Согласовано
Председатель ППР
Детского сада №200 ОАО «РЖД»
_____Соколова Е.С.
Протокол № 6 от 09.01.2023 г.

УТВЕРЖДЕНО
Заведующий
Детским садом №200 ОАО «РЖД»
_____Казак А.М.
Приказ от 09.01.2023 г. №2 о/д

ПОЛИТИКА
по работе с инцидентами информационной безопасности

Настоящее Политика разработана в целях организации работы с инцидентами информационной безопасности в частном дошкольном образовательном учреждении «Детский сад №200 открытого акционерного общества «Российские железные дороги» (далее – Учреждение)

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 – ПД).

1. Общие положения

Политика о работе с инцидентами информационной безопасности (далее – Политика) разработана 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. N 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».

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.

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.

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 заведующего Учреждения.

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 техническое обслуживание ИС;

Ответственными за реагирование на инциденты в ИС являются:
1) лица, имеющих право доступа к ИС;
2) руководитель Учреждения - председатель комиссии по работе с инцидентами;
3) ответственный за защиту ПД в Учреждении, в случае, если ИС является информационной системой персональных данных (далее - ИСПД);

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) ответственный за защиту ПД, в случае, если существует угроза безопасности ПД;
3) 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:
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.

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

3.3. Регистрацию инцидентов осуществляет Председатель комиссии по работе с инцидентами в журнале регистрации инцидентов ИБ. Форма журнала утверждается приказом заведующего Учреждения.

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

Работник Учреждения (пользователь), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, ответственному за защиту ПД (в случае если ИС является ИСПД).

Председатель комиссии по работе с инцидентами, 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) действия организаций и отдельных лиц враждебные интересам Учреждения;
2) отсутствие персональной ответственности сотрудников за обеспечение ИБ, в том числе ПД;
3) недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе ПД;
4) отсутствие моральной и материальной стимуляции за соблюдение правил и требований ИБ;
5) недостаточная техническая оснащённость подразделений, ответственных за обеспечение ИБ;
6) совмещение функций по разработке и сопровождению или сопровождению и контролю за ИС;
7) наличие привилегированных бесконтрольных пользователей в ИС;
8) пренебрежение правилами и требованиями ИБ сотрудниками.

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;
2) проведении мероприятий по обучению сотрудников 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.

Работа с персоналом является основным направлением деятельности по обеспечению требований ИБ.

В работе с персоналом основной упор должен делаться на поощрение за надлежащее выполнение требований ИБ, проявление личной инициативы в укреплении системы ИБ.

Оперативно предоставленные сведения об инциденте ИБ являются основанием для смягчения либо отмены наказания за нарушение требований ИБ.

КАЗАК АННА МИХАЙЛОВНА

Подписан: КАЗАК АННА МИХАЙЛОВНА
DN: C=RU, OU=ЗАВЕДУЮЩИЙ ДЕТСКИМ САДОМ, O=ДЕТСКИЙ САД №200 ОАО "РЖД", CN=КАЗАК АННА МИХАЙЛОВНА, E=200_DETCAD@MAIL.RU
Основание: Подпись документа
Местоположение: с. Балыкса
Дата: 2023-03-15 11:04:42