Муниципальное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа № 18 с углубленным изучением
отдельных предметов города Невинномысска

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Управляющим советом	Директор МБОУ СОШ № 18
МБОУ СОШ № 18	города Невинномысска
города Невинномысска	_____ Г.И. Голоюх
(протокол от 29.07.2016 г. №5)	(приказ от 16.08.2016 г. №184-о/д)

Политика
по работе с инцидентами информационной безопасности муниципального бюджетного общеобразовательного учреждения средняя общеобразовательная школа №18 с углубленным изучением отдельных предметов города Невинномысска

1. Общие положения

1.1. Настоящая Политика развивает положения «Политики информационной безопасности муниципального бюджетного общеобразовательного учреждения средняя общеобразовательная школа №18 с углубленным изучением отдельных предметов города Невинномысска (далее – Учреждение).

1.2. Целью настоящей Политики является установление общих руководящих принципов наблюдения состояния информационной безопасности (далее - ИБ) и использования результатов для осуществления менеджмента инцидентами ИБ.

1.3. Настоящая Политика распространяется на все технологические процессы Учреждения и обязательна для применения всеми работниками Учреждения.

1.4. Мероприятия по обеспечению ИБ Учреждения, выполняемые с

целью реализации требований настоящей Политики, утверждаются внутренними нормативными документами в соответствии с установленным в Учреждении порядком.

2. Список терминов и определений

2.1. **Активы Учреждения** – все, что имеет ценность для Учреждения и находится в его распоряжении.

2.2. **Работники Учреждения** - преподавательский состав, административный и вспомогательный персонал образовательного учреждения.

К активам Учреждения относятся:

- преподавательский и рабочий персонал, финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.;
- различные виды информации - платежная, финансово-аналитическая, служебная, управляющая, персональные данные и пр.;
- Технологические процессы;
- Продукты и услуги, предоставляемые обучающимся и их родителям;

2.3. **Технологический процесс** – технологический процесс, содержащий операции по изменению и (или) определению состояния информации, используемой при функционировании автоматизированных систем Учреждения или необходимой для реализации услуг.

2.4. **Комиссия для расследования инцидентов информационной безопасности** (далее - Комиссия) – действующая на постоянной (временной) основе группа работников Учреждения, которая выполняет процедуры менеджмента инцидентами ИБ в течение их жизненного цикла.

Комиссия способствует оперативному реагированию на инциденты ИБ, в том числе за счет независимости применяемых процедур и средств вычислительной техники от компонентов информационной инфраструктуры Учреждения.

2.5. **Информационно-технологический актив** (далее - ИТ-актив) –

актив Учреждения, к которому относятся:

- информационные активы;
- программные средства;
- аппаратные и программно-аппаратные средства.

2.6. **Информационный актив** – информация с позволяющими ее идентифицировать реквизитами, имеющая ценность для Учреждения, находящаяся в его распоряжении, представленная в виде документов на бумажном носителе, а также в виде электронных копий, пригодных для обработки.

2.7. **Инцидент ИБ** – рисковое событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

Реализация угрозы ИБ – это нарушение свойств ИБ (конфиденциальности, целостности или доступности) информационных активов Учреждения.

Нарушение может вызываться источниками угроз ИБ, либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств, природными факторами), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов.

2.8. **Менеджмент инцидентов ИБ** – деятельность по своевременному обнаружению инцидентов ИБ, адекватному и оперативному реагированию на них в интересах минимизации и/или ликвидации негативных последствий для Учреждения (включая нарушение непрерывности технологических процессов) при нарушениях ИБ.

2.9. **Рисковое событие** – реализовавшееся событие, обусловленное операционным риском, повлекшее или способное повлечь за собой операционные потери Учреждения и произошедшее по причине ошибочности или сбоя процессов, действий людей и систем, а также по причине внешних событий.

2.10. **Событие ИБ** – изменение состояния объекта или области мониторинга ИБ, подлежащее регистрации средствами мониторинга ИБ.

3. Перечень сокращений

АС – автоматизированная система.

БД – база данных.

ИТ – информационные технологии.

ИТ-актив – информационно-технологический актив.

ИБ – информационная безопасность.

4. Общие положения по организации мониторинга ИБ и менеджмента инцидентов ИБ

4.1. Организация мониторинга ИБ

4.1.1. Мониторинг ИБ в Учреждении осуществляется с целью своевременного выявления фактов, оказывающих негативное воздействие на ИТ-активы Учреждения. Указанная цель достигается путем решения следующих задач:

- своевременное выявление угроз ИБ, как внешних, так и внутренних, способных нанести ущерб Учреждению, а также условий и факторов их реализации;
- выявление уязвимостей в сфере ИБ;
- выявление злоумышленных или несанкционированных (выполненных с нарушением установленных правил и прав) действий работников Учреждения и обучающихся (внутренних нарушителей);
- контроль выполнения требований внутренних нормативных и организационно-распорядительных документов Учреждения по обеспечению ИБ.

4.1.2. Перечень ИТ-активов Учреждения, являющихся объектами мониторинга ИБ, и целесообразность изменения состава этого перечня определяются на основании:

- требований законодательства Российской Федерации и внутренних нормативных документов Учреждения;

- результатов оценки важности ИТ-активов Учреждения;
- результатов оценки рисков ИБ Учреждения;
- необходимости контроля состояния защитных мер ИБ;
- технических возможностей потенциальных объектов мониторинга.

Состав перечня ИТ-активов, являющихся объектами мониторинга ИБ, и параметры мониторинга ИБ устанавливаются ответственным и согласовываются с руководителем Учреждения.

4.1.3. Планирование и реализация мероприятий по осуществлению мониторинга ИБ и реагированию на инциденты ИБ выполняется ответственным.

4.1.4. Во внутренних нормативных документах Учреждения должны быть определены условия и временные периоды хранения информации, собранной в процессе мониторинга ИБ.

4.1.5. Доступ к информации мониторинга ИБ должен быть ограничен. Список лиц, допущенных к информации мониторинга ИБ, должен быть определен ответственным.

4.2. Организация менеджмента инцидентов ИБ

4.2.1. Менеджмент инцидентов ИБ должен основываться на результатах мониторинга ИБ.

4.2.2. Основными целями менеджмента инцидентов ИБ являются:

- своевременное обнаружение инцидентов ИБ;
- адекватное и оперативное реагирование на них в интересах предотвращения реализации угроз ИБ;
- минимизация операционных рисков ИБ;
- минимизация и/или ликвидация негативных последствий для Учреждения (включая нарушение непрерывности технологических процессов) при нарушениях ИБ.

4.2.3. Менеджмент инцидентов ИБ должен поддерживаться в Учреждении совокупностью нормативно-правовых, организационных и технических мер.

4.2.4. Для исключения и/или минимизации негативных последствий

инцидентов ИБ на технологические процессы должна поддерживаться согласованность процедур менеджмента инцидентов ИБ с процедурами менеджмента рисков ИБ, процедурами управления операционными рисками, а также с процедурами по обеспечению непрерывности технологических процессов.

4.2.5. Работники Учреждения должны быть проинструктированы на основании материалов, подготавливаемых Ответственным за обработку персональных данных, о возможных инцидентах ИБ и относительно порядка действий в условиях их реализации.

4.2.6. Деятельность в рамках менеджмента инцидентов ИБ должна осуществляться как оперативный, непрерывный и автоматизированный процесс.

4.2.7. Сбор информации в процессе управления инцидентом ИБ, расследование причин возникновения инцидентов ИБ и выявление нарушителей ИБ, а также применение дисциплинарных и административных мер должны осуществляться с соблюдением законодательства Российской Федерации и договорных обязательств Учреждения.

5. Реализация положений настоящей Частной политики

5.1. Критерии идентификации и оценки инцидентов ИБ

5.1.1. Причинами инцидентов ИБ в Учреждении могут являться действия, техногенных, антропогенных, природных факторов. По отношению к Учреждению эти факторы могут быть как внешними, так и внутренними, а их действие носить как случайный, так и умышленный характер.

5.1.2. Для целей идентификации и классификации инцидентов ИБ, а также выбора способов и методов последующего управления ими должны применяться следующие критерии:

- локализация воздействия, которая характеризует локальный или распределенный характер воздействия;
- масштаб (число ИТ-активов, на которые негативно повлиял или может повлиять инцидент ИБ);

- вовлеченные ИТ-активы (например, резервные копии данных, коммуникационное оборудование, программные средства электронной почты);
- связанные с инцидентом области ИБ (например, защита от вредоносных программ, управлением доступом);
- продолжительность, определяющая длительность и/или определенную последовательность нежелательных действий/событий во времени;
- вовлеченные в инцидент ИБ работники Учреждения, посторонние лица и их роль в инциденте (например, лицо, обнаружившее инцидент; предполагаемые нарушитель, владелец ИТ-актива);
- источник воздействия – природное явление, техногенный фактор или человеческий фактор;
- нарушаемые в результате инцидента свойства безопасности ИТ-активов, а также технологические процессы, непрерывность которых нарушена;
- степень опасности: оцениваются потенциальные негативные последствия для Учреждения, рассчитываемые исходя из степени потенциального или явного воздействия последствий инцидента на технологические процессы;
- категория потерь – прямые финансовые и/или материальные потери Учреждения, ущерб здоровью персонала, ущерб репутации Учреждения, снижение доверия к Учреждению со стороны заинтересованных лиц, нарушение законодательства РФ и договорных обязательств и т.д.;
- приоритет – степень срочности требуемого отклика на инцидент ИБ;
- объем имеющейся информации об инциденте.

Приведенный перечень критериев может быть при необходимости уточнен в рамках процесса планирования и подготовки менеджмента инцидентов ИБ.

5.2. **Роли и ответственность**

5.2.1. Для обеспечения процессов и процедур мониторинга и

менеджмента инцидентов ИБ и минимизации воздействия инцидента на основную деятельность в Учреждении создается Комиссия.

5.2.2. Допускается совмещение одним работником Учреждения исполнения роли члена Комиссии с исполнением других ролей ИБ. Не допускается исполнение роли члена Комиссии лицом, в отношении которого проводится расследование.

5.2.3. Работники Учреждения могут быть включены в состав Комиссии как обязательные эксперты на постоянной основе или как привлекаемые эксперты по мере необходимости. Постоянными членами Комиссии являются руководитель группы (работник ответственного подразделения), несущий ответственность за организацию и координацию всех работ, а также работники ответственного подразделения, непосредственно выполняющие различные процедуры по обеспечению ИБ.

5.2.4. В функции обязательных экспертов Комиссии входит:

- участие в следующих процессах:
  - согласования с ответственным за обработку персональных данных деятельности по управлению инцидентами ИБ;
  - выбора критериев классификации инцидентов ИБ;
  - разработки операционных процедур менеджмента инцидентов ИБ;
  - проверки и тестирования процессов и процедур менеджмента инцидентов ИБ;
- сбор и регистрация информации о событиях, связанных с обеспечением ИБ, полученной из различных источников, включая:
  - информацию мониторинга ИБ;
  - результаты анализа информации мониторинга ИБ;
  - информацию об инцидентах ИБ, получаемую от работников Учреждения обучающихся и их родителей;
- контроль процесса мониторинга ИБ в целях его планирования и дальнейшего совершенствования, а именно:
  - выявление и регистрация инцидентов ИБ;
  - анализ инцидентов ИБ, определение и регистрация их

характеристик (масштаб, воздействие, вовлеченные лица и др.), идентификация инцидентов ИБ на основе критериев классификации, оценка инцидентов ИБ, планирование дальнейших действий по управлению конкретным инцидентом ИБ на основе предварительного плана для соответствующего класса инцидентов ИБ;

- регистрация инцидента ИБ в качестве рискового события операционного риска в соответствии с порядком, определенным в соответствующих внутренних нормативных документах Учреждения;

- оповещение об инцидентах ИБ лиц, заинтересованных в обеспечении ИБ, организация, координирование и регистрация действий по управлению инцидентами ИБ, а также участие в данных действиях в рамках своей компетенции;

- организация расследования инцидента ИБ и (или) участие в расследовании инцидента ИБ (выявление причин, вызвавших инцидент, анализ и оценка эффективности и адекватности мер, предпринимаемых исполнителями соответствующих ролей в рамках своей компетенции), в частности, сбор, регистрация и анализ дополнительных сведений об инциденте ИБ;

- участие в процессах пересмотра и улучшения менеджмента инцидентов ИБ, включая:

- подготовку информационных материалов для проведения оценки эффективности менеджмента инцидентов ИБ;

- участие в проведении оценки эффективности менеджмента инцидентов ИБ;

- формирование предложений по повышению качества менеджмента инцидентов ИБ;

- реализацию принятых решений по улучшению менеджмента инцидентов ИБ в пределах своей компетенции;

- администрирование и использование инструментальных средств автоматизации менеджмента инцидентов ИБ.

5.2.5. Главная задача Комиссии состоит в реализации процедур

мониторинга и менеджмента инцидентов ИБ, кроме того на Комиссию может быть возложен и ряд других задач, таких как:

- разработка рекомендаций по ИБ;
- мониторинг уязвимости сетей, систем и приложений;
- обнаружение вторжений;
- повышение осведомленности персонала Учреждения в сфере ИБ;
- исследование тенденций развития ИБ в целях выявления новых угроз;
- менеджмент изменений и обновлений сетей, систем и приложений.

5.3. **Процедуры мониторинга ИБ, проводимые с использованием программно-технических средств**

5.3.1. Сбор и фильтрация информации мониторинга.

5.3.1.1. При проведении мониторинга ИБ с использованием программно-технических средств источниками информации мониторинга ИБ должны быть журналы регистрации событий (аудита) штатных систем, регистрации событий контролируемых объектов, входящих в состав прикладных и общесистемных продуктов и платформ, и/или специализированные средства сбора информации о событиях ИБ.

5.3.1.2. Регистрации событий ИБ обеспечивается путём:

- защиты от неавторизованного отключения средств регистрации событий ИБ;
- защиты от неавторизованного изменения списка регистрируемых событий ИБ;
- защиты от неавторизованного редактирования или удаления файлов с записями информации мониторинга (журналов регистрации событий ИБ);
- сохранения архива файлов с записями журналов регистрации событий ИБ.

5.3.2. Администрирование базы данных мониторинга должно включать следующие операции:

- архивирование БД мониторинга;

- резервное копирование БД мониторинга;
- восстановление архивных и резервных копий БД мониторинга.

5.3.3. Сохраненная в БД информация мониторинга в дальнейшем может использоваться как доказательства инцидентов ИБ при анализе этих инцидентов.

5.3.4. Анализ информации мониторинга

5.3.4.1. В ходе анализа множества собранных событий ИБ выявляется множество параметров, характеризующих действия/поведение/состояние объектов мониторинга. Анализ выявленных параметров выполняется по правилам (критериям мониторинга ИБ), применение которых обеспечивает решение следующих задач мониторинга:

- оперативное выявление событий ИБ, свидетельствующих об инцидентах ИБ, в целях их последующего использования в рамках менеджмента инцидентов ИБ;
- оперативное выявление фактов нарушения функционирования и/или нештатного функционирования средств обеспечения ИБ (защитных мер);
- наблюдение за действиями пользователей систем и средств, находящихся во владении и/или под управлением (в распоряжении) Учреждения, с целью контроля соблюдения ими норм и требований ИБ, установленных в Учреждении;
- наблюдение за состоянием ИТ- активов и поведением участников информационных технологических процессов (в т.ч. внешних по отношению к ней субъектов) с целью выявления их нетипичного состояния/поведения, представляющего опасность для информационных активов или для ее деятельности в целом;
- наблюдение за критичными для Учреждения ИТ-активами в интересах обеспечения непрерывности технологических процессов.

5.3.4.2. Применяемые программно-технические средства мониторинга должны обеспечивать возможность проведения анализа данных мониторинга в оперативном режиме, а также на основе информации из архивной БД мониторинга по запросам уполномоченных сотрудников Комиссии (за

прошедший период).

5.3.5. Контроль и пересмотр процедур мониторинга ИБ.

5.3.5.1. Контроль и пересмотр процедур мониторинга ИБ, применяемых средств мониторинга должно производиться по результатам анализа и оценки эффективности функционирования средств мониторинга ИБ, их адекватности требованиям по своевременному выявлению и идентификации инцидентов ИБ, связанных с контролируемыми объектами.

5.3.5.2. Пересмотр должен выполняться периодически, в плановом порядке, не реже одного раза в год или во внеплановом порядке при необходимости.

5.3.6. Процедура улучшения.

5.3.6.1. В рамках этой процедуры должно проводиться изменение параметров и критериев мониторинга ИБ, совершенствование средств сбора и анализа информации мониторинга на основании результатов оценки эффективности мониторинга, изменения задач мониторинга, изменения состава и свойств контролируемых ИТ- активов.

5.4. **Процедуры мониторинга ИБ, проводимые на основе организационных мер**

5.4.1. Отслеживание изменений нормативно-правовой базы в области ИБ. Требования по обеспечению ИБ в Учреждении определяются в частности:

- законодательством Российской Федерации;
- международными актами и межгосударственными соглашениями;
- законодательством государств, с резидентами которых Учреждение осуществляет взаимодействие;
- стандартами (межгосударственными и Российской Федерации);
- внутренними нормативными документами Учреждения.

5.4.2. Проверка соблюдения процедур ИБ работниками Учреждения.

Контроль соблюдения процедур ИБ организационными мерами проводится в целях выявления нарушений ИБ работниками Учреждения в форме проверок деятельности структурных подразделений и отдельных

работников. Указанный контроль должен быть направлен на:

- наличие и достаточность документов, регламентирующих в Учреждении деятельность в области обеспечения ИБ;
- соблюдение процедур хранения, использования и уничтожения носителей конфиденциальной информации и документов, содержащих сведения ограниченного доступа;
- использование работниками Учреждения при выполнении своих должностных обязанностей документов, регламентирующих деятельность в области обеспечения ИБ;
- соблюдение работниками Учреждения и обучающимися правил по ИБ в случае необходимости выполнения своих обязанностей, обучения за пределами установленной продолжительности рабочего времени и состояния рабочего места (мест обучения);
- соблюдение работниками Учреждения процедур использования съемных машинных носителей информации;
- соблюдение договорных обязательств (соглашений) в части обеспечения ИБ.

5.4.3. Результаты мониторинга ИБ организационными мерами должны использоваться для принятия решений, направленных на формирование и реализацию корректирующих и превентивных действий по совершенствованию системы менеджмента инцидентов ИБ, в том числе для выработки предложений по повышению эффективности организационных мер проведения мониторинга.

5.5. **Планирование и подготовка менеджмента инцидентов ИБ**

В рамках процесса планирования и подготовки менеджмента инцидентов ИБ ответственным должно быть предусмотрено выполнение следующих процедур:

- разработка и документирование организационных мер и программно-технических средств управления инцидентами ИБ. Формы, процедуры и инструменты поддержки для обнаружения, оповещения, оценки и

реагирования на инциденты ИБ должны быть изложены в соответствующих внутренних нормативных документах Учреждения;

- распределение ролей и назначение ответственных исполнителей по выполнению процедур менеджмента инцидентов ИБ;
- обеспечение осведомленности исполнителей ролей ИБ по вопросам выполнения процедур менеджмента инцидентов ИБ;
- обеспечение исполнителей ролей менеджмента инцидентов ИБ необходимыми ресурсами для выполнения процедур менеджмента инцидентов ИБ;
- выработка (уточнение) критериев, используемых для идентификации и оценки инцидента ИБ;
- определение/уточнение перечня новых инцидентов, подлежащих выявлению. Выбор может основываться на результатах оценки рисков ИБ Учреждения;
- разработка планов по управлению различными инцидентами ИБ с участием всех заинтересованных самостоятельных структурных подразделений Учреждения и их согласование (при необходимости) с планами обеспечения непрерывности технологических процессов и процедурами управления операционными рисками Учреждения;
- проверка и тестирование процессов и процедур менеджмента инцидентов ИБ;
- составление форм сообщений и отчетов об инцидентах ИБ;
- оповещение персонала Учреждения и других организаций, чьи информационные ресурсы находятся во владении (распоряжении) Учреждения, о том, что они находятся в зоне действия процедур управления инцидентами ИБ.

5.6. **Реализация (использование) менеджмента инцидентов ИБ**

5.6.1. Обнаружение и фиксирование инцидентов ИБ

5.6.1.1. Своевременное обнаружение и фиксирование всех инцидентов ИБ должно основываться на сборе и анализе необходимой для этого

информации, а также на выявлении тенденций, указывающих на негативное развитие ситуации, связанной с идентифицированным инцидентом ИБ.

5.6.1.2. Инициирование процедур менеджмента инцидентов ИБ должно выполняться:

- в оперативном режиме по данным систем/средств мониторинга;
- после получения сообщения об инциденте ИБ.
- по запросам заинтересованных лиц (руководства, администраторов ИБ и др.) данных об инцидентах ИБ за любой прошедший период.

5.6.1.3. Источниками информации об инцидентах ИБ являются:

- системы/средства мониторинга ИБ;
- программные (технические) средства обнаружения вторжений;
- антивирусное программное обеспечение;
- средства регистрации событий операционных систем, услуг и приложений;
- средства регистрации событий активного сетевого оборудования;
- устройства сигнализации;
- работники Учреждения (пользователи систем/средств, администраторы ИБ, администраторы систем);
- работники других организаций, имеющие доступ к информационным активам, находящимся под управлением (в распоряжении) Учреждения.

5.6.1.4. Для обнаружения инцидентов ИБ должны реализовываться механизмы мониторинга ИБ Учреждения.

5.6.1.5. Для обнаружения и фиксирования инцидентов ИБ должны применяться специализированные инструментальные средства, обеспечивающие возможность фиксирования работниками Учреждения, а также, при необходимости, работниками других организаций, информация об инцидентах ИБ при помощи специализированных форм регистрации.

5.6.1.6. Вся информация об инцидентах ИБ, полученная от различных источников, должна быть сохранена в отдельной базе данных. Эта информация может быть в дальнейшем использована для анализа и проведения

расследования инцидента ИБ.

5.6.2. Анализ и оценка инцидентов ИБ

5.6.2.1. Анализ и оценка (по степени опасности) идентифицированных инцидентов ИБ проводится с целью выявления среди них инцидентов, представляющих непосредственную угрозу ИБ Учреждения.

5.6.2.2. Для анализа и оценки инцидентов ИБ используется информация из хранилища данных об инцидентах ИБ, позволяющая определить источник и детальные характеристики инцидента ИБ.

5.6.2.3. В ходе анализа и оценки инцидентов ИБ определяется их приоритетность и действия по управлению в соответствии с установленными критериями для предотвращения и/или минимизации возможных негативных последствий (ущерба) для Учреждения.

5.6.2.4. Менеджмент инцидентов ИБ должен выполняться в соответствии со следующими установленными приоритетами:

- приоритет № 1 – обеспечение здоровья и безопасности работников Учреждения, обучающихся и их родителей;
- приоритет № 2 – обеспечение непрерывности технологических процессов;
- приоритет № 3 – обеспечение требуемых свойств безопасности ИТ-активов;
- приоритет № 4 – минимизация финансовых и материальных потерь (в т. ч., связанных с нарушением договорных обязательств);
- приоритет № 5 – соблюдение законодательства РФ и требований регулирующих органов;
- приоритет № 6 – поддержание деловой репутации Учреждения.

5.6.3. Сообщение (оповещение) об инциденте ИБ

5.6.3.1. Работники Учреждения должны быть проинструктированы о процедурах оповещения об инцидентах ИБ различных типов.

5.6.3.2. Сообщение об инциденте ИБ должно содержать следующие основные параметры:

- информацию о факте обнаружения инцидента ИБ;

- краткое описание инцидента ИБ с указанием вовлеченных в инцидент ИТ- активов;
- действия, предпринятые членами Комиссии в отношении этого инцидента ИБ;
- контактную информацию для заинтересованных сторон (например, владельцев ИТ-актива, системных администраторов ИБ);
- комментарии членов Комиссии;
- перечень мер, которые должны быть предприняты для нейтрализации инцидента ИБ.

5.6.4. Сбор и регистрация информации об инциденте ИБ и о действиях по управлению этим инцидентом.

5.6.4.1. Сбор и регистрация информации об инциденте ИБ и действиях по управлению этим инцидентом проводится для поддержания процедур последующего анализа и расследования (при необходимости) и выработки мер по совершенствованию деятельности по обеспечению ИБ.

5.6.4.2. Сообщение об инциденте ИБ и другая дополнительная информация, включающая доказательства (свидетельства) инцидента ИБ, собранная автоматизированными и организационными способами, должны быть оформлены и сохранены. При этом должна сохраняться информация, относящаяся к инциденту ИБ, необходимая для его дальнейшего анализа, формирования отчета об инциденте ИБ и потенциального использования в качестве свидетельства в дисциплинарных процессах.

5.6.4.3. Вся информация об инцидентах ИБ и действиях по управлению ими должна быть сохранена в базе данных инцидентов ИБ. По ходу выполнения анализа и процедур реагирования на инцидент ИБ, данные об инциденте ИБ в базе данных должны обновляться. Указанные действия должен осуществлять ответственный за обработку персональных данных (администратор информационных ресурсов Учреждения).

5.6.4.4. На инциденты ИБ распространяются требования действующего в Учреждении порядка регистрации рисковых событий.

5.6.4.5. Управление информацией об инцидентах ИБ и действиях по

управлению ими включает:

- определение места, условий и времени оперативного и архивного хранения данных;
- документирование инструкций и описаний инструментов и правил выполнения резервирования, дублирования, архивирования и порядок доступа к архивным и резервным копиям;
- обеспечение конфиденциальности, целостности и доступности данных;
- обеспечение доступа к данным только авторизованным лицам.

5.6.5. Действия ответственного за обработку персональных данных по управлению инцидентом ИБ.

5.6.5.1. Сдерживание/предотвращение:

- после обнаружения и оценки инцидента ИБ необходимо предпринять все необходимые и доступные меры по сдерживанию/пресечению распространения негативного воздействия на ИТ-активы Учреждения;
- для обеспечения своевременной и эффективной реакции на выявленный инцидент ИБ должны быть разработаны соответствующие действия и защитные меры по сдерживанию/пресечению инцидента ИБ. Действия по сдерживанию должны зависеть от типа инцидента ИБ и должны выполняться в соответствии с установленным регламентом и планом по управлению каждым из основных типов инцидентов. Процедуры сдерживания инцидента ИБ должны учитывать потенциальный ущерб ИТ - активам от инцидента; время и ресурсы, необходимые для сдерживания; эффективность сдерживания (частичное или полное сдерживание инцидента).

5.6.5.2. Расследование инцидента ИБ:

- процедура расследования предназначена для выявления, в том числе с применением организационных процедур, причин (условий и факторов), вызвавших инцидент ИБ, и/или негативную тенденцию развития связанной с этим инцидентом ИБ ситуации, а также анализа и оценки адекватности и эффективности действий, предпринятых в Учреждении, по

управлению инцидентом ИБ;

- процедура расследования инцидента ИБ может включать идентификацию нарушителя ИБ по данным, собранным при обнаружении инцидента ИБ, а также при необходимости эскалацию инцидента ИБ. Уровень эскалации инцидента ИБ выбирает руководитель Комиссии на основании возможных операционных потерь Учреждения.

5.6.5.3. Восстановление (устранение последствий):

- процедуры восстановления ИТ-активов, которым был нанесен ущерб, служат для минимизации или ликвидации (по возможности) негативных последствий от инцидентов ИБ и зависят от типа инцидента ИБ. Процедуры определяются на этапе планирования для каждого типа инцидентов ИБ и реализуются с учетом доступных ресурсов и потребностей (частичное или полное восстановление);
- деятельность по восстановлению после инцидентов ИБ должна быть согласована с планами обеспечения непрерывности технологических процессов и может быть делегирована для выполнения соответствующим системным администраторам ИБ и/или администраторам систем.

5.6.5.4. Закрытие (разрешение) инцидента ИБ:

- после выполнения всех необходимых действий по анализу, оценке и реагированию инцидент ИБ должен быть закрыт (разрешен);
- решение о закрытии (разрешении) инцидента ИБ может быть принято не только при выполнении процедур реагирования на инцидент, но и ранее – при анализе инцидента, и позже – при оценке инцидента. Решение о закрытии (разрешении) инцидента ИБ должен принимать руководитель Комиссии.

5.7. Пересмотр процессов менеджмента инцидентов ИБ

5.7.1. Процедуры пересмотра и улучшения процессов менеджмента инцидентов ИБ должны выполняться как на регулярной основе (периодически), так и по результатам применения их для любого существенного инцидента ИБ (при необходимости).

5.7.2. Оценка процедур и процессов менеджмента инцидента ИБ включает:

- просмотр документов и отчетов по инциденту ИБ и оценку их полноты;
- рассмотрение эффективности мониторинга ИБ для регистрации инцидента ИБ;
- оценку ущерба от инцидента ИБ;
- определение достаточности принятых мер и ресурсов по управлению инцидентом ИБ;
- оценку адекватности планов и процедур реагирования на инциденты ИБ;
- прогноз мер, которые могли бы предотвратить инцидент ИБ.

5.7.3. Завершающий отчет по инциденту ИБ должен включать информацию, которая может быть использована в будущем при выполнении процедур менеджмента инцидентов ИБ. Также отчет может служить основой для оценки ущерба от инцидента ИБ для дальнейшего дисциплинарного процесса.

В отчете об инциденте ИБ должны быть отражены:

- дата, время и место инцидента ИБ;
- сведения о работнике, выявившем инцидент ИБ, информацию об инциденте ИБ, описание предпринятых действий и мер при обнаружении инцидента (включая использованные инструментальные средства) с обоснованием;
- место хранения свидетельства (информации, показаний) инцидента ИБ, способа архивирования, способа защиты и доступа к нему.

5.7.4. Отчет об инциденте ИБ должен сохраняться в базе данных инцидентов ИБ.

5.7.5. Результаты анализа и оценки инцидентов ИБ после их всестороннего исследования могут быть использованы для принятия решений, направленных на выбор и реализацию мер по совершенствованию менеджмента инцидентов ИБ, оценке рисков ИБ, по подготовке предложений

по улучшению ИБ, обновлению и/или реализации новых защитных мер ИБ.

5.7.6. Предложения по улучшению менеджмента инцидентов ИБ могут касаться:

- изменения или подготовки новых требований к защитным мерам ИБ (программно-техническим и организационным);
- пересмотра политик, стандартов, процедур и регламентирующих документов ИБ;
- изменений в политике менеджмента инцидентов ИБ, а также в процессах, процедурах управления инцидентами ИБ и в отчетных формах;
- подготовки новых организационно-распорядительных документов (мероприятий).
- изменения конфигурации аппаратных и программных средств ИТ-блока и системы менеджмента ИБ;
- разработки новых организационных мер обеспечения ИБ;
- перераспределения финансовых затрат на обеспечение ИБ.

5.8. Улучшение менеджмента инцидентов ИБ

Улучшение менеджмента безопасности должно заключаться в следующем:

- введении новых или изменении действующих защитных мер ИБ, доработке внутренних нормативных документов ИБ, изменении конфигурации аппаратного и программного обеспечения;
- введении в действие усовершенствованных процедур менеджмента инцидентов ИБ и документов, новых отчетных форм и их тестировании до ввода в эксплуатацию.

6. Контроль за соблюдением требований настоящей политики

Контроль за соблюдением настоящей политики осуществляет ответственный за обработку персональных данных на основе проведения мониторинга и оценки состояния ИБ, а также в рамках иных контрольных

мероприятий.

7. Ответственность за несоблюдение требований настоящей политики

Ответственность за несоблюдение требований настоящей политики, повлекших за собой разглашение или утрату информации ограниченного доступа, определяется законодательством РФ, внутренними нормативными документами Учреждения, а также должностными инструкциями работников Учреждения.

8. Заключительные положения

8.1. Настоящая Политика вступает в силу с даты ее утверждения.

8.2. Ответственность за поддержание настоящей Политики в актуальном состоянии, создание, внедрение, координацию процессов системы менеджмента инцидентов ИБ и внесение изменений в процессы системы менеджмента инцидентов ИБ возлагается на руководителя Учреждения.

8.3. В случае изменения законодательства РФ, изменения или введения в действие стандартов, нормативных методических рекомендаций, требований уполномоченных органов настоящая Политика применяется в части, не противоречащей вновь принятым нормативным документам. При необходимости ответственное подразделение незамедлительно инициирует внесение соответствующих изменений в настоящую Политику в установленном в Учреждении порядке.

8.4. Внесение изменений в настоящую Политику должно осуществляться на периодической и внеплановой основе:

- периодическое внесение изменений не реже одного раза в 24 месяца;
- внеплановое внесение изменений может проводиться по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий.