**Приложение № 6**

ПРИНЯТО
на общем собрании работников
протокол № ___ от «___» _____ 20____ г.

УТВЕРЖДЕНО
приказом директора
ГБОУ СОШ «ОЦ»
п.г.т. Рощинский
№360-од от 04.08.2022 года
_____ О.И. Рубина


C=RU, O="ГБОУ СОШ ""ОЦ"" п.г.т. Рощинский",
CN=Рубина О.И., E=roshinsky_sch_vlg@samara.edu.ru
00ea17aca4d591c1ca
2022.08.04 14:54:14+04'00'

# Положение
# по работе с инцидентами информационной безопасности

**1. Общие положения**

1.1. Настоящее Положение по работе с инцидентами информационной безопасности (далее – Положение) государственного бюджетного общеобразовательного учреждения Самарской области средней общеобразовательной школы «Образовательного центра» имени 81 гвардейского мотострелкового полка п.г.т. Рощинский муниципального района Волжский Самарской области (далее – образовательная организация) разработано в целях организации работы с инцидентами информационной безопасности в образовательной организации.

1.2. 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).

1.3. Положение разработано в соответствии с:

- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- 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».

1.4. 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.

1.5. Работа с инцидентами включает в себя следующие направления:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение, идентификация и регистрация инцидентов;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС пользователями и администраторами;
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценка их последствий;
- принятие мер по устранению последствий инцидентов;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

1.6. 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 директора образовательной организации.

**2. Ответственные за выявление инцидентов и реагирование на них**

2.1. В ИС ответственными за выявление инцидентов являются:

- лица, имеющие право доступа к ИС;
- ответственный за техническое обслуживание ИС;
- администратор ИС;
- администратор информационной безопасности ИС.

2.2. Ответственными за реагирование на инциденты в ИС являются:

- лица, имеющих право доступа к ИС;
- администратор ИС, в которой выявлен инцидент;
- администратор ИС;
- администратор информационной безопасности ИС;
- ответственный за организацию обработки ПДн образовательной организации, в случае, если ИС является информационной системой персональных данных (далее - ИСПДн);
- председатель комиссии по работе с инцидентами.

2.3. Вне ИС ответственными за выявление инцидентов являются все работники образовательной организации.

2.4. Ответственными за реагирование на инциденты вне ИС являются:

- работник образовательной организации, обнаруживший инцидент;
- администратор ИС, в которой выявлен инцидент;
- ответственный за организацию обработки ПДн, в случае, если существует угроза безопасности ПДн;
- председатель комиссии по работе с инцидентами.

**3. Обнаружение, идентификация и регистрация инцидентов**

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

- выявление инцидентов в области ИБ с помощью технических средств;
- выявление инцидентов в области ИБ в ходе контрольных мероприятий;
- выявление инцидентов с помощью работников образовательной организации.

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

3.3. Регистрацию инцидентов осуществляет Председатель комиссии по работе с инцидентами в журнале регистрации инцидентов ИБ. Форма журнала утверждается приказом директора образовательной организации.

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. Работник образовательной организации (пользователь), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю (директору), Администратору ИС, Администратору информационной безопасности ИС, Ответственному за организацию обработки ПДн (в

случае если ИС является ИСПДн), председателю комиссии по работе с инцидентами.
4.2. 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**

5.1. Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценку их последствий осуществляет комиссия по работе с инцидентами ИБ.
5.2. Источниками и причинами возникновения инцидентов в области ИБ являются:

- враждебные действия организаций и отдельных лиц интересам образовательной организации;
- отсутствие персональной ответственности работников образовательной организации и их руководителей за обеспечение ИБ, в том числе ПДн;
- недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе ПДн;
- отсутствие моральной и материальной стимуляции за соблюдение правил и требований ИБ;
- недостаточная техническая оснащённость подразделений, ответственных за обеспечение ИБ;
- совмещение функций по разработке и сопровождению или сопровождению и контролю за ИС;
- наличие привилегированных бесконтрольных пользователей в ИС;
- пренебрежение правилами и требованиями ИБ работниками образовательной организации;
- другие причины.

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

**6. Принятие мер по устранению последствий инцидентов**

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

- определение границ инцидента и ущерба от реализации угроз ИБ;
- 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:

- планомерной деятельности по повышению уровня осознания ИБ руководством и работниками образовательной организации;
- проведении мероприятий по обучению работников образовательной организации правилам и способам работы со средствами защиты ИС;
- доведении до работников образовательной организации норм законодательства, внутренних документов образовательной организации, устанавливающих ответственность за нарушение требований ИБ;
- разъяснительной работе с увольняющимися работниками и работниками, принимаемыми на работу;

- своевременной модернизации системы обеспечения ИБ, с учетом возникновения новых угроз ИБ;
- своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

7.2. Работа с персоналом.

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

В работе с персоналом основной упор должен делаться не на наказание сотрудника за нарушения в области ИБ, а на поощрение за надлежащие выполнение требований ИБ, проявление личной инициативы в укреплении системы ИБ.

7.3. Персонал образовательной организации является важным источником сведений об инцидентах ИБ, поэтому необходимо донести до работников информацию о том, что оперативно предоставленные сведения об инциденте ИБ являются основанием для смягчения либо отмены наказания за нарушение требований ИБ.