Регламент
реагирования на компьютерные инциденты информационной безопасности
в ГКУ Пензенской области «Ресурсный центр социального обслуживания населения Пензенской области»

2022

Термины и определения

Информационная безопасность (далее – ИБ) – это процесс обеспечения конфиденциальности, целостности и доступности информации.

Событие информационной безопасности – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Инцидент информационной безопасности (далее – инцидент ИБ) − одно или серия нежелательных или неожиданных событий в системе информационной безопасности, которые имеют большой шанс скомпрометировать деловые операции и поставить под угрозу защиту информации.

Ответственный за информационную безопасность в Центре и системный администратор – ответственные лица за выполнение функций по технической защите информации в Центра

Пользователь – сотрудник Центра.

Автоматизированное рабочее место (далее – АРМ) – индивидуальный комплекс технических и программных средств, предназначенный для автоматизации профессионального труда специалиста и обеспечивающий подготовку, редактирование, поиск и выдачу на экран и печать необходимых ему документов и данных.

1. Общие положения

1.1. Настоящий Регламент разработан в соответствии с федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями), от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с последующими изменениями.

1.1. Целью регламента является обеспечение своевременного реагирования и оповещения об инцидентах информационной безопасности, связанных с совершением компьютерных атак, внедрением вредоносного программного обеспечения, а также возможными техническими сбоями в работе при повседневной работе сотрудников в ГКУ Пензенской области «Ресурсный центр социального обслуживания населения Пензенской области» (далее – Центр).

1.3. Пользователь, ответственный за информационную безопасность в Центре и системный администратор сети в своей работе руководствуется Регламентом, а также иными руководящими, нормативными документами и регламентирующими документами в области информационной безопасности.

2. События информационной безопасности, приводящие к возникновению инцидентов информационной безопасности

2.1. В качестве событий информационной безопасности, приводящих к инцидентам информационной безопасности, могут быть:

- появление файлов с нетипичным именем, форматом или большим размером;
- исчезновение файлов или папок;
- модификация файлов или их содержимого;
- выполнение процессов, не запускаемых пользователем;
- значительное замедление работы программного обеспечения;
- резкое сокращение свободного пространства на жестком диске;
- блокировка экрана монитора или средств ввода/вывода информации;
- появление рекламных или иных баннеров на экране монитора;
- самопроизвольное скачивание и/или запуск/установка файлов;
- изменение/блокировка учетных данных пользователя или доступа к ресурсам;
- умышленные действия пользователя, включающие самовольную установку системного и/или программного обеспечения, а также действия, приводящие к техническим сбоям в работе компьютерного оборудования (отказу в обслуживании);
- другие события, которые могут привести к несанкционированному доступу к ресурсам или отказу в обслуживании.

3. Первоочередные меры при обнаружении инцидента информационной безопасности, связанного с совершением компьютерных атак и внедрением вредоносного программного обеспечения

3.1. Инцидентом информационной безопасности, связанного с совершением компьютерных атак и внедрением вредоносного программного обеспечения, необходимо считать состояние системы, которое привело к несанкционированному доступу к служебной информации и/или ресурсам Центра, а также отказу в обслуживании вследствие наступления одного или нескольких состояний информационной безопасности.

3.2. При наступлении инцидента информационной безопасности важно не пытаться самостоятельно изменять расширения зараженных файлов, а также удалять любые файлы с рабочего компьютера и электронные сообщения.

3.3. Основными первоочередными мерами по нейтрализации последствий инцидентов информационной безопасности, связанных с совершением компьютерных атак и внедрением вредоносного программного обеспечения, являются:

- отключение АРМ сотрудника от локальной сети Центра (производится незамедлительно при обнаружении события информационной безопасности, приводящего к возникновению инцидента информационной безопасности);
- отключение АРМ сотрудника от информационно-телекоммуникационной сети «Интернет» (производится незамедлительно при обнаружении события информационной безопасности, приводящего к возникновению инцидента информационной безопасности);
- незамедлительное оповещение администратора информационной безопасности вычислительной сети и/или системного администратора Центра;
- незамедлительное отключение питания компьютера (при отключении питания компьютера не пытаться его перезагрузить или включить заново, так как эти действия приводят к изменению файловой системы);
- подготовка докладной записки на имя начальника отдела перспективных разработок и технического обслуживания, в которой отражена последовательность действий, приведших к наступлению инцидента информационной безопасности (в произвольной форме);
- внесение записи администратором информационной безопасности вычислительной сети в журнал инцидентов информационной безопасности.

4. Обязанности должностных лиц при наступлении инцидентов информационной безопасности

4.1. Обязанности пользователя:

- Соблюдение требований Свода правил по безопасной работе при осуществлении организации информационного взаимодействия с использованием информационно-телекоммуникационной сети «Интернет» (далее – Свод правил).

- Выполнение требований и рекомендации администратора информационной безопасности вычислительной сети и системного администратора в рамках соблюдения настоящего Регламента.

- При обнаружении событий, указанных в п. 3, незамедлительное информирование администратора информационной безопасности вычислительной или системного администратора Центра.

4.2. Общие обязанности администратора информационной безопасности вычислительной сети и системного администратора:

- осуществление контроля за соблюдением пользователями Свода правил;

- информирование непосредственного руководства о фактах нарушений требований Свода правил со стороны пользователей;

- обеспечение функционирования установленных средств защиты информации;

- информирование непосредственного руководства обо всех фактах инцидентов, повлекших выход из строя либо временную приостановку автоматизированного рабочего места, информационных ресурсов или серверного оборудования, а также о фактах несанкционированного воздействия, заражения вредоносными программами.

4.3. Обязанности администратора информационной безопасности вычислительной сети:

- своевременно информировать руководство об истечении сроков действия сертификатов соответствия и лицензий на средства защиты информации;

- проводить при приеме нового сотрудника инструктажа пользователей по вопросу информационной безопасности согласно Своду правил, настоящему Регламенту и действующему законодательству по защите информации;

- проведение при необходимости дополнительного инструктажа пользователей по вопросу информационной безопасности;

- отметки о проведении инструктажа заносить в журнал регистрации инструктажей и заверять собственноручной подписью инструктируемого сотрудника;

- ведение журнала инцидентов информационной безопасности.