Утверждаю
Директор МБОУ «Начальная
общеобразовательная школа № 14»
_____ Н.А. Зильберман
«25» 10 20 15

ИНСТРУКЦИЯ
по управлению событиями информационной безопасности

1. Введение.

1.1. Настоящая инструкция предназначена для обеспечения защиты информации, содержащейся в автоматизированной информационной системе МБОУ «Начальная общеобразовательная школа №14» (далее – АИС), в том числе персональных данных (далее – ПДн), при работе с событиями информационной безопасности.

1.2. Настоящая инструкция определяет:

1.2.1. перечень событий безопасности АИС, подлежащих регистрации и сроки их хранения;

1.2.2. состав и содержание информации о событиях безопасности, подлежащих регистрации;

1.2.3. порядок сбора, записи и хранения информации о событиях безопасности в течение определенного времени хранения;

1.2.4. порядок анализа зарегистрированных событий безопасности;

1.2.5. порядок защиты информации о событиях безопасности.

2. Перечень событий информационной безопасности АИС, подлежащих регистрации.

2.1. Перечень событий информационной безопасности АИС, подлежащих регистрации, составляет администратор безопасности и утверждает ответственный за защиту информации.

2.2. В перечень событий информационной безопасности АИС должны быть включены события безопасности, имеющие отношение к возможности реализации угроз безопасности информации, обрабатываемой в АИС, описанных в модели угроз безопасности информации.

2.3. В перечень событий безопасности АИС должны быть включены события безопасности, регистрируемые в журналах операционной системы технических средств АИС и средств защиты информации (далее – СЗИ), а также события, связанные с информационной безопасностью в инфраструктуре АИС.

3. Состав и содержание информации о событиях информационной безопасности.

3.1. Состав и содержание информации о событиях безопасности АИС, подлежащих регистрации, составляет администратор безопасности и утверждает ответственный за защиту информации.

3.2. Состав и содержание информации по каждому событию, включенному в список регистрации должны идентифицировать источник, время и результат события.

4. Порядок сбора, записи и хранения информации о событиях безопасности.

4.1. Настройку журналов регистрации событий информационной безопасности в программном обеспечении АИС и СЗИ осуществляет администратор системный АИС на основании предоставленных полномочий и администратор безопасности каждый в своей части. Настройка осуществляется на основе утвержденного перечня событий безопасности, подлежащих регистрации и перечня состава и содержания информации о событиях безопасности в соответствии с эксплуатационной документацией на программно – технические средства АИС.

4.2. Администраторы системные АИС и администратор безопасности должны не реже 1 раза в неделю просматривать журналы регистрации событий безопасности.

4.3. Настройки журналов регистрации событий информационной безопасности должны обеспечивать запись в память технических средств АИС и СЗИ информации о поступающих событиях безопасности без переполнения памяти в течение 1 месяца.

4.4. Информация о событиях безопасности в АИС, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана) должна фиксироваться администратором безопасности при ее обнаружении в журнале организационных событий безопасности.

5. Порядок анализа зарегистрированных событий безопасности.

5.1. При просмотре и сохранении журналов регистрации событий безопасности и при регистрации организационных событий информационной безопасности администратор безопасности должен анализировать события на наличие инцидентов. При подозрении на инцидент администратор безопасности действует в соответствии с разделом 2 «Положения по защите информации».

5.2. Администратор безопасности должен подробно исследовать наиболее часто повторяющиеся события безопасности, выяснить причины их возникновения и устранить эти причины.

5.3. На основании регистрируемой и сохраняемой информации о событиях информационной безопасности в АИС администратор безопасности один раз в 3 месяца (квартал) составляет отчет о событиях

безопасности и передает его ответственному за защиту информации для анализа защищенности АИС.

6. Порядок защиты информации о событиях безопасности.

6.1. Права доступа к файлам отчетов журналов безопасности и настройкам журналов установлены администратору безопасности и администраторам системным АИС и отражены в матрице доступа.

6.2. На информацию о событиях информационной безопасности распространяются все требования к защите информации в соответствии с «Положением по защите информации».

7. Заключительные положения.

7.1. Администратор безопасности и администраторы системные АИС должны быть предупреждены об ответственности за действия, нарушающие требования настоящей инструкции.

7.2. Администратор безопасности и администраторы системные АИС должны быть ознакомлены с настоящей инструкцией до начала работы с АИС под роспись. Обязанность ознакомления администратора безопасности и администраторов системных АИС с настоящей инструкцией лежит на ответственном за защиту информации.

8. Нормативные и правовые документы.

1.1. Методический документ, утвержден ФСТЭК России 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.2. Приказ ФСТЭК России от 18.02.2013 года №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.4. Постановление правительства РФ от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Подготовил:
Администратор безопасности информации _____ О.И. Шаталова