Частное дошкольное образовательное учреждение
«Детский сад №103 открытого акционерного общества
«Российские железные дороги»
(Детский сад № 103 ОАО «РЖД»)

УТВЕРЖДЕНО
Приказом заведующего
Детским садом № 103 ОАО «РЖД»
от 30.12.2021г. № 94/ОД

ПОЛОЖЕНИЕ
о работе с инцидентами информационной безопасности в Детском саду № 103 ОАО «РЖД»

I. Общие положения

1. Настоящее Положение разработано в целях организации работы с инцидентами информационной безопасности в частном дошкольном образовательном учреждении «Детский сад № 103 открытого акционерного общества «Российские железные дороги» (Детский сад № 103 ОАО «РЖД») (далее - ДОУ).

2. Инцидент - одно событие или группы событий, которые могут привести к возникновению угроз безопасности информации, в том числе персональных данных.

3. Положение о работе с инцидентами информационной безопасности (далее - Положение) разработано в соответствии с:

– Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных";

– Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации";

– требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119;

– 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;

– Положением об обработке и защиты персональных данных работников Детского сада № 103 ОАО «РЖД».

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.

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 информационной системе пользователями и администраторами;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– принятие мер по устранению последствий инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

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 распоряжением заведующего ДОУ.

II.Ответственные за выявление инцидентов и реагирование на них

7. В информационных системах.

а) Ответственными за выявление инцидентов в ИС являются:

– лица, имеющие право доступа к ИС;

б) Ответственными за реагирование на инциденты в ИС являются:

– лица, имеющие право доступа к ИС;

– заведующий ДОУ

– ответственный за организацию обработки персональных данных в ДОУ, в случае если ИС является информационной системой персональных данных (далее - ИСПДн);

– Председатель комиссии по работе с инцидентами.

8. Вне информационных систем.

а) Ответственными за выявление инцидентов вне ИС являются все работники ДОУ.

б) Ответственными за реагирование на инциденты вне ИС являются:

– работник ДОУ, обнаруживший инцидент;

– заведующий ДОУ

– ответственный за организацию обработки персональных данных в ДОУ, в случае если существует угроза безопасности персональных данных;

– Председатель комиссии по работе с инцидентами.

III.Обнаружение, идентификация и регистрация инцидентов

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

– выявление инцидентов в области информационной безопасности с помощью технических средств;

– выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

– выявление инцидентов с помощью работников ДОУ

10. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до работников ДОУ информации, позволяющей идентифицировать инциденты.

11. Регистрацию инцидентов осуществляет Председатель комиссии по работе с инцидентами в журнале регистрации инцидентов информационной безопасности (Приложение № 1).

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

IV.Информирование о возникновении инцидентов

13. Работник ДОУ (пользователь ИС), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте:

– заведующему ДОУ;

– ответственному за организацию обработки персональных данных в ДОУ (в случае если ИС является ИСПДн);

– Председателю комиссии по работе с инцидентами.

14. Председатель комиссии по работе с инцидентами, в случае необходимости, информирует пользователей ИС о возникновении инцидента и дает указания по дальнейшим действиям.

V.Анализ инцидентов, а также оценка их последствий

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

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

– действия организаций и отдельных лиц враждебные интересам ДОУ;

– отсутствие персональной ответственности работников ДОУ и их руководителей за обеспечение информационной безопасности, в том числе персональных данных;

– недостаточная работа с персоналом по обеспечению необходимого

режима соблюдения конфиденциальности, в том числе персональных данных;

– отсутствие дисциплинарной мотивации соблюдения правил и требований информационной безопасности;

– недостаточная техническая оснащённость ответственных за обеспечение информационной безопасности;

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

– наличие привилегированных бесконтрольных пользователей в информационной системе;

– пренебрежение правилами и требованиями информационной безопасности работниками ДОУ;

– и другие причины.

17. Оценка последствий инцидента производится на основании потенциально возможного или фактического ущерба.

VI.Принятие мер по устранению последствий инцидентов

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

– определение границ инцидента и ущерба от реализации угроз информационной безопасности;

– ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

VII.Планирование и принятие мер по предотвращению инцидентов

19. Планирование и принятие мер по предотвращению возникновения инцидентов осуществляет комиссия по работе с инцидентами информационной безопасности и основывается на:

– планомерной деятельности по повышению уровня осознания информационной безопасности работниками ДОУ.

– проведении мероприятий по обучению работников ДОУ правилам и способам работы со средствами защиты информационных систем;

– доведении до работников норм законодательства, внутренних документов ДОУ, устанавливающих ответственность за нарушение требований информационной безопасности;

– разъяснительной работе с увольняющимися работниками и работниками, принимаемыми на работу;

– 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;

– своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

20. Работа с персоналом.

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

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

в) Персонал ДОУ 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.

Приложение № 1
к Положению о работе с инцидентами
информационной безопасности
в Детском саду № 103 ОАО "РЖД"

ЖУРНАЛ
учета инцидентов информационной безопасности
в Детском саду № 103 ОАО «РЖД»

N п/п	**Дата**	**Краткое описание инцидента**	**Действия сотрудников**	**Заключение по фактам возникновения инцидентов**	**ФИО, подпись ответственных лиц за действия сотрудников**	**ФИО, подпись ответственных за обработку и безопасность**	**Примечание**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**