МИНИСТЕРСТВО ЭНЕРГЕТИКИ, ПРОМЫШЛЕННОСТИ И СВЯЗИ СТАВРОПОЛЬСКОГО КРАЯ

государственное бюджетное профессиональное образовательное учреждение «Невинномысский химико-технологический колледж»

(ГБПОУ НХТК)

УТВЕРЖДАЮ
Директор ГБПОУ НХТК

_____ А.П. Москвитин
«25» 01 2018

ПОЛОЖЕНИЕ

по работе с инцидентами информационной безопасности

1 Общие положения

1.1 Настоящее Положение разработано в целях организации работы с инцидентами информационной безопасности в государственном бюджетном профессиональном образовательном учреждении «Невинномысский химико-технологический колледж» (далее – Учреждение).

1.2 Инцидент – одно событие или группа событий, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности, в том числе защищаемой информации.

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

1) Федеральным законом № 152-ФЗ «О персональных данных»;

2) Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3) Постановлением Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4) Приказом ФСТЭК России № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

5) Приказом ФСТЭК России № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

6) политикой информационной безопасности Учреждения.

1.4 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.

1.5 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 также оценка их последствий;

5) принятие мер по устранению последствий инцидентов;

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

1.6 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 Учреждения.

2 Ответственные за выявление инцидентов и реагирование на них

2.1 В информационных системах (далее – ИС) ответственными за выявление инцидентов являются:

1) лица, имеющие право доступа к ИС;
2) ответственный за техническое обслуживание ИС;
3) администратор ИС;
4) администратор информационной безопасности ИС.
5) ответственный за организацию защиты информации Учреждения.

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 техническое обслуживание ИС;
4) администратор ИС;
5) администратор информационной безопасности ИС;
6) ответственный за организацию защиты информации Учреждения;
7) председатель комиссии по работе с инцидентами.

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

Ответственными за реагирование на инциденты вне ИС являются:

1) сотрудник Учреждения, обнаруживший инцидент;
2) руководитель подразделения Учреждения, в котором выявлен инцидент;
3) ответственный за организацию защиты информации Учреждения, в случае, если существует угроза безопасности защищаемой информации;
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 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 Регистрацию инцидентов осуществляет председатель комиссии по работе с инцидентами в журнале регистрации инцидентов информационной безопасности. Форма журнала утверждается приказом директора Учреждения.

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

4 Информирование о возникновении инцидентов

4.1 Работник Учреждения (пользователь), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, администратору ИС, администратору информационной безопасности ИС, ответственному за организацию защиты информации, 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

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 Учреждения;

2) отсутствие персональной ответственности сотрудников Учреждения и их руководителей за обеспечение информационной безопасности;

3) недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности;

4) отсутствие моральной и материальной стимуляции за соблюдение 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 сотрудниками Учреждения и другие причины.

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

1) планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками Учреждения;

2) проведении мероприятий по обучению сотрудников Учреждения правилам и способам работы со средствами защиты информационных систем;

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

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

5) своевременной модернизации системы обеспечения информационной безопасности, с учетом возникновения новых угроз 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 информационной безопасности.

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.

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

Начальник отдела автоматизации О. А. Просвирина