Министерство образования
Оренбургской области
Государственное казенное
общеобразовательное учреждение
«Специальная (коррекционная)
школа № 10» г. Орска

П Р И К А З

« 09 » августа 2023 г. № 65

«Об утверждении Инструкции
по управлению нештатными ситуациями»

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию по управлению нештатными ситуациями согласно приложению, к данному приказу.

2. Специалисту по IT- технологиям учреждения ***Смирнову Андрею Алексеевичу,*** довести приказ до сведения сотрудников учреждения.

3. Контроль за исполнением настоящего приказа оставляю за собой.

4. Настоящий приказ вступает в силу с даты его подписания.

Директор школы: С.П. Онищенко

Ознакомлен: Смирнов А.А.

Приложение к приказу

от « 09 »__08___2023 г. № 65

Инструкция
по управлению нештатными ситуациями в учреждении

1. Термины и определения

В рамках данной инструкции используются следующие термины и определения:

Доступ к информации – возможность получения информации и ее использования.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Нештатная ситуация информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Корпоративная сеть учреждения (далее - СКС) – объединение информационных систем, в том числе информационных систем персональных данных, компьютерного, телекоммуникационного и офисного оборудования всех подразделений учреждения, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Пользователь информационной системы – сотрудник учреждения (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в корпоративной сети учреждения в установленном порядке.

Событие – это наблюдаемое явление, которое невозможно предсказать (целиком) или которым невозможно управлять.

Инцидент – событие, которое может привести к явлению или эпизоду, не являющемуся серьезным.

Инцидент безопасности – это любое неблагоприятное событие, в результате которого некий аспект безопасности может подвергнуться угрозе.

Кризис – это состояние, вызванное некоторым событием, или знание о приближающемся событии, которое может вызвать серьезные негативные последствия.

2. Назначение

2.1. Настоящая Инструкция определяет содержание и порядок проведения мероприятий при обнаружении нештатных ситуаций и инцидентов информационной безопасности, их оценке, реагировании и ликвидации в учреждении.

2.2. Целью процесса управления инцидентами является восстановление нормального функционирования информационных систем министерства, включая ИСПДн и функционирующих в рамках систем сервисов в минимально возможные сроки, и минимизация негативного влияния на деятельность учреждения и субъектов персональных данных.

3. Применение

Требования настоящей Инструкции распространяются на:

3.1 Корпоративную сеть учреждения, включая сегменты ИСПДн.

3.2 Ответственному за процесс, отвечающему за бесперебойное и безопасное функционирование информационных систем (включая ИСПДн), сетей, сервисов и технологических процессов.

4. Ответственный за процесс

Ответственным за процесс является программист.

5. Общие сведения

5.1.Для учреждения важно применять структурный и плановый подход к обнаружению событий, инцидентов и инцидентов безопасности, их оценке, реагированию, извлечению уроков из инцидентов, введению превентивных защитных мер.

5.2. Перечень актуальных угроз для информационной системы персональных данных учреждения, которые могут приводить к появлению инцидентов безопасности, содержится в документе «Модель угроз безопасности информационных систем персональных данных учреждения».

6. Основные положения

6.1. Процедура обнаружения событий безопасности.

Событие может быть обнаружено человеком визуально, т. е. путем отслеживания сообщений об ошибках, чтения записей в файле аудита, а также в форме наблюдения за несанкционированным действием или нештатной ситуацией.

Событие может быть обнаружено конечным пользователем, эксплуатационным персоналом, функцией безопасности и т.д. Это может быть аварийный сигнал от антивирусной программы, аудиторской подсистемы, брандмауэра или системы обнаружения проникновения, от пожарной или охранной сигнализации и т.д.

К внешним обнаружениям событий можно отнести случаи, когда информация поступает, например:

из новостей;

от правоохранительных органов, которые уведомляют учреждение во время расследования преступления и др.

6.2. Процедура оповещения о событиях безопасности.

Сотрудники учреждения, ставшие свидетелями произошедшего события или инцидента безопасности, информируют об этом ответственного за информационную безопасность: какое событие произошло, какие приняты меры.

В других случаях события могут обнаруживать сами сервисные службы, которые получают аварийные сигналы от логических или физических датчиков, систем сбора, анализа и корреляции событий информационной безопасности, либо от внешних источников.

Когда событие обнаружено, должна производиться начальная оценка ситуации для подтверждения категории и серьезности.

6.3. Процедура сбора информации.

Сотрудник, обнаруживший событие или инцидент безопасности, должен собрать информацию о нем. При этом важны не только точность, но и своевременность.

Лицо, сообщающее о событии или инциденте безопасности, должно сообщить о нем как можно больше информации, доступной ему в тот момент, при необходимости, связаться со своим руководителем.

6.4. Первичная оценка и предварительное решение.

Первичная оценка должна быть выполнена сотрудником учреждения, получившим аварийный сигнал или другую информацию о событии или инциденте безопасности. Событие должно быть определено по принадлежности к одной из трех категорий:

инцидент безопасности;

событие;

ложный аварийный сигнал.

Если какое-либо событие не может быть отнесено к одной из категорий, указанных выше, то оно должно рассматриваться как инцидент.

Реакция на инцидент должна быть по возможности незамедлительной. Она предполагает начальное уведомление об инциденте в сервисную службу учреждения и первичную оценку ущерба.

Сервисной службой в зависимости от сложности и серьезности инцидента безопасности может быть принято решение о создании группы реагирования на инциденты безопасности.

6.5. Вторичная оценка и подтверждение инцидента. Эта оценка выполняется группой реагирования на инциденты безопасности (если создана) или сервисной службой. При этом лицо, принявшее информацию об инциденте безопасности, должно:

зарегистрировать инцидент в базе данных событий/инцидентов безопасности;

проанализировать содержание введенной информации;

собрать дополнительную информацию об инциденте (при необходимости).

Если все еще остается неопределенность относительно аутентичности инцидента ИБ или полноты полученной информации, то сотрудник сервисной службы должен провести вторичную оценку для определения того, является ли инцидент реальным или это ложная тревога. Если событие определено как ложная

тревога, отчет о событии ИБ должен быть завершен и передан специалисту по информационной безопасности или руководителю сервисной службы.

Если инцидент определяется как реальный, то сотрудник сервисной службы должен провести его дальнейшую оценку. При этом определить:
что представляет собой данный инцидент;

Вероятностная значимость/незначительность инцидента по следующей шкале классов:

Класс 1	Очень серьезно	Инцидент безопасности, который имеет значительные последствия для ГКОУ «С(к) ш№10» г. Орска, например, скоординированные атаки, проникновение в компьютер, кража уязвимостей и конфиденциальной информации и т.д. Инцидент безопасности, который подпадает под этот класс, требует значительных контрмер и приводит к значительному ущербу.
Класс 2	Серьезно	Инцидент безопасности, который имеет последствия для ГКОУ «С(к) ш№10» г. Орска, например, компьютерная диверсия, компьютерное мошенничество, злоупотребление корпоративной или пользовательской информацией или раскрытие информации.
Класс3	Менее серьезно	Инцидент попытки проникновения - неправильное использование компьютерных ресурсов и т. д. Инцидент, который попадает под этот класс, имеет меньшие последствия, требует незначительных контрмер и приводит к небольшому ущербу.
Класс 4	Без последствий	Инцидент, который может перерасти в инцидент другого класса (например, одиночный вирус). Инцидент, который попадает под этот класс, требует незначительных контрмер или не требует их вообще, приводит к небольшому ущербу или не приводит к ущербу.

- что явилось его причиной;
- чем или кем он вызван;
- на что повлиял или мог повлиять;
- как обрабатывался инцидент до сих пор.

При анализе потенциального или фактического негативного влияния инцидента безопасности на деятельность учреждения вследствие несанкционированного раскрытия информации, в том числе персональных данных, несанкционированной модификации информации, недоступности информации и/или сервиса, разрушения информации и/или сервиса необходимо подтвердить, какие последствия имели место. Примерные категории:

- финансовые потери;
- коммерческие и экономические интересы;
- ущерб субъектам персональных данных;

- потеря престижа учреждения.

Вся дополнительная информация должна быть внесена в отчет об инциденте.

6.6. Обработка инцидентов безопасности.

Когда инцидент безопасности входит в фазу обработки, обработка выполняется сотрудниками сервисных служб по следующему алгоритму:
определение типа инцидента, области его действия и последствий;

- локализация, т.е. остановка явления и ограничение последствий инцидента безопасности;
- ликвидация причины и предотвращение повторения;
- восстановление нормальной работы.

Если инцидент разрешен, то отчет должен содержать детали предпринятых защитных мер и любых извлеченных уроков, например, дополнительные защитные меры, которые следует предпринять для предотвращения повторного появления данного инцидента или ему подобного.

По результатам обработки инцидентов безопасности, ответственным сотрудником сервисной службы составляется отчет, содержащий данные о том, какие типы событий чаще встречались, по каким причинам возникли, как были обнаружены, их область действия, последствия и затраты. Отчет представляется на имя специалиста по информационной безопасности или руководителя сервисной службы.

Важным аспектом является регистрация событий, которые не являются инцидентами безопасности и их системное рассмотрение.

7. Ответственность

7.1. Ответственность за осуществление общего контроля выполнения правил настоящей Инструкции, а также за поддержание данного документа в актуальном состоянии несет ответственный за информационную безопасность.

7.2. Ответственность за доведение положений настоящего документа до сотрудников учреждения и иных лиц в части их касающейся, а также контроль соблюдения требований документа возлагается на ответственного за информационную безопасность.

7.3. Ответственность за выполнение Инструкции возлагается на всех сотрудников учреждения, а также на третьих лиц, использующих.

7.4. Указанные лица несут ответственность за ущерб, причиненный учреждению и субъектам персональных данных вследствие нарушения ими установленных требований в области обеспечения конфиденциальности информации, в соответствии с законодательством Российской Федерации.

7.5. На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования настоящей Инструкции, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы за неоднократное грубое нарушение правил работы в СКС.