Приложение 1
к приказу ГБУ КЦСОН
Дубровского района
от 11.06.2024 г. № 86

# ПОЛОЖЕНИЕ
# по работе с инцидентами информационной безопасности в ГБУ КЦСОН Дубровского района

## 1. Общие положения

1.1. Настоящее Положение о работе с инцидентами информационной безопасности в ГБУ КЦСОН Дубровского района (далее – Положение) разработано в целях организации работы с инцидентами информационной безопасности в ГБУ КЦСОН Дубровского района (далее – Учреждение).

1.2. Положение разработано в соответствии с:

1.2.1. Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

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

1.2.3. Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

1.2.4. Требованиями по реализации мер, предусмотренных составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждёнными приказом ФСТЭК России от 18.02.2013 № 21.

1.2.5. Правилами обработки персональных данных в Учреждении.

1.3. Основные понятия:

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

1.3.2. Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов и информационных систем.

1.4. Основные направления:

1.4.1. Определение лиц, ответственных за выявление инцидентов и реагирование на них;

1.4.2. Обнаружение, идентификация и регистрация инцидентов;

1.4.3. Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

1.4.4. Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценка их последствий;

1.4.5. Принятие мер по устранению последствий инцидентов;

1.4.6. Планирование и принятие мер по предотвращению повторного возникновения инцидентов.

1.5. Для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также 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 Учреждения.

## 2. Сотрудники, ответственные за выявление инцидентов и реагирование на них

2.1. Ответственными за выявление инцидентов являются:

2.1.1. Сотрудники, имеющие право доступа к ИС и/или право доступа в кабинет, в котором произошел инцидент.

2.1.2. Администратор ИС.

2.1.3. Сотрудник, ответственный за обеспечение безопасности персональных данных в ИС.

2.2. Ответственными за реагирование на инциденты в ИС являются:

2.1.4. Сотрудники, имеющие право доступа к ИС и/или право доступа в кабинет, в котором произошел инцидент.

2.1.5. Администратор ИС.

2.1.6. Ответственный за обеспечение безопасности персональных данных в ИС.

2.1.7. Сотрудник, ответственный за организацию обработки персональных данных.

2.1.8. Председатель комиссии по работе с инцидентами.

## 3. Обнаружение, идентификация и регистрация инцидентов

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

3.1.1. Выявление инцидентов в области информационной безопасности с помощью технических средств.

3.1.2. Выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий.

3.1.3. Выявление инцидентов с помощью сотрудников Учреждения.

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

3.3. Форма журнала утверждается приказом руководителя Учреждения.

3.4. 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 - председатель комиссии по работе с инцидентами.

## 4. Информирование о возникновении инцидентов

4.1. Сотрудник Учреждения, обнаруживший инцидент, должен незамедлительно сообщить об инциденте сотруднику, ответственному за обеспечение безопасности персональных данных в ИС; ответственному за организацию обработки персональных данных; председателю комиссии по работе с инцидентами.

4.2. Сотрудник, ответственный за обеспечение безопасности персональных данных в ИС или председатель комиссии по работе с инцидентами, в случае необходимости, информирует пользователей ИС и прочих сотрудников Учреждения о возникновении инцидента и дает указания по дальнейшим действиям.

## 5. Анализ инцидентов, а также оценка их последствий

5.1. Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий осуществляет комиссия по работе с инцидентами информационной безопасности.

5.2. Источниками и причинами возникновения инцидентов в области информационной безопасности являются:

5.2.1. Действия организаций и отдельных лиц враждебные интересам Учреждения.

5.2.2. Отсутствие персональной ответственности сотрудников Учреждения обеспечение информационной безопасности, в том числе персональных данных.

5.2.3. Недостатки в работе ответственных сотрудников по обеспечению необходимого режима соблюдения конфиденциальности в Учреждении, в том числе персональных данных.

5.2.4. Недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности.

5.2.5. Совмещение функций по работе в информационной системе и с персональными данными с прочими функциями и обязанностями.

5.2.6. Наличие избыточных привилегированных полномочий у пользователей в информационной системе.

5.2.7. Пренебрежение сотрудниками Учреждения правил и требований по соблюдению информационной безопасности.

5.2.8. Другие причины.

5.3. Оценка последствий инцидента производится комиссией по работе с инцидентами на основании выявления фактического или потенциально возможного ущерба.

## 6. Принятие мер по устранению последствий инцидентов

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

6.1.1. Определение причин и последствий инцидента, ущерба причиненного инцидентом.

6.1.2. 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 возникновения инцидентов осуществляет комиссия по работе с инцидентами информационной безопасности и основывается на:

7.1.1. Планомерной деятельности по повышению уровня знания сотрудников Учреждения правил и порядка информационной безопасности.

7.1.2. Проведении обучения сотрудников Учреждения правилам и способам работы со средствами защиты информационных систем.

7.1.3. Доведении до сотрудников требований законодательства, внутренних документов Учреждения, устанавливающих ответственность за нарушение требований информационной безопасности.

7.1.4. Поддержание в актуальном, рабочем состоянии системы обеспечения информационной безопасности, с учетом возникновения новых угроз информационной безопасности и/или в случаях изменения требований законодательства и руководящих документов регуляторов по организации обеспечения информационной безопасности;

7.1.5. Своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

7.2. Работа с персоналом:

7.2.1. Как правило, самым слабым звеном в любой системе безопасности является человек. Поэтому работа с персоналом является основным направлением деятельности по обеспечению требований информационной безопасности.

7.2.2. В работе с персоналом основной упор должен делаться не на наказание сотрудника за нарушения в области информационной безопасности, а на поощрение за надлежащие выполнение требований

информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

7.2.3. Персонал Учреждения является основным источником сведений о возможных и произошедших инцидентах информационной безопасности. Оперативное информирование персоналом об инциденте информационной безопасности ответственных сотрудников Учреждения позволяют снизить ущерб от инцидента и являются основанием для смягчения либо отмены наказания сотрудников за нарушение требований информационной безопасности.