

УТВЕРЖДАЮ
директор МБОУ ДО ЦТ
_____ Е.С.Миндрина
" ____ " _____ 2015 года

ПОЛОЖЕНИЕ
по работе с инцидентами информационной безопасности
Аннотация

Настоящее Положение разработано в целях организации работы с инцидентами информационной безопасности в муниципальном бюджетном образовательном учреждении дополнительного образования Центре творчества (далее – МБОУ ДО ЦТ).

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. Общие положения

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

- 1) Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- 2) Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 3) требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119;
- 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 февраля 2013 года № 21;
- 5) политикой информационной безопасности МБОУ ДО ЦТ.

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.

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 информационной системе 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.

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 директора МБОУ ДО ЦТ .

2. Ответственные за выявление инцидентов и реагирование на них

2.1. В информационных системах.

Ответственными за выявление инцидентов в ИС являются:

- 1) лица, имеющие право доступа к ИС;
- 2) ответственный за техническое обслуживание ИС;
- 3) администратор ИС;
- 4) администратор информационной безопасности ИС.

Ответственными за реагирование на инциденты в ИС являются:

- 1) лица, имеющих право доступа к ИС;
- 2) руководитель подразделения МБОУ ДО ЦТ, в котором выявлен инцидент;
- 3) ответственный за техническое обслуживание ИС;
- 4) администратор ИС;
- 5) администратор информационной безопасности ИС;
- 6) ответственный за организацию обработки персональных данных МБОУ ДО ЦТ в случае, если ИС является информационной системой персональных данных (далее - ИСПДн);
- 7) Председатель комиссии по работе с инцидентами.

2.2. Вне информационных систем.

Ответственными за выявление инцидентов вне ИС являются все работники МБОУ ДО ЦТ.

Ответственными за реагирование на инциденты вне ИС являются:

- 1) работник МБОУ ДО ЦТ , обнаруживший инцидент;
- 2) руководитель подразделения МБОУ ДО ЦТ, в котором выявлен инцидент;
- 3) ответственный за организацию обработки персональных данных

МБОУ ДО ЦТ, в случае, если существует угроза безопасности персональных данных;

4) 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:

1) выявление инцидентов в области информационной безопасности с помощью технических средств;

2) выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

3) выявление инцидентов с помощью работников МБОУ ДО ЦТ.

3.2. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до работников МБОУ ДО ЦТ информации, позволяющей идентифицировать инциденты.

3.3. Регистрацию инцидентов осуществляет Председатель комиссии по работе с инцидентами в журнале регистрации инцидентов информационной безопасности. Форма журнала утверждается приказом директора МБОУ ДО ЦТ

Хранение журнала осуществляется в местах, исключающих доступ к журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Ответственный за хранение ведения и хранение журнала - Председатель комиссии по работе с инцидентами.

4. Информирование о возникновении инцидентов

Работник МБОУ ДО ЦТ (пользователь ИС), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, администратору ИС, администратору информационной безопасности ИС, ответственному за организацию обработки персональных данных МБОУ ДО ЦТ (в случае если ИС является ИСПДн), Председателю комиссии по работе с инцидентами.

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 также оценку их последствий осуществляет комиссия по работе с инцидентами информационной безопасности.

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

1) действия организаций и отдельных лиц враждебные интересам МБОУ ДО ЦТ;

2) отсутствие персональной ответственности работников МБОУ ДО ЦТ и их руководителей за обеспечение информационной безопасности, в том числе персональных данных;

3) недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе персональных данных;

4) отсутствие дисциплинарной мотивации соблюдения правил и требований информационной безопасности;

5) недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности;

6) совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;

7) наличие привилегированных бесконтрольных пользователей в информационной системе;

8) пренебрежение правилами и требованиями информационной безопасности работниками МБОУ ДО ЦТ;

9) и другие причины.

5.2. Оценка последствий инцидента производится на основании потенциально возможного или фактического 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 информационной безопасности;

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:

1) планомерной деятельности по повышению уровня осознания информационной безопасности руководством и работниками МБОУ ДО ЦТ;

2) проведении мероприятий по обучению работников МБОУ ДО ЦТ правилам и способам работы со средствами защиты информационных систем;

3) доведении до работников норм законодательства, внутренних

документов МБОУ ДО ЦТ, устанавливающих ответственность за нарушение требований информационной безопасности;

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

5) своевременной модернизации системы обеспечения информационной безопасности, с учетом возникновения новых угроз информационной безопасности, либо в случае изменения требований руководящих документов по организации обеспечения информационной безопасности;

6) 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 информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание работника за нарушения в области информационной безопасности, а на поощрение за надлежащее выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

Персонал МБОУ ДО ЦТ является важным источником сведений об инцидентах информационной безопасности, поэтому необходимо донести до работников информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности являются основанием для смягчения либо отмены наказания за нарушение требований информационной безопасности.

Директор

Е.С.Миндрина