию лица, раскрывшего информацию, в соответствии с требованием законодательства в части защиты персональных данных. В равной степени необходимо, чтобы информация, содержащая персональные данные, была всегда правильной, поскольку ее несанкционированное изменение, приводящее к появлению некорректных данных, может иметь такое же последствие, что и ее несанкционированное раскрытие. Важно, чтобы информацию, содержащую персональные данные, нельзя было сделать доступной или уничтожить, поскольку это может привести к принятию неправильных решений юридическими лицами или их бездействию во время инцидента ИБ, что может иметь такое же воздействие, что и несанкционированное раскрытие или модификация информации. Следует руководствоваться следующим рекомендациями по градации нанесения ущерба информации, содержащей персональные данные:

1) нанесение (причинение) незначительного ущерба (беспокойства) конкретному лицу (гнев, расстройство, разочарование), но не нарушение правовых или нормативных требований;

2) нанесение (причинение) ущерба (беспокойства) конкретному лицу (гнев, расстройство, разочарование), но не нарушение правовых или нормативных требований;

3) нарушение правовых, нормативных или этических требований, а также опубликование намерения относительно нарушения защиты информации, приводящее к незначительному дискомфорту конкретного лица или группы лиц;

4) нарушение правовых, нормативных или этических требований, а также опубликование намерений относительно нарушения защиты информации, приводящее к чувству значительного дискомфорта для конкретного лица или к незначительному дискомфорту - группы лиц;

5) нарушение правовых, нормативных или этических требований, а также опубликованных намерений относительно защиты информации, приводящее к серьезным проблемам конкретного лица;

6) нарушение правовых, нормативных или этических требований, а также опубликование намерений относительно нарушения защиты информации, приводящее к серьезному дискомфорту для группы лиц;

7) нет записи;

8) нет записи;

9) нет записи;

10) нет записи.

B.5. Правовые и нормативные обязательства

Данные, хранимые и обрабатываемые организацией, могут подчиняться правовым и нормативным обязательствам или храниться и обрабатываться с целью обеспечения соответствия организации данным обязательствам. Несоблюдение таких обязательств, намеренное или ненамеренное, может привести к принятию правовых или административных мер к лицам, работающим в данной организации. Результатом принятия данных мер могут быть штрафы и (или) тюремное заключение. Предлагается руководствоваться следующими рекомендациями:

1) нет записи;

2) нет записи;

3) предупреждение о правоприменении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу z_1 или меньше;

4) предупреждение, гражданский иск или уголовное преступление, приводящее к финансовому ущербу/штрафу между $z_1 + 1$ и z_2;

5) предупреждение о правоприменении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу между $z_2 + 1$ и z_3 или тюремному заключению сроком до двух лет;

6) предупреждение о правонарушении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу между $z_3 + 1$ и z_4 или тюремному заключению сроком от двух до 10 лет;

7) предупреждение о правонарушении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу или тюремному заключению сроком более 10 лет;

8) нет записи;

9) нет записи;

10) нет записи.

B.6. Менеджмент и бизнес-операции

Информация может быть такой, что ее компрометация способна нанести ущерб эффективности работы организации. Например, будучи раскрытой, относящаяся к внесению изменений в политике информация может спровоцировать такую общественную реакцию, что реализация данной политики станет невозможной. Модификация, изменение смысла переданной информации или недоступность информации, касающейся финансовых аспектов или компьютерного программного обеспечения, могут также иметь серьезные последствия для работы организации. Кроме того, отказ от обязательств по обеспечению ИБ может иметь негативные последствия для бизнеса. Предлагается руководствоваться следующими рекомендациями по оценке последствий:

1) неэффективная работа одного подразделения организации;

2) нет записи;

3) нарушение функций (деятельности) по эффективному руководству организацией и ее работы;

4) нет записи;

5) создание препятствий для эффективной разработки или функционирования политик организации;

6) причинение ущерба организации при коммерческих или политических переговорах с другими организациями;

7) создание препятствий для разработки или функционирования главных политик организации, отключение или значительное прерывание важных операций каким-либо другим способом;

8) нет записи;

9) нет записи;

10) нет записи.

В.7. Утрата престижа

Несанкционированное раскрытие информации, отказ от обязательств по обеспечению ИБ или модификация информации, а также недоступность информации могут привести к потере престижа организации с последующим возможным нанесением ущерба ее репутации, к потере доверия и другим негативным последствиям. Предлагается руководствоваться следующими рекомендациями по оценке престижа организации:

1) нет записи;

2) создание атмосферы недовольства внутри организации;

3) негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям местного/регионального масштаба;

4) нет записи;

5) негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям национального масштаба;

6) нет записи;

7) значительное негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям;

8) нет записи;

9) нет записи;

10) нет записи.

Приложение 4.

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

Состав
постоянно действующей комиссии по информационной безопасности (защите информации) в Администрации Качканарского городского округа Свердловской области

№ п.п.	Фамилия Имя Отчество	Должность
1	Блинов Петр Алексеевич	Заместитель главы Качканарского городского округа по социальным вопросам **председатель комиссии**
2	Симаненко Марина Евгеньевна	Начальник отдела по организационной работе **заместитель председателя комиссии**
3	Зеленин Владимир Сергеевич	Главный специалист отдела по организационной работе **секретарь комиссии**
Члены комисии		
4	Симакова Наталья Анатольевна	Начальник отдела по делам гражданской обороны, чрезвычайным ситуациям, мобилизационной подготовке и безопасности
5	Пономарев Максим Михайлович	Системный администратор муниципального казенного учреждения «Административный исполнительный центр» (по согласованию)

Приложение 5.

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

Состав
группы реагирования на инциденты информационной безопасности
в Администрации Качканарского городского округа
Свердловской области

№ п.п.	Фамилия Имя Отчество	Должность
1	Блинов Петр Алексеевич	Заместитель главы Качканарского городского округа по социальным вопросам
2	Симаненко Марина Евгеньевна	Начальник отдела по организационной работе
3	Симакова Наталья Анатольевна	Начальник отдела по делам гражданской обороны, чрезвычайным ситуациям, мобилизационной подготовке и безопасности
4	Зеленин Владимир Сергеевич	Главный специалист отдела по организационной работе
5	Пономарев Максим Михайлович	Системный администратор муниципального казенного учреждения «Административный исполнительный центр»

Приложение 6.

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

Инструкция пользователя Администрации Качканарского городского округа Свердловской области

Общие обязанности сотрудников по обеспечению информационной безопасности

Сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации, несет персональную ответственность за свои действия и обязан:

1) использовать предоставленные ему аппаратно-программные средства только для выполнения своих должностных обязанностей;
2) использовать предоставленное ему дисковое пространство сервера только для хранения информационных ресурсов, необходимых для осуществления своих должностных обязанностей;
3) использовать пароли, отвечающие установленным требованиям информационной безопасности;
4) использовать антивирусное программное обеспечение при работе с внешними носителями информации и файлами полученными из интернета;
5) соблюдать требования федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи», федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и защите информации», Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»;
6) при утере пароля пользователь немедленно поставить в известность ответственного по информационной безопасности. Ответственность за несвоевременность уведомления о факте компрометации пароля несет непосредственно пользователь;
7) при утере или компрометации электронной цифровой подписи немедленно поставить в известность непосредственного руководителя и ответственного по информационной безопасности. Ответственность за несвоевременность уведомления о факте утери или компрометации электронной цифровой подписи несет непосредственно пользователь;
8) при обнаружении несанкционированных изменений в аппаратных или программных средствах немедленно поставить в известность ответственного по информационной безопасности;
9) при обнаружении некорректного функционирования программного обеспечения по защите информации немедленно поставить в известность ответственного по информационной безопасности.

Сотруднику запрещается:

1) передавать любые пароли, предназначенные для работы с информационными системами, в том числе при убытии в командировку, отпуск и в случае болезни;

2) использовать в работе принадлежащие другим сотрудникам пароли, предназначенные для работы с информационными системами, в том числе при убытии сотрудника в командировку, отпуск и в случае болезни;
3) осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
4) осуществлять несанкционированный доступ к информационным ресурсам;
5) самостоятельно производить установку, настройку и модификацию программного обеспечения;
6) использовать сменные машинные носители информации без предварительной проверки на наличие программных вирусов;
7) самостоятельно вскрывать и производить разборку компьютеров, периферийного оборудования;
8) производить какие-либо изменения в электрических схемах, монтаже, размещения и комплектации технических средств на автоматизированных рабочих местах.

Обязанности сотрудников по работе с корпоративной электронной почтой

Электронная почта является собственностью учреждения и может быть использована ТОЛЬКО в служебных целях. Использование электронной почты в других целях категорически запрещено.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления сотрудника по требованию непосредственного либо вышестоящего руководителя.

Сотруднику запрещается:

1) распространять информацию содержание и направленность которой запрещены международным и Российским законодательством;
2) осуществлять массовую рассылку почтовых сообщений;
3) предоставлять, кому бы-то ни было пароль доступа к своему почтовому ящику;
4) отправлять во вложениях файлы мультимедиа и исполняемые файлы, письма с такими вложениями не обрабатываются почтовым сервером и не могут быть доставлены;

При работе с почтовой обратить на следующие моменты :

1) Внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;
2) Проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
3) Не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyuri.com и т.д.);
4) Не нажимать на ссылки из письма, если они заменены на слова, не наводить на них мышкой и просматривать полный адрес сайтов;
5) Проверять ссылки, даже если письмо получено от другого пользователя информационной системы;

6) Не открывать вложения, особенно если в них содержаться документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;
7) Пересылать все подозрительные электронные письма на почтовый ящик электронной почты sd@kgo66.ru с темой «Подозрительное письмо»

Внимание!

Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политиками учреждения.

Вся информация о ресурсах, посещаемых сотрудниками компании, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а так же руководству учреждения для детального изучения.

Сотрудники могут нести дисциплинарную ответственность за нарушение данной инструкции.

Приложение 7.
УТВЕРЖДЕНО
Распоряжением Администрации
Качканарского городского округа
Свердловской области
От 29.09.2023 № 83
«Об информационной безопасности (защите информации) в Администрации Качканарского городского округа Свердловской области»

Лист № ________________

Журнал регистрации пользователей Администрации Качканарского городского округа

№ п.п.	**Дата подключения / отключения**	**Организация пользователя / Полная должность**	**Фамилия / Имя / Отчество**	**Учетная запись**	**Дата/Подпись**