ПОЛОЖЕНИЕ
по работе с инцидентами информационной безопасности

Настоящее Положение разработано в целях организации работы с инцидентами информационной безопасности в ГКУ Пензенской области «Ресурсный центр социального обслуживания населения Пензенской области» (далее по тексту Центр).

Инцидент - одно событие или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы (далее - ИС) и (или) к возникновению угроз безопасности, в том числе персональных данных (далее – ПДн).

1. Общие положения

1.1.Положение о работе с инцидентами информационной безопасности (далее – Положение) разработано в соответствии с:

1) Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2) Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3) Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4) Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5) Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6) Политикой информационной безопасности Центра.

1.2. Работа с инцидентами в области информационной безопасности (далее – ИБ) помогает определить наиболее актуальные угрозы ИБ, создает обратную связь в системе обеспечения ИБ, что способствует повышению общего уровня защиты информационных ресурсов и ИС.

1.3. Работа с инцидентами включает в себя следующие направления:

1) определение лиц, ответственных за выявление инцидентов и реагирование на них;

2) обнаружение, идентификация и регистрация инцидентов;

3) своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС пользователями и администраторами;

4) анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценка их последствий;

5) принятие мер по устранению последствий инцидентов;

6) планирование и принятие мер по предотвращению повторного возникновения инцидентов.

1.4.Для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а так же оценки их последствий, планирования и принятия мер по предотвращению повторного возникновения инцидентов, назначается постоянно действующая комиссия по работе с инцидентами в соответствии с приказом руководителя Центра.

2. Ответственные за выявление инцидентов и реагирование на них

2.1. В ИС ответственными за выявление инцидентов являются:

1) лица, имеющие право доступа к ИС;

2) ответственный за обеспечение безопасности персональных данных в информационной системе Центра;

3) системный администратор;

4) администратор баз данных.

Ответственными за реагирование на инциденты в ИС являются:

1) лица, имеющих право доступа к ИС;

2) руководитель подразделения Учреждения, в котором выявлен инцидент;

3) ответственный за обеспечение безопасности персональных данных в информационной системе Центра ;

4) системный администратор;

5) администратор баз данных.

2.2. Вне ИС ответственными за выявление инцидентов являются все сотрудники Центра.

Ответственными за реагирование на инциденты вне ИС являются:

1) сотрудник Центра, обнаруживший инцидент;

2) руководитель подразделения Центра, в котором выявлен инцидент;

3) ответственный за обеспечение безопасности персональных данных в информационной системе Центра., в случае, если существует угроза безопасности ПДн.

3. Обнаружение, идентификация и регистрация инцидентов

3.1. Работа по обнаружению инцидентов в области ИБ включает в себя мероприятия, направленные на:

1) выявление инцидентов в области ИБ с помощью технических средств;

2) выявление инцидентов в области ИБ в ходе контрольных мероприятий;

3) выявление инцидентов с помощью сотрудников Центра.

3.2. Работа по идентификации инцидентов в области ИБ включает в себя мероприятия, направленные на доведение до сотрудников Центра информации, позволяющей идентифицировать инциденты.

3.3. Регистрацию инцидентов осуществляет Председатель комиссии по работе с инцидентами в журнале регистрации инцидентов ИБ.

Хранение журнала осуществляется в местах, исключающих доступ к журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Ответственный за хранение ведение и хранение журнала - ответственный за обеспечение безопасности персональных данных в информационной системе Центра.

4. Информирование о возникновении инцидентов

Работник Центра (пользователь), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, Администратору ИС, ответвеннорму за информационную безопасность в Ценнтре, Ответственному за организацию обработки ПДн (в случае если ИС является ИСПДн).

Администратор ИС, в случае необходимости, информирует пользователей ИС о возникновении инцидента и дает указания по дальнейшим действиям.

5. Анализ инцидентов, а также оценка их последствий

Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценку их последствий осуществляет комиссия по работе с инцидентами ИБ.

5.1. Источниками и причинами возникновения инцидентов в области ИБ являются:

1) отсутствие персональной ответственности сотрудников Центра и их руководителей за обеспечение ИБ, в том числе ПДн;

2) недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе ПДн;

3) отсутствие моральной и материальной стимуляции за соблюдение правил и требований ИБ;

4) пренебрежение правилами и требованиями ИБ сотрудниками Центра.

5.2. Оценка последствий инцидента производится на основании потенциально-возможного ущерба.

6. Принятие мер по устранению последствий инцидентов

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

1) определение границ инцидента и ущерба от реализации угроз ИБ;

2) ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

7. Планирование и принятие мер по предотвращению инцидентов

7.1. Планирование и принятие мер по предотвращению повторного возникновения инцидентов осуществляет комиссия по работе с инцидентами ИБ и основывается на:

1) планомерной деятельности по повышению уровня осознания ИБ руководством и сотрудниками Центра;

2) проведении мероприятий по обучению сотрудников Центра правилам и способам работы со средствами защиты ИС;

3) доведении до сотрудников норм законодательства, внутренних документов Учреждения, устанавливающих ответственность за нарушение требований ИБ;

4) разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимаемыми на работу;

5) своевременной модернизации системы обеспечения ИБ, с учетом возникновения новых угроз ИБ;

6) своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

7.2. Работа с персоналом.