



МУНИЦИПАЛЬНОЕ КАЗЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 14  
ИМЕНИ В.И.МУРАВЛЕНКО СТАНИЦЫ НЕЗАМАЕВСКОЙ

ПРИКАЗ

от 29.12.2018.

№ 552

ст. Незамаевская

**О работе с инцидентами информационной безопасности**

В целях обеспечения требуемого режима информационной безопасности в МКОУ СОШ № 14 ст. Незамаевской, п р и к а з ы в а ю:

1. Утвердить положение по работе с инцидентами информационной безопасности (приложение № 1).

2. Назначить ответственным по работе с инцидентами информационной безопасности в учителя информатики Толмачеву Татьяну Николаевну.

3. Утвердить состав комиссии по работе с инцидентами информационной безопасности (приложение № 2).

4. Утвердить форму журнала регистрации инцидентов информационной безопасности (приложение № 3).

5. Ответственному по работе с инцидентами информационной безопасности:

5.1. Регистрировать в журнале все инциденты информационной безопасности.

5.2. При выявлении инцидентов информационной безопасности вносить в журнал следующую информацию:

- фамилия, имя, отчество, должность, сотрудника обнаружившего инцидент;

- дата выявления инцидента;

- описание инцидента;

- принятые меры по устранению последствий инцидента;

- причины возникновения инцидента;

- размер потенциально-возможного ущерба;

- размер фактического ущерба;

- принятые меры по предотвращению повторного возникновения инцидента.

6. Хранение журнала осуществлять в местах, исключаящих доступ к журналу посторонних лиц.

7. Хранить журнал в течение 5 лет после завершения ведения.

8. Контроль исполнения настоящего приказа оставляю за собой.

Директор

Е.П.Мигитко

ПРИЛОЖЕНИЕ № 1  
к приказу МКОУ СОШ № 14  
ст. Незамаевской  
от 29.12.2018. № 552

ПОЛОЖЕНИЕ  
по работе с инцидентами информационной безопасности

Настоящее Положение разработано в целях организации работы с инцидентами информационной безопасности в МКОУ СОШ № 14 ст. Незамаевской (далее - Школа).

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.

1. Общие положения

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

- Федеральным Законом № 152-ФЗ «О персональных данных»;
- Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановлением Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 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»;
- Политикой информационной безопасности Школы.

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:  
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 так же оценка их последствий;
- принятие мер по устранению последствий инцидентов;
- 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 директора Школы.

2. Определение лиц, ответственных за выявление инцидентов и реагирование на них

2.1. В информационных системах.

Ответственными за выявление инцидентов в ИС являются все лица, имеющих право доступа к ИС;

Ответственными за реагирование на инциденты в ИС являются:

- лица, имеющих право доступа к ИС;
- Ответственный за организацию обработки персональных данных Школы, в случае, если ИС является информационной системой персональных данных (далее - ИСПДн);
- Председатель комиссии по работе с инцидентами.

2.2. Вне информационных систем.

Ответственными за выявление инцидентов вне ИС являются все сотрудники Школы.

Ответственными за реагирование на инциденты вне ИС являются:

- сотрудник Школы, обнаруживший инцидент;
- ответственный за организацию обработки персональных данных Школы, в случае, если существует угроза безопасности персональных данных;
- 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:

- выявление инцидентов в области информационной безопасности с помощью технических средств;
- выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;
- выявление инцидентов с помощью сотрудников Школы.

3.2 Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

- доведение до сотрудников Школы 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 Школы.

Хранение журнала осуществляется в местах, исключаящих 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. Допускается ведение журнала в электронном виде.

4. Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами

Работник Школы (пользователь), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, ответственному за организацию обработки персональных данных (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, в том числе определение источников и причин возникновения инцидентов, а так же 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 информационной безопасности.

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

- действия организаций и отдельных лиц враждебные интересам Школы;

- отсутствие персональной ответственности сотрудников Школы 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 моральной и материальной стимуляции за соблюдение правил и требований информационной безопасности;

- недостаточная техническая оснащённость подразделений, 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 сотрудниками Управления;

- 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:

- определение границ инцидента и ущерба от реализации угроз информационной безопасности;
- ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

7. Планирование и принятие мер по предотвращению повторного возникновения инцидентов

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

- планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками Школы;
- проведении мероприятий по обучению сотрудников Школы правилам и способам работы со средствами защиты информационных систем;
- доведении до сотрудников норм законодательства, внутренних документов Школы, устанавливающих ответственность за нарушение требований информационной безопасности;
- разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимаемыми на работу;
- своевременной модернизации системы обеспечения информационной безопасности, с учетом возникновения новых угроз информационной безопасности;
- 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 сотрудника за нарушения в области информационной безопасности, а на поощрение за надлежащее выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

Персонал Школы 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.

Директор

Е.П.Мигитко

ПРИЛОЖЕНИЕ № 2  
к приказу МКОУ СОШ № 14  
ст. Незамаевской  
от 29.12.2018. № 552

Состав  
комиссии по работе с инцидентами информационной безопасности  
в МКОУ СОШ № 14 ст. Незамаевской

Председатель комиссии:

Мигитко Елена Петровна, директор.

Секретарь комиссии:

Толмачева Татьяна Николаевна, учитель информатики.

Члены комиссии:

Полевик Светлана Валерьевна, учитель русского языка и литературы;

Жеребненко Татьяна Николаевна, учитель математики;

Сальникова Ирина Николаевна, педагог-библиотекарь, председатель профсоюзного комитета

Директор

Е.П.Мигитко

ПРИЛОЖЕНИЕ № 3  
к приказу МКОУ СОШ № 14 ст.Незамаевской  
от 29.12.2018. № 552

ЖУРНАЛ  
регистрации инцидентов информационной безопасности  
в МКОУ СОШ № 14 ст.Незамаевской

№ п/п	ФИО, должность сотрудника, обнаружившего инцидент	Дата выявления инцидента	Описание инцидента	Принятые меры по устранению последствий	Причины возникновения инцидента	Размер потенциально возможного ущерба	Размер фактического ущерба	Принятые меры по предотвращению повторного возникновения инцидента

Директор

Е.П.Мигитко



