УТВЕРЖДАЮ
Директор КГКОУ ШИ 3

_____ Н.А. Васильева

«04» декабря 2018 года

П О Л И Т И К А

по обеспечению информационной безопасности Краевого государственного казенного общеобразовательного учреждения для детей-сирот и детей, оставшихся без попечения родителей, реализующее адаптированные основные общеобразовательные программы «Школа-интернат № 3»

г. Хабаровск, 2018

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящей Политике используются следующие термины и определения:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Анализ уязвимостей – мероприятия по выявлению, идентификации и оценке уязвимостей информационной системы в интересах определения возможности реализации угроз безопасности информации и способов предотвращения ущерба.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе).

Безопасность информации (данных) – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

Доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

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.

Информационные ресурсы – совокупность данных, организованных для эффективного получения достоверной информации; документы и массивы документов в информационных системах.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами. Ограничение доступа к информации регламентировано статьей 9 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Инцидент информационной безопасности – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Компонент информационной системы – часть информационной системы, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

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

Локальный доступ – доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту информационной системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).

Многофакторная аутентификация – аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Оператор информационной системы персональных данных (Оператор) – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационных систем персональных данных, в том числе по обработке и защите персональных данных, содержащихся в ее базах данных.

Объект доступа – единица информационного ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) и хранимая в информационных системах в электронном виде.

Привилегированные пользователи – пользователи из состава администраторов, а также Ответственный за организацию обработки персональных данных.

Роль – предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой.

Событие безопасности – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

Удаленный доступ – процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

Угроза – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

Уязвимость – недостаток (слабость) информационной системы, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

Целостность – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	–	Автоматизированное рабочее место
АС	–	Автоматизированная система
БД	–	База данных
ВПр	–	Вредоносные программы (вирусы)
ГОСТ	–	Государственный стандарт
ИБ	–	Информационная безопасность
ИР	–	Информационные ресурсы
ИС	–	Информационная система
ИСПДн	–	Информационная система персональных данных
КЗ	–	Контролируемая зона
ЛВС	–	Локальная вычислительная сеть
МНИ	–	Машинные носители информации
МЭ	–	Межсетевые экраны
НДВ	–	Недекларированные возможности
НСД	–	Несанкционированный доступ
ОРД	–	Организационно-распорядительные документы
ОС	–	Операционная система
ПАК	–	Программно-аппаратный комплекс
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
РД	–	Руководящий документ
СВТ	–	Средства вычислительной техники
СЗИ	–	Система защиты информации
СрЗИ	–	Средства защиты информации
СКЗИ	–	Средства криптографической защиты информации
СОВ	–	Система обнаружения вторжений

СУБД	–	Система управления базами данных
ТС	–	Технические средства
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю Российской Федерации
(П)ЭВМ	–	(Персональная) электронная вычислительная машина

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение

1.1.1. «Политика по обеспечению информационной безопасности» (далее – Политика) Краевого государственного казенного общеобразовательного учреждения для детей-сирот и детей, оставшихся без попечения родителей, реализующее адаптированные основные общеобразовательные программы «Школа-интернат №3» (далее – КГКОУ ШИ 3, Оператор) регламентирует порядок реализации организационных мер, направленных на обеспечение информационной безопасности и определяет процедуры, направленные на выявление инцидентов; порядок контроля за обеспечением уровня защищенности информации; правила управления конфигурацией; формы и методы управления системой защиты необходимые для предоставления услуг, требованиям к защите информации, в том числе при выводе из эксплуатации структурных элементов, содержащейся в информационных системах.

1.1.2. Настоящая Политика направлено на защиту информационных ресурсов КГКОУ ШИ 3 от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации.

1.1.3. Обработка информации ограниченного доступа (в том числе персональные данные), не содержащей сведения, составляющие государственную тайну от несанкционированного доступа, специальных воздействий на такую информацию в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в информационных системах КГКОУ ШИ 3 осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области информационной безопасности и настоящей Политики.

1.1.4. Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

1.2. Источники разработки и правовые основания

1.2.1. Настоящая Политика разработана в соответствии с требованиями следующих стандартов и нормативных документов:

– Конституция Российской Федерации;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

– Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Методический документ ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»;

– ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

– иных федеральных законов, нормативных и правовых актов Российской Федерации.

1.3. Область действия

1.3.1. Требования настоящей Политики распространяются на все процессы обработки и защиты информации ограниченного доступа (в том числе персональные данные), не содержащей сведения, составляющие государственную тайну (далее – защищаемую информацию; на всех работников и все структурные подразделения, прямо или косвенно задействованные в процессах обеспечения ИБ, администрирования, мониторинга и(или) развития (модернизации) ИС либо ее отдельных компонентов, а также на всех работников КГКОУ ШИ 3, допущенных к обработке персональных данных в ИС.

1.3.2. Особенности контроля безопасности информации могут регулироваться дополнительными инструкциями и регламентами.

2. ПРАВИЛА И ПРОЦЕДУРЫ, ОСНОВНЫЕ МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ

2.1. Назначение правил и процедур по защите информации

2.1.1. Правила и процедуры по защите информации – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и обработка информации в ИС.

2.1.2. Обеспечение безопасности информации при ее обработке в ИС достигается применением организационных и технических мер, причем в интересах обеспечения безопасности в обязательном порядке подлежат защите технические и программные средства, используемые при обработке информации, и носители информации.

2.1.3. Правила и процедуры по защите информации регламентируют эффективную работу системы обеспечения ИБ. Правила и процедуры по защите информации реализуются посредством административно-организационных мер, физических и программно-технических средств и определяют архитектуру системы защиты.

2.1.4. Все документально оформленные решения, формирующие правила и процедуры по защите информации в ИС, должны быть утверждены директором КГКОУ ШИ 3.

2.2. Основные принципы управления ИБ

2.2.1. Основными принципами управления ИБ являются:

– непрерывность комплексного анализа информационного пространства ИС с целью выявления уязвимостей информационных ресурсов;

– своевременность обнаружения проблем, потенциально способных повлиять на ИБ ИС, корректировка моделей угроз и нарушителя;

– адекватность защитных мер характеру выявленных угроз;

– обоснованность затрат на реализацию защитных мер;

– обязательность контроля эффективности принимаемых защитных мер;

– персонификация и разделение ролей между работниками КГКОУ ШИ 3;

– персональная ответственность за совершаемые операции.

2.3. Основные меры по обеспечению информационной безопасности

2.3.1. Основными мерами, правилами и процедурами обработки и защиты информации являются:

– управление (администрирование) системой защиты, в том числе при выводе из эксплуатации структурных элементов;

– выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации (далее — инциденты), и реагирования на них;

– управление конфигурацией ИС и СЗИ, в том числе определение порядка обновления ПО, управление параметрами настройки СрЗИ, составом и конфигурацией ТС, обработки информации и ПО, контроль за несанкционированными подключениями ТС обработки информации и установкой ПО;

– контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;

– идентификация и аутентификация субъектов доступа и объектов доступа, в том числе управление учетными записями пользователей, установление полномочий пользователей, правил генерации, смены и восстановления паролей пользователей;

– управление доступом субъектов доступа к объектам доступа, в том числе установление перечня лиц, имеющих доступ к объектам доступа ИС, и их прав (привилегий) доступа к этим объектам;

– ограничение программной среды информационных систем;

– защита МНИ, в том числе определение порядка вывода информации на внешние носители информации, учета, хранения и использования съемных МНИ, процедуры архивирования информации, порядок стирания (уничтожения) данных и остаточной информации с МНИ и (или) уничтожения МНИ;

– регистрация событий безопасности, в том числе предусматривающая порядок контроля за действиями пользователей (администраторов) в ИС;

– антивирусная защита и процедуры реагирования на обнаружение в информационной системе вредоносного программного обеспечения;

– обнаружение (предотвращение) вторжений и процедуры реагирования на них;

– контроль (анализ) защищенности информации;

– целостность и доступность ИС и информации, в том числе предусматривающая контроль целостности СЗИ, порядок периодического анализа уязвимостей ИС и принятия первоочередных мер по устранению вновь выявленных

уязвимостей, восстановления работоспособности и настроек СЗИ в случае нарушения функционирования ИС;

– защита среды виртуализации;

– защита ТС, в том числе определяющая перечень лиц, имеющих доступ в помещения, в которых расположены ТС, и порядок их доступа в помещения и к ТС;

– защита ИС, ее средств, систем связи и передачи данных, в том числе определяющая порядок использования периферийных устройств, которые могут активироваться удаленно, технологий мобильного кода, технологий передачи речи и видеоинформации, порядок защиты внутренних и внешних беспроводных соединений, порядок использования и защиты мобильных устройств;

– порядок обучения и информирования пользователей о правилах эксплуатации СЗИ и СрЗИ, а также информирования об угрозах безопасности информации.

3. ПРАВИЛА УПРАВЛЕНИЯ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Назначение и область действия правил управления и администрирования СЗИ (СЗПДн)

Процессы обеспечения ИБ направлены на обеспечение следующих характеристик защищаемой информации ИС:

– конфиденциальности (предотвращение неправомерного доступа, копирования, предоставления или распространения информации);

– целостности (предотвращение неправомерного уничтожения или модифицирования информации);

– доступности (предотвращение неправомерного блокирования информации).

3.2. Управление и администрирование СЗИ (СЗПДн)

3.2.1. Управление (администрирование) системой защиты информации ИС КГКОУ ШИ 3 осуществляет исключительно администратор информационной безопасности (далее – Администратор ИБ). Настройка всех внедрённых для защиты информации ИС СрЗИ производится под администраторской учётной записью, пароль администраторской учётной записи известен только Администратору ИБ.

3.2.2. В целях исключения утери доступа к настройке (администрированию) СрЗИ при форс-мажорных ситуациях пароль администратора хранится в запечатанном конверте в сейфе директора КГКОУ ШИ 3. При отсутствии Администратора ИБ и необходимости доступа для администрирования СрЗИ конверт с паролем к учётной записи Администратора ИБ вскрывается директором (или лицом, его замещающим). При назначении нового Администратора ИБ незамедлительно нужно сменить пароль администраторской учётной записи, запечатать новый пароль в конверт и передать его для хранения. Администратор ИБ обязан подготавливать новый конверт с паролем каждый раз при изменении пароля своей учётной записи.

3.2.3. Ключевыми аспектами управления информационной безопасностью являются:

- назначение ответственных должностных лиц;
- обеспечение неизменности среды функционирования;
- защита технических средств;
- обеспечение регистрации и мониторинга событий безопасности.

3.2.4. В ходе администрирования СЗИ осуществляется:

– заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИС;

– управление СрЗИ в ИС, включая восстановление их работоспособности, генерацию, смену и восстановление паролей;

– централизованное управление и сопровождение функционирования СЗИ (при необходимости) и сопровождение функционирования в ходе ее эксплуатации;

– установка обновлений ПО, включая ПО СрЗИ, выпускаемых разработчиками (производителями) СрЗИ или по их поручению;

– управление параметрами настройки ПО, включая ПО СрЗИ, управление учетными записями пользователей, восстановление работоспособности СрЗИ, генерацию, смену и восстановление паролей;

– внесение изменений в ОРД по защите информации (при необходимости);

– корректировка эксплуатационной документации на СЗИ;

– анализ и регистрация событий в ИС, относящихся к безопасности информации;

– информирование пользователей о правилах эксплуатации СЗИ ИС и отдельных СрЗИ, а также об угрозах безопасности информации;

– обучение пользователей ИБ и повышение их уровня осведомленности по вопросам защиты информации.

3.2.5. В ходе управления защитой информации в ИС осуществляется:

– выполнение организационных мер защиты информации;

– контроль состояния защиты информации в ИС, включая контроль за событиями и действиями пользователей ИС;

– анализ и оценка функционирования СЗИ, включая выявление, анализ и устранение недостатков в функционировании СЗИ;

– периодический анализ уязвимостей ИС и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности;

– периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

– анализ влияния на СЗИ планируемых изменений в ИС;

– доработка (модернизация) СЗИ и ее повторная аттестация при изменении класса защищенности ИС, состава актуальных угроз безопасности информации или проектных решений по СЗИ;

– сопровождение СЗИ в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.

3.2.6. Безопасность среды эксплуатации ИС обеспечивается:

– организацией КЗ, в пределах которой постоянно размещаются ТС, обрабатывающие информацию, и СрЗИ, а также средства, обеспечивающие функционирование информационной;

– контролем и управлением доступом к ТС, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

– защитой ТС, СрЗИ и средств обеспечения функционирования.

4.ФОРМЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЫВОДЕ ИЗ ЭКСПЛУАТАЦИИ ИС ИЛИ ЕЕ СТРУКТУРНЫХ ЭЛЕМЕНТОВ

4.1. Назначение и область действия методов защиты информации при выводе из эксплуатации ИС

4.1.1. Решение о выводе из эксплуатации ИС принимается директором КГКОУ ШИ 3.

4.1.2. При выводе ИС из эксплуатации утверждается план вывода из эксплуатации ИС. В плане учитываются мероприятия по архивированию и/или уничтожению защищаемой информации, уничтожению (при необходимости) машинных носителей информации, содержащих информацию ограниченного доступа, мероприятия по подготовке документации о выводе ИС КГКОУ ШИ 3 из эксплуатации.

4.2. Способы защиты информации при выводе из эксплуатации ИС

4.2.1. Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации осуществляется Оператором в соответствии с эксплуатационной документацией на СЗИ и ОРД по защите информации и в том числе включает:

– архивирование информации, содержащейся в ИС, которое должно осуществляться при необходимости дальнейшего использования информации в деятельности Оператора;

– уничтожение (стирание) данных и остаточной информации с МНИ производится при необходимости передачи МНИ другому пользователю ИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

4.2.2. При выводе из эксплуатации МНИ, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих МНИ.

4.2.3. В случае принятия решения о необходимости хранения и (или) дальнейшего использования ИР, содержащихся в ИС, ИР хранятся в КГКОУ ШИ 3, являющемся Оператором системы, либо передаются определенному Оператором юридическому лицу для хранения и дальнейшего использования. Срок хранения ИР определяется руководством КГКОУ ШИ 3 и не может быть меньше срока хранения

информации, содержащейся в указанных ИР. Хранение ИР должно обеспечивать возможность их дальнейшего использования.

4.2.4. ПО и СрЗИ, выводимые из эксплуатации, подлежат дальнейшему использованию при наличии такой возможности или списанию в установленном порядке.

5. ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ И РЕАГИРОВАНИЯ НА НИХ

5.1. Назначение и область действия процедур по инцидентам

5.1.1. Правила и процедуры по инцидентам составлены с учетом требований ГОСТ Р ИСО/МЭК ТО 18044-2007 и раздела XV. Приложения 1 к приказу ФСТЭК России от 18.02.2013 № 21.

5.1.2. В ходе реагирования на инциденты (уязвимости), связанные с защитой информации, осуществляется:

– обнаружение, квалификация и регистрация инцидентов, связанных с защитой информации, в том числе сбоев в работе ТС, ПО и СрЗИ, внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иные событий, связанных с защитой информации;

– определение лиц (структурного подразделения), ответственных за выявление инцидентов и реагирование на них;

– своевременное информирование структурного подразделения или должностного лица, ответственных за защиту информации, пользователями и администраторами ИС об инцидентах, связанных с защитой информации;

– выявление причин возникновения инцидентов, связанных с защитой информации, оценка и анализ их последствий, планирование и принятие мер по предупреждению и устранению инцидентов, в том числе по восстановлению ИС и ее сегментов после сбоев, выявлению и устранению последствий внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей, неправомерных действий по сбору информации, устранению последствий нарушения правил разграничения доступа и иных событий, связанных с защитой информации;

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

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

5.1.3. Должны быть определены, выполняться, регистрироваться и контролироваться:

– процедуры хранения и распространения информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ;

– действия работников организации при обнаружении нетипичных событий, связанных с ИБ, и информировании о данных событиях. Работники КГКОУ ШИ 3 должны быть осведомлены об указанных порядках;

– роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ и назначены ответственные за выполнение указанных ролей.

5.1.4. Должны приниматься, фиксироваться и выполняться решения по всем выявленным инцидентам ИБ.

5.2. Классификация инцидентов ИБ

5.2.1. Инциденты ИБ классифицируются по следующим признакам:

– по степени тяжести последствий для функционирования ИС;

– по степени вероятности повторного возникновения инцидента ИБ;

– по видам источников угроз ИБ, вызывающих инциденты ИБ;

– по преднамеренности возникновения инцидента ИБ (случайный, намеренный, ошибочный);

– по видам объектов информационной инфраструктуры, задействованных (пораженных) при реализации инцидента ИБ;

– по уровню информационной инфраструктуры, на котором происходит инцидент ИБ;

– по нарушенным свойствам объектов защиты (конфиденциальность, целостность, доступность);

– по типу инцидента ИБ (свершившийся инцидент ИБ, попытка осуществления инцидента ИБ, подозрение на инцидент ИБ);

– по области распространения и действия инцидента ИБ;

– по сложности обнаружения инцидента ИБ;

– по сложности закрытия инцидента ИБ.

5.2.2. Выделяются 4 уровня опасности инцидента:

– высокоопасный;

– опасный;

– малоопасный;

– неопасный.

5.2.3. К высокоопасным инцидентам относятся следующие инциденты:

– вирусная эпидемия;

– взлом ключевых элементов ИС (сервер, АРМ управления, АРМ администратора безопасности);

– выход из строя критичных элементов СКЗИ;

– выход из строя механизмов безопасности;

– выход из строя средств защиты информации;

– затопление оборудования;

– злоупотребление правами доступа;

– несанкционированная модификация настроек СрЗИ;

– несанкционированные акты социального характера (забастовки, саботаж, массовые беспорядки и т.п.);

– передача защищаемой информации по открытым линиям связи;

– пожар;

– потеря доступа к сетям связи общего пользования и (или) сети Интернет свыше 48 часов;

– разглашение защищаемой информации;

– сбой ключевого элемента системы (сервер, АРМ управления, АРМ администратора безопасности);

– сетевые атаки и угрозы (подмены доверенного объекта сети, навязывание ложного маршрута сети, внедрения ложного объекта сети и др.);

– стихийные бедствия (наводнения, ураганы, землетрясения, удары молний и т.п.);

– умышленное искажение или удаление ПО и защищаемой информации;

– уничтожение доказательной базы при работе над инцидентами безопасности;

– хищение технических средств ИС, носителей информации, документов.

5.2.4. К опасным инцидентам относятся следующие инциденты:

– взлом неключевых элементов ИС (АРМ пользователя ИС);

– дефекты, сбои и отказы, аварии технических средств ИС;

– ненадлежащее управление криптографическими ключами;

– несанкционированная модификация системного и прикладного ПО;

– несанкционированная передача защищаемой информации третьим лицам с использованием средств электронной почты и сервисов сети Интернет;

– несанкционированное изменение базового программного обеспечения (BIOS, UEFI);

– несанкционированное использование электронной подписи;

– несанкционированное проникновение в здание и (или) служебные помещения, в которых размещены технические средства ИС;

– несанкционированный доступ к информации при проведении работ по техническому обслуживанию, ремонту или уничтожению технических средств ИС;

– несанкционированный доступ к техническим средствам и ресурсам ИС;

– подбор атрибутов доступа к системному и прикладному ПО, используемому в ИС;

– подмена загружаемой гостевой ОС;

– потеря доступа к сети Интернет на время до 24 часов;

– преднамеренный вывод из строя ТС ИС, носителей информации, элементов поддерживающей инфраструктуры (линии связи, передающее оборудование), документов;

– предоставление доступа к СКЗИ без служебной необходимости;

– предоставление доступа к ТС и ресурсам ИС лицам, не имеющим прав легального доступа;

– утрата носителей информации, документов и т.п.;

– утрата паролей к привилегированным учетным записям;

– хранение критически важной информации на мобильных устройствах.

5.2.5. К малоопасным инцидентам относятся следующие инциденты:

– аварии поддерживающей инфраструктуры (отключение электропитания, повреждение системы заземления, обрывы линий связи и т.п.);

– вирусное заражение узлов ИС;

– внедрение вредоносных программ;

– выход из строя инфраструктуры жизнеобеспечения зданий и персонала;

– выход из строя источников электропитания;

– выход из строя носителей информации;

– выход из строя систем электроснабжения;

– выход из строя элементов ИС из-за ошибок в работе;

– дефекты, сбои и отказы ПО ИС;

– загрузка стороннего ПО с отчуждаемых носителей информации;

– истощение вычислительных мощностей ИС;

– истощение полосы пропускания сети;

– нарушение климатических условий работы для технических средств;

– нарушение работоспособности из-за запыления технических средств и (или) помещений;

– несанкционированное внедрение беспроводных точек доступа;

– несанкционированное изменение настроек сетевого оборудования;

– несанкционированное подключение отчуждаемых носителей информации или подключения к сети Интернет с использованием сторонних устройств (USB-модемов, мобильных телефонов и т.п.);

– несанкционированное сканирование сетевого трафика;

– несанкционированный удаленный запуск приложений;

– несообщение о фактах или подозрении о компрометации ключевой информации;

– обработка информации ограниченного доступа на незащищенных технических средствах обработки информации;

– повреждение ключевой информации, выход из строя носителя ключевой информации;

– расположение монитора, не исключающее визуальный просмотр с экрана информации посторонним лицам;

– случайное или умышленное искажение/уничтожение образов виртуальных машин;

– снижение пропускной способности каналов связи;

– установка стороннего ПО в ИС.

5.2.6. К неопасным инцидентам относятся следующие инциденты:

– штатная сработка антивирусных средств на вирусы и систем обнаружения и предотвращения вторжений на сетевые атаки;

– спам;

– использование ИС в личных целях.

5.2.7. При возникновении высокоопасного инцидента:

– незамедлительно оповещается директор КГКОУ ШИ 3 (или его заместитель);

– принимаются меры по:

- устранению причины инцидента в срок не более 1 часа с момента обнаружения инцидента;
- устранению последствий инцидента в срок не более 4 часов с момента обнаружения инцидента.
- при невозможности устранить последствия инцидента в указанный срок, корректировка сроков и действий производится директором КГКОУ ШИ 3.

5.2.8. При возникновении опасного инцидента:

– незамедлительно оповещается Администратор ИБ;

– принимаются меры по:

- устранению причины инцидента в срок не более 8 часов с момента обнаружения инцидента.

- устранению последствий инцидента в срок не более 1 дня с момента обнаружения инцидента.
- при невозможности устранить последствия инцидента в указанный срок, корректировка сроков и действий производится Администратором ИБ.

5.2.9. При возникновении малоопасного инцидента:

– принимаются меры по:

- устранению причины инцидента в срок не более 1 дня с момента обнаружения инцидента;
- устранению последствий инцидента в срок не более 2 дней с момента обнаружения инцидента;
- при невозможности устранить последствия инцидента в указанный срок, корректировка сроков и действий производится Администратором ИБ.

5.2.10. При возникновении неопасного инцидента:

– принимаются меры по:

- устранению причины инцидента в срок не более 3 дней с момента обнаружения инцидента.
- устранению последствий инцидента в срок не более 1 недели с момента обнаружения инцидента.

5.2.11. Выбор мер по нейтрализации последствий инцидентов и ликвидации возможности повторного возникновения инцидента осуществляет директор КГКОУ ШИ 3 по представлению Администратора ИБ.

5.3. Обнаружение, идентификация и регистрация инцидентов

5.3.1. Оповещение о возникновении событий ИБ производится пользователями ИС или автоматизированными средствами мониторинга.

5.3.2. При оповещении о возникновении событий ИБ Администратором ИБ ИС инициируются мероприятия, направленные на:

– сбор информации, связанной с событиями ИБ;

– обеспечение регистрации всех действий и принятых решений для последующего анализа;

– обеспечения сбора свидетельств и их безопасное хранение, на случай судебного преследования или внутреннего расследования;

– передача информации о событии ИБ на более высокий уровень ответственности для дальнейшей оценки и принятии решения в случае необходимости таких решений.

5.3.3. В рамках идентификации инцидента производится оценка события ИБ с целью определить является ли оно инцидентом ИБ или ложной тревогой.

5.3.4. В случае положительного заключения о выявлении инцидента ИБ, Администратором ИБ ИС производится его регистрация в «Журнале учета инцидентов информационной безопасности», форма которого приведена в Приложении № 1 к настоящей Политики.

5.4. Реагирование на инциденты (уязвимости) ИБ

5.4.1. Реагирование на инциденты (уязвимости) ИБ может происходить по двум основным сценариям:

– действия позднего реагирования, в случае, если инцидент ИБ завершен и не оказал негативного влияния на состояние защищенности ИС;

– антикризисные действия, в случае, если инцидент ИБ не завершен (может быть предотвращен в стадии, на которой был зафиксирован) и(или) зафиксировано снижение состояния защищенности ИС.

5.4.2. Целью действий позднего реагирования является расследование и нейтрализация причин, по которым стала возможна реализация инцидента ИБ.

5.4.3. Целью антикризисных действий является незамедлительное устранение причин, повлекших реализацию инцидента ИБ, и проведение мероприятий по нейтрализации негативного воздействия на состояние защищенности ИС.

5.4.4. Должностные лица Оператора самостоятельно либо с привлечением сторонних организаций определяют и выполняют мероприятия по устранению последствий инцидентов ИБ.

5.5. Правила и процедуры разбирательства инцидента

5.5.1. Решение о проведении разбирательства инцидента принимает директор КГКОУ ШИ 3 по представлению Администратора ИБ.

5.5.2. Разбирательство по факту инцидента проводится в случае возникновения высокоопасных и опасных инцидентов.

5.5.3. Разбирательство малоопасных инцидентов может быть проведено в случае присутствия закономерностей и большой частоты их возникновения.

5.5.4. Целями разбирательства инцидентов являются:

– обеспечение безопасности информации в ИС;

– предотвращение несанкционированного доступа к информации и (или) передачи их лицам, не имеющим права доступа к такой информации;

– выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;

– минимизация последствий инцидента.

5.5.5. Разбирательство инцидента состоит из следующих этапов:

– подтверждение/опровержение факта возникновения инцидента.

– уточнение дополнительных обстоятельств (деталей) инцидента.

– получение (сбор) доказательств возникновения инцидента, обеспечение их сохранности и целостности.

5.5.6. Разбирательство инцидентов проводится Администратором ИБ.

5.5.7. Для проведения разбирательства привлекается постоянно действующая техническая комиссия по защите информации. Результаты работы комиссии оформляются актом.

5.5.8. В процессе проведения разбирательства инцидентов обязательными для установления являются:

– дата и время совершения инцидента;

– Ф. И. О., должность виновного в инциденте (нарушителя);

– обстоятельства и мотивы совершения инцидента;

– характер и размер реального и потенциального ущерба;

– информационные ресурсы, затронутые инцидентом;

– обстоятельства, способствовавшие совершению инцидента.

5.5.9. Решение по результатам работы комиссии принимает директор КГКОУ ШИ 3.

5.5.10. Материалы разбирательств инцидентов хранятся у Администратора ИБ в течение трех лет.

5.6. Планирование и принятие мер по предотвращению повторного возникновения инцидентов

5.6.1. В рамках планирования и принятия мер по предотвращению повторного возникновения инцидентов силами Оператора выполняется:

– изучение последствий инцидентов ИБ;

– определение улучшений организационно-технических мер защиты ИС с использованием имеющихся средств защиты информации;

– инициирование улучшений в области ИБ, включая внедрение новых и(или) уточненных организационно-технических мер защиты ИС.

5.7. Планирование и принятие мер по предотвращению повторного возникновения инцидентов

5.7.1. Нормативно-методической документацией определены следующие характеристики ИС, об изменениях которых требуется обязательно извещать орган по аттестации (организацию):

– состав и условия размещения технических средств и систем;

– состав (комплектность) продукции, используемой в целях защиты информации, схема ее монтажа (параметры установки и настройки), способствующие снижению уровня защищенности объекта информатизации.

5.7.2. Орган по аттестации (организация) принимает решение о необходимости проведения оценки соответствия ИС требованиям по защите информации после изменений вышеуказанных характеристик.

5.7.3. Обязательная проверка эффективности системы защиты проводится при изменении условий эксплуатации, а также технических, программных и программно-технических средств ИС, приводящих к нарушению их штатной работы, включая штатную работу системы защиты информации, или к образованию угроз безопасности информации.

5.7.4. Эксплуатация ИС разрешается только после проведения проверки эффективности системы защиты организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

6. ПОРЯДОК УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ ИС И ЕЕ СИСТЕМОЙ ЗАЩИТЫ

6.1. Назначение и область действия порядка управления конфигурацией, аттестованной ИС и ее СЗИ

6.1.1. Правила и процедуры управления конфигурацией аттестованной информационной системы и ее системы защиты информации составлены с учетом ГОСТ Р ИСО/МЭК 17799-2005.

6.1.2. Обработка защищаемой информации в ИС разрешается исключительно при наличии действующего аттестата соответствия требованиям.

6.1.3. Перечень условий, при которых аттестат теряет своё действие:

– изменение состава технических средств ИС;

– перенос технических средств ИС в другие помещения;

– изменение технологического процесса обработки информации в ИС;

– прекращение действия сертификатов ФСТЭК / ФСБ на используемые в ИС средства защиты;

– истечение срока действия аттестата соответствия требованиям информационной безопасности.

6.1.4. В ходе управления конфигурацией ИС и ее СЗИ осуществляется:

– обеспечение целостности СЗИ, включая резервирование СрЗИ;

– установка обновлений ПО, включая ПО СрЗИ, выпускаемых их разработчиками (по поручению разработчиков);

– управление параметрами настройки ПО, включая ПО СрЗИ, составом и конфигурацией ТС и ПО, а также контроль за несанкционированными подключениями ТС и установкой ПО.

6.1.5. Перед реализацией планируемых в процессе управления конфигурацией изменений в ИС и ее СЗИ проводится оценка их потенциального воздействия на обеспечение защиты информации и работоспособность ИС.

6.1.6. Изменения в ИС и ее СЗИ, внесенные в процессе управления конфигурацией, подлежат документированию Оператором.

6.1.7. Каждое внесение изменения в информационную систему несет в себе риск нарушения функционирования ИС. Риск несет в себе как новое состояние ИС, так и процесс перехода из старого состояния в новое. Каждое изменение должно быть обосновано. Решение о внесении изменения принимается Администратором ИБ.

6.1.8. Для любого компонента ИС реализовано ограничение прав доступа пользователей на изменение критичных для функционирования системы данных.

6.2. Оценка потенциального воздействия изменений

6.2.1. Оценка потенциального воздействия изменений должна быть выполнена для всех субъектов изменений, а также для всех взаимосвязанных с ними информационных ресурсов и компонентов ИС.

6.2.2. Оценка потенциального воздействия должна включать в себя следующие направления:

– оценка технического воздействия и совместимости;

– оценка на соответствие законодательным и внутренним требованиям и стандартам;

– оценка влияния на состояние защищенности ИС;

– оценка влияния на целевые функции и процессы ИС.

6.2.3. Все изменения до внедрения должны быть в обязательном порядке согласованы Администратором ИБ и Ответственным за организацию обработки персональных данных.

6.3. Внесение изменений в компоненты

6.3.1. Внесение изменений в компоненты ИС производятся в период наименьшей загруженности. В случае необходимости, после внесения изменений в ИС должна обновляться связанная с системой документация.

6.3.2. Принятию решения о внесении изменения в ИС предшествует:

– анализ целесообразности внесения изменения с точки зрения возможного влияния изменения на работоспособность ИС в целом;

– тестирование предлагаемого изменения на тестовой среде, максимально приближенной по своим характеристикам к промышленной;

– анализ результатов тестирования и принятие решения о возможности изменения промышленной системы;

– составление плана внесения изменения в ИС;

– составление плана восстановления работоспособности в случае необходимости отката изменений;

– авторизация изменения уполномоченными работниками.

6.3.3. Контроль отдельных этапов процедуры внесения изменений осуществляется Администратором ИБ.

6.3.4. Все запросы на внесение изменений создаются и обрабатываются в электронном виде.

6.3.5. Запрос на внесение изменения в должен содержать:

– порядок действий при внесении изменений и ожидаемый результат;

– описание необходимых системных, программных и человеческих ресурсов;

– порядок контроля результатов внесения изменений;

– процедуры возврата к первоначальному состоянию системы.

6.4. Внесение плановых и неплановых изменений

6.4.1. Внесение плановых и неплановых изменений в ИС производится уполномоченными работниками в соответствии с запросом на внесение изменений, при условии успешного завершения тестирования, результаты которого зафиксированы в Акте тестирования и завизированы Администратором ИБ.

6.4.2. По возможности изменения должны фиксироваться в журналах регистрации событий системного или прикладного ПО. Форма журнала регистрации изменений в конфигурации ИС приведена в Приложении №2 к настоящей Политике.

6.4.3. После внесения изменений в ИС, должна выполняться проверка правильности функционирования функций компонентов ИС, затронутых изменениями. В случае, если компонент ИС функционирует некорректно, проводится откат к его предыдущей версии.

6.5. Уточнение статуса Аттестата соответствия

6.5.1. С момента выдачи КГКОУ ШИ 3 Аттестата соответствия необходимо производить уведомление Органа по аттестации ИС о произведенных изменениях конфигурации ИС с целью получения заключения о влиянии внесенных изменений на статус выданного Аттестата соответствия.

6.5.2. В случае, если внесенные изменения затронули статус Аттестата соответствия, Оператором должен быть рассмотрен вопрос о проведении повторной аттестации ИС или проведении дополнительных аттестационных испытаний на соответствие требованиям информационной безопасности.

7. МОНИТОРИНГ ЗА ОБЕСПЕЧЕНИЕМ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

7.1. Назначение и область действия контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС

7.1.1. В ходе мониторинга (контроля) за обеспечением уровня защищенности информации, содержащейся в ИС осуществляются:

– контроль за событиями безопасности и действиями пользователей в ИС;

– контроль (анализ) защищенности информации, содержащейся в ИС;

– анализ и оценка функционирования СЗИ, включая выявление, анализ и устранение недостатков в функционировании СЗИ;

– периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;

– принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) СЗИ, повторной аттестации ИС или проведении дополнительных аттестационных испытаний.

7.1.2. Контрольные мероприятия за обеспечением уровня защищенности информации и соблюдений условий использования СЗИ, а также соблюдением требований законодательства Российской Федерации по обработке защищаемой информации, в том числе ПДн в ИС проводятся в следующих целях:

– проверка выполнения требований ОРД по защите информации в КГКОУ ШИ 3 и действующего законодательства Российской Федерации в области обработки и защиты информации;

– оценка уровня осведомленности и знаний работников КГКОУ ШИ 3 в области обработки и защиты информации;

– оценка обоснованности и эффективности применяемых мер и средств защиты.

7.2. Правила и процедуры контроля за обеспечением уровня защищенности информации

7.2.1. Перед вводом системы защиты информации СрЗИ настраиваются в соответствии с требованиями нормативно-правовых актов Российской Федерации

по вопросам ИБ, руководящими и нормативными документами ФСБ России, ФСТЭК России, документами по защите информации, утверждёнными в КГКОУ ШИ 3, эксплуатационной документацией на СрЗИ. Параметры настройки СрЗИ соответствуют установленному классу (уровню) защищённости информационной системы.

7.2.2. Администратор ИБ обязан с периодичностью 1 раз в квартал (три месяца) проводить контроль состояния системы защиты информации (далее – Контроль). При планировании Контроля Администратор ИБ должен учесть следующие **виды контроля** системы защиты информации:

– документальный контроль;
– контроль физического доступа в ИС;
– контроль состава аппаратных средств ИС;
– контроль состава программных средств ИС;
– контроль работоспособности и правильности настройки средств защиты информации;
– поиск уязвимостей;
– контроль использования МНИ;
– и при необходимости другие виды контроля.

7.2.3. Результаты контроля состояния защиты информации, в том числе, перечисленными выше, анализа и оценки функционирования СЗИ, анализа уязвимостей и изменения угроз безопасности информации в ИС документируются.

8.ПРАВИЛА ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА

8.1. Назначение и область действия правил аутентификации и идентификации

8.1.1. Настоящие Правила определяют алгоритм идентификации и аутентификации субъектов доступа к объектам доступа в ИС КГКОУ ШИ 3.

8.1.2. В ИС обеспечивается идентификация и аутентификация работников КГКОУ ШИ 3 перед началом работы в системе. Идентификации и аутентификации подлежат также все запускаемые процессы (включая процессы, запускаемые от имени системных учетных записей). Идентификаторы и аутентификаторы создаются исключительно для пользователей, которым разрешена обработка информации в ИС КГКОУ ШИ 3.

8.1.3. В ИС используются два типа идентификаторов и аутентификаторов:

- учетная запись для работы в прикладном и специализированном ПО;
- учетная запись в операционной системе АРМ ИС.

8.1.4. Требования к сложности и времени действия аутентификаторов определены в правилах и процедурах управления доступом.

8.1.5. Аутентификация пользователя может осуществляться с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации – определенной комбинации указанных средств.

8.1.6. Оператором должны быть установлены и реализованы функции управления средствами аутентификации (паролями) устройств в ИС, такие как изменение аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении СЗИ (СЗПДн).

8.1.7. Оператор должен обеспечить получение (запросить) у поставщика технических средств (далее – ТС) и ПО ИС аутентификационную информацию, заданную производителем этих ТС и ПО и не указанную в эксплуатационной документации.

8.1.8. Организационное обеспечение процессов генерации, инициализации, хранения, выдачи, использования, смены, блокирования и прекращения действия паролей в ИС, за правильную реализацию настоящих правил и процедур идентификации и аутентификации субъектов доступа к объектам доступа осуществляет Администратор ИБ.

8.1.9. Техническое обеспечение процессов генерации, хранения, выдачи, использования, смены блокирования и прекращения действия паролей в ИС и контроль над действиями пользователей осуществляет Администратор ИБ.

8.2. Правила и процедуры идентификации и аутентификации пользователей, являющихся работниками КГКОУ ШИ 3

8.2.1. Идентификация и аутентификация пользователей, являющихся работниками КГКОУ ШИ 3 (далее – внутренние пользователи), должна производиться техническими средствами и системами.

8.2.2. К внутренним пользователям относятся должностные лица КГКОУ ШИ 3, выполняющие свои должностные обязанности с использованием информации, информационных технологий, информационной системы и технических средств ИС, в соответствии с должностными инструкциями и которым в ИС также присвоены учетные записи.

8.2.3. Идентификация внутренних пользователей должна осуществляться по уникальным учетным записям, которые однозначно идентифицируют пользователя. Запрещается применять учетные неидентифицируемые учетные записи, например: «user», «пользователь», «administrator» и т.д. без четкого определения принадлежности учетной записи к субъекту доступа.

8.2.4. В качестве идентификаторов внутренних пользователей должен использоваться логин.

8.2.5. Допускается использование иных идентификаторов внутренних пользователей, таких как:

– уникальное устройство (iButton, eToken, RuToken, iKey, смарт-карты и др.);

– электронная подпись;

– совокупность идентификаторов, указанных выше.

8.2.6. Для каждого идентификатора должна быть определена следующая информация о пользователе: фамилия, имя, отчество пользователя, должность.

8.2.7. Учет идентификаторов, выданных внутренним пользователям, производится:

– средствами службы каталогов для идентификаторов, указанных в пункте 8.2.3 настоящего раздела Политики;

– в журнале учета для идентификаторов, указанных в пункте 8.2.5 настоящего раздела Политики.

– в журнале учета средств криптографической защиты информации удостоверяющего центра для идентификаторов, указанных в пункте 8.2.5 настоящего раздела Политики.

8.2.8. Типовые формы учета идентификаторов разрабатываются Администратором ИБ.

8.2.9. Для аутентификации внутренних пользователей могут использоваться следующие факторы аутентификации:

– пароль, пин-код.

– уникальное устройство аутентификации: iButton, eToken, RuToken, iKey, смарт-карты и др.

– биометрия.

8.2.10. Допускается в качестве усиления процедур аутентификации использовать комбинации факторов аутентификации ИС.

8.3. Правила и процедуры управления идентификаторами

8.3.1. Администратор ИБ является лицом, ответственным за создание, присвоение и уничтожение идентификаторов пользователей.

8.3.2. Запрещается повторно использовать идентификатор пользователя в течение не менее одного года.

8.3.3. Администратор ИБ обязан блокировать или инициировать блокировку идентификаторов пользователей через период времени неиспользования более 90 дней.

8.4. Правила и процедуры управления средствами аутентификации (аутентификационной информацией)

8.4.1. Администратор ИБ является лицом, ответственным за хранение, выдачу, инициализацию, блокирование средств аутентификации.

8.4.2. На всех средствах вычислительной техники Администратор ИБ должен осуществлять изменение аутентификационной информации (средств аутентификации), заданной их производителями.

8.4.3. Администратор ИБ устанавливает и регистрирует в инструкции по организации парольной защиты следующие характеристики паролей:

– длина пароля;

– алфавит пароля (при наличии соответствующих механизмов);

– максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки программно-технического средства или учетной записи пользователя;

– время блокировки программно-технического средства или учетной записи пользователя после превышения количества неуспешных попыток аутентификации (ввода неправильного пароля);

– максимальное время действия пароля;

– минимальное время действия пароля.

8.4.4. В случае компрометации или подозрения компрометации паролей, пользователь ИС обязан незамедлительно обратиться к Администратору ИБ.

8.4.5. Администратор ИБ после сообщения о компрометации обязан осуществить незамедлительное блокирование скомпрометированных средств аутентификации. При необходимости, информация о компрометации сообщается директору КГКОУ ШИ 3 или его заместителю.

8.4.6. Доступ к администрированию технических средств и систем, содержащим службы каталогов, должен быть предоставлен только Администратору ИБ.

8.5. Правила и процедуры защиты обратной связи при вводе аутентификационной информации

8.5.1. Администратор ИБ обеспечивает исключение отображения для пользователя ИС действительного значения аутентификационной информации (пароля) путем:

– использования встроенных средств защиты обратной связи (вводимые символы отображаются условными знаками «*», «|»).

– доработки прикладного программного обеспечения с целью установления средства защиты обратной связи (вводимые символы отображаются условными знаками «*», «|»).

8.5.2. Пользователю ИС запрещается ввод аутентификационной информации в случае, если существует возможность наблюдения за вводом со стороны посетителей или посторонних лиц.

8.6. Правила и процедуры идентификации и аутентификации внешних пользователей

8.6.1. При необходимости в ИС может быть предоставлен доступ внешним пользователям.

8.6.2. Внешним пользователем ИС является лицо, не относящееся к внутренним пользователям.

8.6.3. Правила и процедуры доступа внешних пользователей идентичны правилам и процедурам доступа пользователей, являющихся работниками КГКОУ ШИ 3.

8.6.4. В качестве дополнительных мер идентификации внешних пользователей для каждого идентификатора должно быть добавлено наименование организации субъекта доступа.

8.7. Управление учетными записями и установление полномочий пользователей

8.7.1. С целью ограничения доступа к информационным ресурсам, содержащим защищаемую информацию, устанавливается единая система паролирования, включающая в себя следующие основные пароли: пароль BIOS и личные пользовательские пароли: входа в операционную систему и прикладное ПО.

8.7.2. Идентификаторы для работы в ИС создаются таким образом, чтобы по идентификатору была понятна роль пользователя в информационной системе (например, «Пользователь»).

9.ПРОЦЕДУРЫ УПРАВЛЕНИЯ ДОСТУПОМ СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА

9.1. Назначение и область действия процедур управления доступом

Доступ субъектов доступа к объектам доступа ИС отражен в «Матрице доступа к защищаемой информации, обрабатываемой в информационной системе».

9.2. Правила и процедуры управления учетными записями пользователей

9.2.1. Пользователями ИС могут являться как штатные работники КГКОУ ШИ 3, так и внешние пользователи, в случае производственной необходимости.

9.2.2. Пользователи ИС должны иметь возможность работать только с теми средствами и ресурсами ИС, которые необходимы им для выполнения установленных функциональных обязанностей.

9.2.3. За создание/изменение/удаление учетных записей в ИС отвечает Администратор ИБ. Администратор безопасности не реже 1-го раза в квартал проводит контроль актуальности учётных записей в ИС. Неактуальные учётные записи в информационной системе удаляются. В ИС не должно быть неиспользуемых учетных записей или учетных записей с истекшим сроком действия, регламентированным настоящими Правилами.

9.2.4. По умолчанию, все создаваемые Администратором ИБ учетные записи являются учетными записями внутренних пользователей.

9.2.5. В ИС КГКОУ ШИ 3 разрешается по умолчанию использовать **основные** типы учётных записей:

– Администратор;
– Пользователь.

9.2.6. Учётная запись **«Администратор»** используется Администратором ИБ для настройки средств защиты и параметров работы операционной системы.

Учётная запись **«Пользователь»** используется для выполнения всех видов работ, не связанных с администрированием ИС. Права доступа для данной учётной записи настраиваются таким образом, чтобы пользователи ИС, работающие под данной учётной записью, не имели возможность (случайно или преднамеренно) изменить настройки средств защиты информации, параметры работы операционной системы или установки в операционной системе новых программ.

Встроенная учётная запись операционной системы **«Гость»** отключается Администратором ИБ. Создание иных учётных записей в ИС не предусмотрено.

9.2.7. При создании Администратором ИБ **дополнительных** учетных записей, не принадлежащих работникам КГКОУ ШИ 3, в описании учетной записи должна быть добавлена информация о типе создаваемой учетной записи (внешний пользователь; системная, приложения; гостевая (анонимная), временная и (или) иной тип записи).

9.2.8. Для разграничения прав доступа к ресурсам ИС могут использоваться следующие методы разграничения доступа:

– дискреционный (управление доступом для индивидуального субъекта доступа);

– ролевой (управление доступом по группам субъектов доступа);

– мандатный (сопоставление классификационных меток каждого субъекта доступа и каждого объекта доступа).

9.2.9. Методы разграничения доступа в ИС определяются на этапе проектирования ИС или в процессе функционирования ИС Администратором ИБ.

9.2.10. Создание новой учетной записи в ИС осуществляется Администратором ИБ.

9.2.11. Временные учетные записи:

– временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для произведения настройки, тестирования информационной системы, для организации гостевого доступа.

– после выполнения задач, временная учетная запись должна быть заблокирована или удалена Администратором ИБ.

– при создании временных учетных записей срок их действия контролируется: вручную Администратором ИБ и автоматически (средствами службы каталогов).

9.3. Правила разграничения доступа

9.3.1. Для всех технических средств и систем ИС, содержащих службы каталогов, Администратором ИБ должны быть разработаны разрешительные системы доступа субъектов доступа к объектам доступа (матрица доступа).

9.3.2. В матрице доступа должны быть определены права доступа (операции воздействия) субъектов доступа на объекты доступа (полный доступ, чтение, запись, удаление, выполнение и др.), реализуемые в ИС.

9.3.3. Администратором ИБ должно быть обеспечено назначение прав и привилегий пользователям, минимально необходимых для выполнения ими своих должностных обязанностей.

9.4. Правила и процедуры управления информационными потоками между устройствами, сегментами ИС, а также между информационными системами

9.4.1. В ИС Администратором ИБ обеспечивается управление информационными потоками при передаче информации между устройствами, сегментами в рамках ИС.

9.4.2. Для каждого устройства, сегмента ИС Администратор ИБ определяет минимальный набор правил фильтрации, необходимость ограничивать информационные потоки, необходимость записи во временное хранилище информации для анализа и принятия решений о возможности ее дальнейшей передачи.

9.4.3. Условия, установленные пунктом 9.4.2 настоящего раздела Правил определяются на основании анализа угроз безопасности информации и требований нормативных правовых актов.

9.4.4. При установлении правил фильтрации должен быть обеспечен принцип «Запрещено всё, кроме разрешенного», например, при формировании правил фильтрации основным правилом фильтрации должен быть «запрещены любые сетевые пакеты в любом направлении».

9.5. Правила и процедуры ограничения неуспешных попыток входа и блокирования сеансов доступа

9.5.1. Параметры ограничения неуспешных попыток входа и блокирования сеансов доступа определяются Администратором ИБ.

9.5.2. Необходимые параметры ограничений:

– пороговое значение блокировки – от 3 до 10 ошибок входа в систему;
– продолжительность блокировки учетной записи – от 5 до 30 минут.

Применяемое СрЗИ от НСД настраивается таким образом, чтобы обеспечить блокирование доступа к АРМ по данным параметрам.

9.5.3. Необходимые параметры блокировки сеанса доступа:

– максимальное время бездействия (неактивности) пользователя должно быть не более 7 мин, по истечению заданного времени средствами системы защиты текущий сеанс должен блокироваться.

– в информационной системе на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы).

Для возобновления сеанса работы пользователь вводит пароль, соответствующий его учётной записи. СЗИ от НСД настраивается таким образом, чтобы запретить пользователю ИС любые действия до прохождения процедур идентификации и аутентификации. Действия, проводимые до процедур идентификации и аутентификации разрешаются исключительно Администратору ИБ в целях восстановления работоспособности ИС.

9.6. Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации

9.6.1. Действия пользователей до прохождения ими процедуры идентификации и аутентификации в ИС запрещены.

9.6.2. Загрузка АРМ ИС предусмотрена с жёсткого диска, данный вариант загрузки настраивается в BIOS материнской платы АРМ. Доступ к настройкам BIOS материнской платы АРМ в случае необходимости может защищаться средствами доверенной загрузки, сертифицированных по требованиям ФСТЭК России. Средство доверенной загрузки может быть программным, аппаратным, программно-аппаратным, внедрение такого СЗИ не должно ухудшать скорость и надёжность работы ИС.

9.7. Правила и процедуры применения удаленного доступа

9.7.1. Под удаленным доступом понимается процесс получения доступа (через внешнюю сеть) к объектам доступа ИС из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

9.7.2. Защита удаленного доступа к ресурсам ИС осуществляется с использованием защищенных каналов связи (VPN, шифрование и т.д.).

9.7.3. Виды удаленного доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) для ИС устанавливаются

на этапе проектирования ИС, модифицируются в процессе ее использования и регламентируются Администратором ИБ в Описании технологического процесса обработки информации.

9.7.4. Для ИС должно использоваться ограниченное (минимально необходимое) количество точек подключения при организации удаленного доступа.

9.7.5. Для ИС запрещен удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования ИС и ее систем защиты информации.

9.7.6. Администратор ИБ осуществляет контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС.

9.8. Правила и процедуры применения технологий беспроводного доступа

9.8.1. Для каждой ИС устанавливается возможность использования технологий беспроводного доступа (исходя из технологического процесса обработки информации), что должно быть отражено в технической документации на ИС. Решение по использованию в ИС технологий беспроводного доступа определяется Администратором ИБ.

9.8.2. В случае запрета использования технологий беспроводного доступа служба ИТ обеспечивает его запрет при помощи имеющейся инфраструктуры и средств защиты информации.

9.8.3. В пределах контролируемой зоны допускается устанавливать средства беспроводного доступа, физически либо логически отделенные от ИС, при этом должны быть выполнены следующие условия:

– получено разрешение от Администратора ИБ на размещение средства беспроводного доступа;

– Администратором ИБ должны быть установлены безопасные настройки средства беспроводного доступа.

9.8.4. Создание беспроводных точек доступа возможно только по согласованию с Администратором ИБ, осуществляется на основании письменного запроса, подписанного руководителем структурного подразделения, в котором планируется создание таких точек, содержащего обоснование необходимости создания беспроводной точки подключения.

9.9. Правила и процедуры применения мобильных технических средств

9.9.1. Мобильными техническими средствами являются портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

9.9.2. Для каждой ИС устанавливается возможность использования мобильных технических средств (исходя из технологического процесса обработки информации), что должно быть отражено в технической документации на ИС. Решение по использованию в ИС технологий мобильных технических средств должно быть согласовано с Администратором ИБ.

9.9.3. В ИС мобильные технические средства допускается использовать только тем субъектам доступа, для которых использование таких мобильных технических средств необходимо для выполнения своих должностных обязанностей.

9.9.4. Учет мобильных технических средств осуществляется в соответствии с установленными КГКОУ ШИ 3 требованиями по обращению с мобильными техническими средствами. Учет портативных вычислительных устройств ведет Администратор ИБ по идентификаторам этих устройств (MAC-адрес, имя устройства, серийные заводские номера и т.д.).

9.9.5. В ИС запрещено использовать не входящие в ее состав (находящихся в личном использовании) мобильные технические средства.

9.9.6. В ИС запрещено использовать мобильные технические средства информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации).

9.9.7. Контроль за использованием мобильных технических средств осуществляет Администратор ИБ.

9.10. Правила и процедуры управления взаимодействием с внешними ИС

9.10.1. Для ИС Администратором ИБ определяются требования к подключению внешних информационных систем. В требованиях должны быть учтены:

– алгоритм действий для получения доступа;
– требования к организации защищенного взаимодействия;
– требования к оценке соответствия внешних ИС требованиям безопасности информации.

9.10.2. Для ИС устанавливается возможность использования системных учетных записей, что должно быть отражено в «Матрице доступа к защищаемой информации, обрабатываемой в информационной системе». Решение по использованию в ИС системных учетных записей принимается Администратором ИБ.

10. МЕРЫ ПО ОГРАНИЧЕНИЮ ПРОГРАММНОЙ СРЕДЫ

10.1. Назначение и область действия мер по ограничению программной среды

10.1.1. Установка нового ПО должна быть согласована с органом по аттестации с целью исключения прекращения действия аттестата соответствия.

10.1.2. При необходимости установки в ИС нового ПО, оно сверяется с перечнем разрешённого ПО (далее «белый список»). При отсутствии планируемого к установке ПО в «белом списке» Администратор ИБ обращается за разрешением на доработку «белого списка» к Директору КГКОУ ШИ 3. Только после доработки «белого списка» Администратор ИБ производит установку необходимого ПО. Администратору запрещается устанавливать ПО, которого нет в «белом списке».

10.2. Правила и процедуры установки программного обеспечения

10.2.1. Всё устанавливаемое ПО должно быть полученным из доверенных источников, пройти антивирусную проверку и не иметь в своём составе компонентов, позволяющих обойти систему защиты.

10.2.2. При необходимости решением Администратора ИБ ограничение программной среды может быть также реализовано соответствующей настройкой антивируса, который имеет действующий сертификат ФСТЭК России.

10.2.3. Администратор ИБ обеспечивает установку (инсталляцию) в ИС только разрешенного к использованию в ИС ПО и (или) его компонентов.

10.2.4. Администратор ИБ обеспечивает установку (инсталляцию) в ИС программного обеспечения и (или) его компонентов только от имени администратора ИБ.

10.2.5. Администратор ИБ обеспечивает периодический контроль установленного в ИС ПО на предмет соответствия его перечню программного обеспечения, разрешенному к установке в ИС.

10.2.6. При обнаружении постороннего программного обеспечения Администратором ИБ производится полная антивирусная проверка АРМ, на котором было найдено постороннее ПО, постороннее ПО удаляется, пароли всех пользователей и администраторов подлежат замене.

11. ПРАВИЛА УЧЕТА, ХРАНЕНИЯ И УНИЧТОЖЕНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ НА МАШИННЫХ НОСИТЕЛЯХ

11.1. Назначение и область действия правил защиты машинных носителей информации

11.1.1. Все машинные МНИ, используемые в ИС для обработки защищаемой информации подлежат учёту.

11.1.2. Перед подключением к ИС должно быть обеспечено уничтожение (стирание) информации с носителей информации после их приобретения и при первичном подключении к ИС, при использовании в иных ИС, при передаче для постоянного использования от одного пользователя другому пользователю, после возвращения из ремонта.

11.1.3. Используемые в ИС СрЗИ от НСД настраиваются таким образом, чтобы исключить использование МНИ, не зарегистрированных в журнале учёта МНИ. При попытке использования в ИС неучтённых МНИ применяемые СрЗИ от НСД блокируют доступ к ИС, данное событие регистрируется в журнале безопасности СрЗИ от НСД.

11.2. Правила и процедуры учета МНИ

11.2.1. К машинным носителям информации, используемым в ИС, относятся:

– съемные МНИ (флэш-накопители, внешние накопители на жестких дисках и иные устройства) (далее – СМНИ);

– портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые фото-видео камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства).

– стационарно устанавливаемые в корпус технических средств (далее – ТС) МНИ (например, накопители на жестких дисках).

– файлы образов виртуальных машин (при использовании систем виртуализации).

11.2.2. Принципы учета МНИ:

– учету подлежат все используемые в ИС МНИ, предназначенные для обработки защищаемой информации, в том числе ПДн;

– учет должен быть журналируемым;

– МНИ учитываются Администратором ИБ в журналах учета машинных и съемных носителей информации;

– учет осуществляется по любым идентификационным признакам (заводской номер, инвентаризационный номер, регистрационный номер);

– МНИ, стационарно установленные в ТС ИС, могут учитываться в журналах материально-технического учета в составе соответствующих ТС. Допускается для одного ТС при использовании нескольких МНИ присвоение одного регистрационного номера;

– съемные и перезаписываемые МНИ должны подлежать раздельному учету;

– учет файлов образов виртуальных машин ведется средствами виртуальной инфраструктуры по уникальным логическим именам (ID) (при использовании систем виртуализации).

11.3. Правила и процедуры доступа к машинным носителям информации

11.3.1. Выдача МНИ осуществляется Администратором ИБ.

11.3.2. Список лиц, имеющих доступ к МНИ, утверждается Директором КГКОУ ШИ 3.

11.3.3. При использовании МНИ должны соблюдаться требования, обеспечивающие сохранность МНИ:

– хранение съемных МНИ осуществляется в сейфах или надежно запираемых металлических ящиках, оборудованных внутренними замками.

– в нерабочее время хранение любых видов съемных МНИ вне сейфов/металлических ящиков/выдвижных ящиках – не допускается.

– использование личных МНИ для обработки защищаемой информации запрещено.

11.4. Процедуры уничтожения (стирания) информации на МНИ

11.4.1. Оператором должны проводиться периодическая проверка процедур и тестирование средств стирания информации и контроля удаления информации

11.4.2. При передаче МНИ пользователю, который по технологии работы в ИС (служебной необходимости) не имеет права доступа к информации на передаваемых МНИ, а также в сторонние организации для ремонта или утилизации, вся информация, хранящаяся на них, подлежит уничтожению (стиранию).

11.4.3. Удаление временных файлов, создаваемых при работе в ИС, обеспечивается СрЗИ от НСД, которые настраиваются Администратором ИБ для затирания области МНИ, содержащей такие временные файлы.

11.4.4. Уничтожение (стирание) информации с МНИ осуществляется Администратором ИБ и производится с помощью встроенных в операционные системы системных утилит (Cipher.exe для Windows, WIPE для LINUX и др.), после этого – программного/аппаратного обеспечения гарантированного затирания информации.

11.4.5. Уничтожение информации на учтённых МНИ производится СрЗИ путём перезаписи области МНИ, где хранится защищаемая информация и (или) с помощью средств гарантированного уничтожения информации.

11.4.6. Уничтожению подлежат все пришедшие в негодность МНИ путем их физического уничтожения.

11.4.7. Уничтожение МНИ, предназначенных для обработки защищаемой информации, оформляется актом об уничтожении МНИ. Акты сдаются на хранение Администратору ИБ. Срок хранения актов – не менее одного года. Факт об уничтожении отражается в журнале учета МНИ и съемных МНИ.

11.4.8. Перед удалением информации или уничтожением МНИ и съемных МНИ необходимо сообщить Администратору ИБ.

11.4.9. После проведенных мероприятий, указанных в пунктах 11.4.2 – 11.4.6 настоящего раздела, акт об уничтожении направляется Администратору ИБ и хранится у Администратора ИБ.

12. ТРЕБОВАНИЯ К РЕГИСТРАЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ

12.1. Назначение и область действия требований регистрации событий безопасности

Обеспечение регистрации и мониторинга событий безопасности в ИС направлено на постоянную фиксацию и контроль проявлений состояния ИС и ее подсистемы обеспечения ИБ КГКОУ ШИ 3, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов ИС, нарушения процедур, установленных настоящей Политикой и (или) иными ОРД по защите информации в ИС, а также на нарушение штатного функционирования СрЗИ.

12.2. Правила и процедуры определения событий безопасности

12.2.1. Для ИС Администратор ИБ определяет перечень событий безопасности, подлежащих регистрации. Перечень определяется на этапе проектирования ИС, модифицируются в процессе ее использования.

12.2.2. События безопасности, подлежащие регистрации, должны определяться Администратором ИБ с учетом способов реализации угроз безопасности для ИС.

12.2.3. Для каждого типа событий Администратор ИБ определяет минимальный срок хранения журналов событий, регламентирует его в перечне регистрируемых событий.

12.2.4. Перечень событий безопасности, подлежащих регистрации в ИС, уточняется по результатам контроля (анализа) защищенности, но не менее чем один раз в год.

12.2.5. События безопасности, а также сроки хранения должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС.

12.3. Правила и процедуры определения состава и содержания информации о событиях безопасности

12.3.1. Для каждого регистрируемого типа событий безопасности Администратор ИБ определяет состав и содержание информации о событиях безопасности.

12.3.2. Состав и содержание информации о событиях безопасности должны обеспечивать возможность идентификации:

– типа события безопасности;

– даты и времени события безопасности;
– идентификационной информации источника события безопасности;
– результат события безопасности;
– субъект доступа.

12.4. Состав событий безопасности обязательной регистрации

12.4.1. В ИС КГКОУ ШИ 3 обязательной регистрации подлежат следующие события информационной безопасности:

– вход (выход), а также попытки входа субъектов доступа в ИС и загрузки (останова) операционной системы (ОС) в составе: дата и время входа (выхода) в систему (из системы) или загрузки (останова) ОС, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) ОС (успешная или неуспешная), идентификатор, предъявленный при попытке доступа;

– запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации, в составе: дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

– подключение машинных носителей информации (МНИ) в составе: дата и время подключения МНИ, логическое имя (номер) подключаемого МНИ;

– попытки несанкционированного доступа к объектам защиты в составе: дата и время попытки несанкционированного доступа к объекту защиты с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства, ПО), логическое имя и тип объекта защиты;

– попытки доступа программных средств к вычислительным сетям, сети Интернет, USB-портам АРМ, приводам оптических дисков, внешним устройствам, программам, томам, каталогам, файлам, средствам защиты информации;

– попытки удаленного доступа в составе: дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа;

– изменение привилегий учетных записей пользователей ИС в составе: дата и время изменения привилегий учетной записи, тип и идентификатор учетной записи, идентификатор субъекта, инициировавшего изменение привилегий, характер изменения привилегий.

12.5. Правила и процедуры сбора, записи и хранения информации о событиях безопасности

12.5.1. Администратор ИБ обеспечивает регистрацию установленных в разделе 12.2 событий безопасности, а также устанавливает состав и содержание регистрируемой информации в соответствии с разделом 12.3 с использованием средств защиты информации, установленных в ИС, в том числе событий обязательной регистрации.

12.5.2. Объем памяти для хранения информации о событиях безопасности рассчитывается Администратором ИБ с учетом типов событий безопасности, их состава, содержания, прогнозируемой частоты возникновения, а также срока их хранения.

12.5.3. Хранение информации о зарегистрированных событиях безопасности и записей системных журналов, которые послужили основанием для регистрации события безопасности, производится в течение трех месяцев.

12.5.4. Средства защиты информации (СрЗИ), применяемые в ИС, настраиваются таким образом, чтобы хранить записи о событиях безопасности в течение 30 дней (минимум). В целях защиты информации о событиях безопасности доступ к настройкам СрЗИ разрешён исключительно Администратору ИБ, попытки изменения настроек средств защиты информации регистрируются в журналах безопасности.

12.5.5. Устранение сбоев при регистрации событий (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) осуществляется администратором ИС в отношении журналов регистрации общесистемного ПО и Администратором ИБ в отношении журналов регистрации СрЗИ.

12.5.6. При переполнении журналов регистрации событий ИБ Администратор ИБ копирует содержимое журналов на учтённый установленным образом носитель информации и очищает журнал. При необходимости увеличивается квота на размер журнала.

12.6. Мониторинг и реагирование на сбои при регистрации событий безопасности

12.6.1. Просмотр журналов событий в ИС осуществляется Администратором ИБ при возникновении инцидента информационной безопасности или, в случае отсутствия инцидентов, не реже одного раза в месяц.

12.6.2. Мониторинг событий безопасности Администратор ИБ производит изучением содержимого журналов СрЗИ с целью выявления инцидентов ИС. При необходимости, для получения полной информации о событии ИБ, Администратор ИБ изучает также журналы ОС и (или) специализированного ПО.

12.6.3. В случае обнаружения сбоев в системе регистрации событий, администратор ИБ:

– выясняет причину сбоя (переполнение журнала, отсутствие связи с базой данных и т.д.).

– устраняет причину сбоя путем изменения параметров регистрации в соответствии с разделами 12.3 – 12.5 настоящей Политики.

12.6.4. При выявлении инцидентов безопасности Администратор ИБ действует в соответствии с процедурами выявления инцидентов и реагирования на них. При обнаружении попыток несанкционированного доступа к ИС Администратор ИБ обязан поставить в известность руководство КГКОУ ШИ 3 и проверить настройки всех СрЗИ, используемых в ИС. Скомпрометированные пароли подлежат немедленной замене.

12.7. Правила и процедуры генерирования временных меток и синхронизации системного временив ИС

12.7.1. Администратор ИБ для каждого узла и сегмента ИС:

– устанавливает службы протокола сетевого времени (NTP) с одними и теми же источниками (NTP-серверами).

– в отсутствии возможности установки службы протокола сетевого времени, производит синхронизацию часов и календаря узлов и сегментов ИС с погрешностью не более одной минуты ежемесячно.

12.8. Методы защиты информации о событиях безопасности

12.8.1. В ИС Администратором ИБ используются следующие методы защиты информации о событиях безопасности:

– логическое ограничение доступа к местам хранения журналов событий.

– управление журналами событий. Доступ к управлению журналами должен быть разрешен только для привилегированных пользователей ИС.

12.8.2. Контроль реализации методов защиты осуществляется Администратором ИБ не реже одного раза в год.

13. ПРАВИЛА АНТИВИРУСНОЙ ЗАЩИТЫ

13.1. Назначение и область действия правил антивирусной защиты

13.1.1. Для антивирусной защиты в ИС КГКОУ ШИ 3 используются антивирусные средства, имеющие действующие сертификаты ФСТЭК России. Администратор ИБ обязан отслеживать срок действия сертификатов и принимать меры в случае истечения сроков действия сертификатов.

13.1.2. Подробные правила, процедуры и действия по обеспечению антивирусной защиты ИС могут быть дополнительно приведены в инструкциях или регламентах по организации антивирусной защиты.

13.2. Процедуры антивирусной защиты

13.2.1. Средства антивирусной защиты (далее – АВЗ) применяются:

– на серверах;
– на автоматизированных рабочих местах (АРМ);
– в виртуальной инфраструктуре;
– в периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), где существует техническая возможность;
– в мобильных технических средствах;
– иных точках доступа в ИС.

13.2.2. Установка, конфигурирование и управление средствами АВЗ осуществляется Администратором ИБ.

13.2.3. Параметры настройки средств АВЗ определяются Администратором ИБ в соответствии с технической документацией.

13.2.4. Все файлы, хранящиеся или копируемые в информационную систему, подлежат обязательной антивирусной проверке. Антивирусные средства настраиваются на автоматическую проверку всех файлов, к которым происходит обращение пользователя / программы / процесса. При подключении к АРМ информационной системы учтённых машинных носителей информации перед началом работы производится их обязательная полная проверка.

13.2.5. На АРМ проводятся следующие виды антивирусных проверок:

– быстрая проверка – при загрузке операционной системы;
– полная проверка – не реже одного раза в неделю.

– подключение съемных носителей информации – принудительно при каждом подключении.

13.2.6. На серверах проводятся следующие виды антивирусных проверок:

– быстрая проверка – при загрузке операционной системы;

– полная проверка – не реже одного раза в неделю;

– подключение съемных носителей информации – принудительно при каждом подключении.

13.2.7. В виртуальной инфраструктуре проводится полная проверка не реже одного раза в неделю:

– проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

– проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

13.2.8. В периметральных средствах защиты информации проводится проверка в режиме реального времени.

13.2.9. В мобильных технических средствах:

– быстрая проверка – при загрузке операционной системы;

– полная проверка – не реже одного раза в неделю;

– проверка устанавливаемого программного обеспечения – принудительно при каждой установке.

13.2.10. Доступ к консоли управления антивирусным средством ограничивается паролем с учетом требований парольной защиты в ИС.

13.2.11. Пользователям запрещается отключать средства АВЗ и самостоятельно вносить изменения в их настройки.

13.2.12. При подключении внешних и съемных носителей информации, в ИС должна проводиться автоматическая быстрая проверка на наличие вирусных программ.

13.2.13. Должна проводиться автоматическая проверка объектов (файлов) при загрузке, открытии или исполнении таких файлов.

13.2.14. Управление средствами АВЗ, при наличии технической возможности, может осуществляться централизованно.

13.2.15. Мониторинг событий средств АВЗ и реагирование на вирусное заражение осуществляется Администратором ИБ. Периодичность мониторинга – не реже одного раза в неделю.

13.2.16. Администратор ИБ по запросу директора КГКОУ ШИ 3 или его заместителя формирует отчет о вирусной активности.

13.3. Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов)

13.3.1. Обновление сигнатур осуществляется в автоматическом режиме по заданному расписанию.

13.3.2. Источником обновлений могут являться:

– серверы обновлений производителей средств АВЗ;
– зеркальный сервер, созданный Администратором ИБ внутри локальной вычислительной сети КГКОУ ШИ 3.

13.3.3. Минимальная периодичность проверки и получения обновлений – один раз в сутки.

13.3.4. Запрещается устанавливать обновление ядра АВЗ.

13.4. Процедуры реагирования на обнаружение в информационной системе вредоносного программного обеспечения

13.4.1. В случае обнаружения вредоносных программ:

– пользователи информационной системы обязаны:
  - приостановить работу на своем компьютере;
  - немедленно сообщить о факте заражения Администратору ИБ;
  - возобновить работу только после удаления вирусной программы и нейтрализации последствий вирусного заражения.

– Администратор ИБ обязан:
  - незамедлительно принять меры по удалению вирусной программы (лечению) и нейтрализации последствий вирусного заражения;
  - при невозможности удаления (лечения) принять меры по нейтрализации возможности деструктивного воздействия со стороны вирусной программы.

13.4.2. В случае выявления инцидентов безопасности Администратор ИБ действует в соответствии с правилами и процедурами выявления инцидентов и реагирования на них. При подозрении на вирусную активность в ИС Администратор

ИБ проводит выборочный антивирусный контроль подозрительных файлов/папок/программ.

13.4.3. Администратор ИБ, при необходимости, инициирует проведение служебного расследования по факту вирусного заражения.

14. ОБНАРУЖЕНИЕ (ПРЕДОТВРАЩЕНИЕ) ВТОРЖЕНИЙ И ПРОЦЕДУРЫ РЕАГИРОВАНИЯ НА НИХ

14.1. Назначение и область действия правил при обнаружении (предотвращению) вторжений

14.1.1. Применяемые системы обнаружения вторжений (далее – СОВ, IDS) должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

14.1.2. Обнаружение вторжений в ИС КГКОУ ШИ 3 обеспечивается применением сертифицированных СОВ.

14.2. Правила установки и администрирования СОВ

14.2.1. СОВ устанавливается на внешней границе ИС с целью предотвращения несанкционированного доступа к информационным ресурсам КГКОУ ШИ 3.

14.2.2. Дополнительно к сетевым системам обнаружения вторжений (NIDS), могут применяться и узловые системы обнаружения вторжений (HIDS).

14.2.3. Администратор ИБ отвечает за правильную настройку решающих правил СОВ и их обновление. Обновление баз решающих правил производится исключительно из доверенных источников. Перед обновлением баз решающих правил администратор безопасности обязан сохранить в резервном файле настройки конфигурации технического средства (ПО) реализующего функции СОВ.

15. КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

15.1. Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей

Анализ защищенности информации заключается в контроле установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

Определяется круг лиц (структурное подразделение) ответственных за выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей. Контроль отсутствия и устранения уязвимостей программного обеспечения ИС осуществляет Администратор ИБ.

Анализ уязвимостей ИС проводится не реже одно раза в квартал.

При выявлении (поиске), анализе и устранении уязвимостей проводится:

– выявление (поиск) уязвимостей, связанных с правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

– разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей;

– анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

– перечень полученных уязвимостей, при наличии возможности, должен быть устранен Администратором ИБ в течении 1 (одного) года путем установки обновлений программного обеспечения, выпущенных производителем программного обеспечения;

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения Администратор ИБ должен предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

15.2. Правила и процедуры контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

15.2.1. Администратором ИБ не реже одного раза в 180 дней должен проводиться:

– контроль работоспособности (неотключения) программного обеспечения и СрЗИ на всех автоматизированных рабочих местах и серверах ИС.

– проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и СрЗИ, объем и содержание которой определяется Администратором ИБ.

15.2.2. Контроль соответствия настроек программного обеспечения и СрЗИ параметрам настройки, приведенным организационно-распорядительных и эксплуатационных документов КГКОУ ШИ 3.

15.2.3. Администратор ИБ, при необходимости, проводит процедуру восстановления работоспособности и настроек функционирования в течении 14 дней после обнаружения несоответствия последних.

15.3. Правила и процедуры контроля состава технических средств, программного обеспечения и средств защиты информации

15.3.1. Администратором ИБ не реже одного раза в 180 дней должен проводиться:

– контроль соответствия состава технических средств, программного обеспечения и СрЗИ ИС, приведенных в техническом паспорте ИС.

15.3.2. Контроль выполнения условий и сроков действия сертификатов соответствия на СрЗИ, использующихся в ИС.

15.3.3. Администратор ИБ, при необходимости, проводит исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и СрЗИ в течении 14 дней после обнаружения несоответствия последних.

15.3.4. В случае если для устранения выявленных недостатков требуется поставка, установка, настройка дополнительных средств защиты, Администратором ИБ производится планирование указанных видов работ на следующий год, в том числе с учетом переаттестации ИС.

15.4. Правила и процедуры контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС

15.4.1. Администратором ИБ не реже одного раза в 180 дней должен проводиться:

– контроль выполнения парольной политики на соответствие правилам и процедурами идентификации и аутентификации субъектов доступа.

– контроль заведения и удаления учетных записей, реализации правил разграничения доступом, реализации полномочий пользователей на соответствие правилам управления доступом субъектов доступа к объектам доступа.

– контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей.

15.4.2. Администратор ИБ, при выявлении нарушений или несоответствий мер, указанных в пункте 15.4.1 настоящего раздела, проводит их устранение в течении 14 дней после обнаружения.

16. МЕРЫ ПО ОБЕСПЕЧЕНИЮ ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ИНФОРМАЦИИ

16.1. Контроль целостности

16.1.1. Контролю целостности в ИС КГКОУ ШИ 3 подлежат компоненты (файлы) ПО средств защиты информации.

16.1.2. В целях оперативного устранения уязвимостей ПО СрЗИ не требуется обязательного ручного подсчёта контрольных сумм файлов и папок, используемого в ИС ПО СрЗИ. Контрольные суммы ПО СрЗИ подсчитываются автоматически за счёт встроенного в СрЗИ функционала подсчёта контрольных сумм.

16.1.3. СрЗИ настраиваются таким образом, чтобы в случае нарушения целостности программного обеспечения СрЗИ производили автоматическую блокировку доступа к информационной системе всем категориям пользователей за исключением Администратора ИБ. В случае блокировки доступа к ИС в результате изменения контрольных сумм файлов, применяемых СрЗИ Администратор ИБ принимает меры для выяснения причин данного инцидента информационной безопасности.

16.2. Порядок периодического анализа уязвимостей ИС и принятия первоочередных мер по устранению вновь выявленных уязвимостей

16.2.1. Обеспечение неизменности среды функционирования направлено на минимизацию возможностей внедрения в ИС КГКОУ ШИ 3 новых, неучтенных при проектировании информационной безопасности уязвимостей, использование которых потенциальными нарушителями безопасности информации может привести к нарушению установленных для обрабатываемой информации характеристик безопасности, а также дискредитации и(или) выводу из строя ИС КГКОУ ШИ 3.

16.2.2. Администратор ИБ проводит антивирусную профилактику информационной системы и производит переустановку программного обеспечения СрЗИ. При выявлении инцидентов информационной безопасности Администратор ИБ действует в соответствии с правилами и процедурами выявления инцидентов и реагирования на них.

16.2.3. Информация о выявленных инцидентах и уязвимостях информационной безопасности копируется на оптические носители сразу после выявления и оформления отчётов по ним. Ответственным за хранение таких дисков является Администратор ИБ.

16.3. Правила и процедуры обеспечения возможности восстановления программного обеспечения

16.3.1. Администратор ИБ обеспечивает возможность восстановления ПО, включая ПО средств защиты информации, при возникновении нештатных ситуаций, предусматривающая:

– принятие планов по действиям персонала при возникновении нештатных ситуаций. Допускается формирование планов в составе правил и процедур контроля и управления физическим доступом;

– восстановление ПО, включая ПО СрЗИ из резервных копий ПО;

– восстановление и проверка работоспособности ПО, включая ПО СрЗИ;

– возврат ИС в начальное состояние, обеспечивающее ее штатное функционирование;

– иные меры, определяемые Администратором ИБ.

16.3.2. В случае сбоя системного программного обеспечения Администратор ИБ производит восстановление его работоспособности с использованием лицензионных дистрибутивов. В случае сбоя ПО СрЗИ администратор ИБ производит восстановление работоспособности системы защиты информации с лицензионных установочных дистрибутивов СрЗИ, имеющих действующие сертификаты ФСТЭК России и/или ФСБ России.

17. ПОРЯДОК ЗАЩИТЫ СРЕДЫ ВИРТУАЛИЗАЦИИ

17.1. Назначение и область действия порядка защиты среды виртуализации

17.1.1. Виртуальная инфраструктура включает среду виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

17.1.2. Порядок защиты среды виртуализации должен исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

17.2. Правила и процедуры идентификации и аутентификации, управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре

17.2.1. В ИС КГКОУ ШИ 3 Администратор ИБ обеспечивает взаимную идентификацию и аутентификацию пользователя и сервера виртуализации (виртуальных машин) при удалённом доступе. Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин Администратор ИБ обеспечивает реализацию правил по идентификации и аутентификации, изложенный в разделе 8, а процедур управления доступом в разделе 9 настоящей Политики.

17.2.2. При реализации процедур по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре должны обеспечиваться:

– идентификация и аутентификация администраторов управления средствами виртуализации;

– идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;

– блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

– защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерного доступа к ней, уничтожения или модифицирования;

– защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;

– идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

17.2.3. При реализации правил по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре должны обеспечиваться:

– контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;

– контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;

– управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;

– контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил).

17.3. Правила и процедуры регистрация событий безопасности в виртуальной инфраструктуре

17.3.1. При реализации процедур по регистрации событий безопасности в виртуальной инфраструктуре дополнительно к событиям, установленным в разделе 12 настоящей Политики, должны подлежать регистрации следующие события:

– запуск (завершение) работы компонентов виртуальной инфраструктуры;

– доступ субъектов доступа к компонентам виртуальной инфраструктуры;

– изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;

– изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

17.4. Рекомендации по управлению (разделению) потоков информации между компонентами виртуальной среды

17.4.1. В ИС КГКОУ ШИ 3, с технологией виртуализации, Администратором ИБ обеспечивается единая точка подключения к виртуальной инфраструктуре (при необходимости резервирования каналов связи, точка подключения должна рассматриваться как комплексное решение, включающее в себя средства взаимодействия с основным и резервными каналами связи).

17.4.2. Администратор ИБ обеспечивает фильтрацию сетевого трафика от (к) каждой гостевой операционной системы, в виртуальных сетях гипервизора и для каждой виртуальной машины.

17.4.3. При реализации правил по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться:

– фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при организации сетевого обмена с сетями связи общего пользования;

– обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности);

– контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объёму и иным характеристикам;

– отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети;

– обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

– обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой) и сетевых потоков виртуальной вычислительной сети;

– семантический и статистический анализ сетевого трафика виртуальной вычислительной сети.

17.5. Порядок контроля резервирования, целостности и перемещения виртуальных машин и обрабатываемой информации

17.5.1. В ИС КГКОУ ШИ 3 Администратор ИБ обеспечивает контроль резервирования и целостности компонентов виртуальной инфраструктуры в соответствии с разделом 16 настоящей Политики.

17.5.2. Администратор ИБ обеспечивает контроль целостности резервных копий виртуальных машин (контейнеров).

17.5.3. При реализации порядка контроля целостности компонентов виртуальной инфраструктуры должны обеспечиваться:

– контроль целостности состава и конфигурации виртуального оборудования;

– контроль целостности компонентов, критически важных для функционирования хостовой ОС, гипервизора, гостевых ОС и (или) обеспечения безопасности, обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);

– контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;

– контроль целостности базовой системы ввода-вывода вычислительных серверов и консолей управления виртуальной инфраструктуры;

– контроль состава аппаратной части компонентов виртуальной инфраструктуры;

– контроль целостности файлов-образов виртуализированного ПО и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы).

17.5.4. В ИС КГКОУ ШИ 3 Администратором ИБ обеспечивается перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных в пределах информационной системы только на контролируемые им (или уполномоченным лицом) технические средства (сервера виртуализации, носители, системы хранения данных).

17.5.5. Администратор ИБ осуществляет обработка отказов перемещения виртуальных машин (контейнеров) и обрабатываемых на них данных.

17.5.6. При перемещении виртуальных машин (контейнеров) и обрабатываемой информации должны обеспечиваться:

– регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);

– управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации;

– управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);

– управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

17.5.7. Управление перемещением виртуальных машин (контейнеров) предусматривает:

– полный запрет перемещения виртуальных машин (контейнеров);

– ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);

– ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

18. РЕГЛАМЕНТЫ РЕЖИМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПОМЕЩЕНИЙ И ТЕХНИЧЕСКИХ СРЕДСТВ

18.1. Назначение и область действия регламентов защиты технических средств. Контроль состава технических средств

18.1.1. К использованию в ИС КГКОУ ШИ 3 допускаются только те ТС или компоненты ТС, которые перечислены в документе «Технический паспорт».

18.1.2. Для мобильных ТС в ИС установлены следующие правила использования:

– мобильные ТС подлежат учету;

– мобильные ТС выдаются пользователям под роспись;

– при передаче мобильных ТС между пользователями или в сторонние организации должно производиться уничтожение (стирание информации).

18.1.3. В ИС запрещаются к использованию мобильные ТС, не входящие в ее состав, в том числе мобильные ТС, находящиеся в личном пользовании пользователей ИСПДн, и мобильные ТС информации, в отношении которых невозможно установить их принадлежность (владельца).

18.1.4. Решение об использовании в составе ИС ТС, не соответствующих перечню ТС, приведенному в документе «Технический паспорт» ИС, принимается в соответствии с порядком управления конфигурацией и в случае их дальнейшей необходимости использования, соответствующие ТС вносятся установленным порядком в «Технический паспорт».

18.1.5. В случае выявления несоответствия состава технических средств, используемых в ИС, перечню технических средств, приведенному в документе «Технический паспорт», Администратор ИБ должен исключить несанкционированное использование несоответствующих ТС.

18.2. Правила и процедуры организации контролируемой зоны

18.2.1. Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

18.2.2. КЗ для ТС ИС КГКОУ ШИ 3 определяется Администратором ИБ.

18.2.3. Для ИС может быть организовано несколько контролируемых зон.

18.3. Правила и процедуры контроля и управления физическим доступом к ТС, СрЗИ, СКЗИ, а также в помещения, в которых они установлены

18.3.1. В контролируемой зоне должен обеспечиваться контроль и управление физическим доступом к техническим средствам.

18.3.2. Доступ в помещения ИС КГКОУ ШИ 3 осуществляется в соответствии с «Перечнем лиц, имеющих право доступа в помещения КГКОУ ШИ 3».

18.3.3. Для обеспечения пункта 18.3.1 этого раздела применяются следующие технические средства:

– двери, расположенные по периметру контролируемой зоны, должны быть оборудованы механическим замком;

– окна, расположенные по периметру контролируемой зоны, должны быть оснащены системами открывания с внутренней стороны;

– дополнительно могут применяться системы контроля и управления доступом, металлические решетки на окнах, охранные датчики (движения, открытия, разбития стекол и т.д.), видеонаблюдение.

18.3.4. Для обеспечения пункта 18.3.1 настоящего раздела Политики применяются следующие организационные меры:

– Администратором ИБ составляются список лиц, допущенных к ТС, средствам защиты информации, средствам обеспечения функционирования, а также в помещения, в которых они установлены;

– запрещается оставлять помещение незапертым в моменты отсутствия в нем лиц, допущенных в контролируемую зону.

– должностным лицом, ответственным за помещение, осуществляется учет физического доступа сторонних лиц, не являющихся работниками КГКОУ ШИ 3 и сотрудниками охранного предприятия КГКОУ ШИ 3, к ТС, средствам защиты информации, средствам обеспечения функционирования, а также в помещения, в которых они установлены.

18.4. Правила и процедуры размещения устройств вывода (отображения и печати) информации

18.4.1. В качестве устройств вывода (отображения) информации в ИС рассматриваются экраны мониторов автоматизированных рабочих мест пользователей.

18.4.2. Устройства вывода (отображения) информации должны располагаться таким образом, чтобы была исключена или сведена к минимуму возможность просмотра информации посторонними лицами.

18.4.3. Размещение устройств вывода (печати) защищаемой информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Устройства вывода (печати) информации не должны быть размещены напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

18.4.4. Потенциальные направления визуального съема информации определяются Администратором ИБ.

18.4.5. Администратор ИБ контролирует расположение устройств вывода (отображения и печати) информации и их изменение расположения пользователями.

18.4.6. Администратор ИБ должен исключить нахождение в помещениях ИС лиц, которым не разрешен доступ к ТС и защищаемой информации, оконные жалюзи помещений при работе с защищаемой информацией закрываются. При необходимости проведения в помещении ИС каких-либо работ, не связанных с обработкой информации, АРМ данной ИС блокируется, монитор выключается, документы, содержащие защищаемую информацию, убираются в сейф или запирающийся ящик стола. Персонал сторонних организаций производит работы исключительно в сопровождении работника ИС КГКОУ ШИ 3. Проведение таких работ производится с разрешения Директора КГКОУ ШИ 3.

19. ПРАВИЛА ЗАЩИТЫ ИС, ЕЕ СРЕДСТВ, СИСТЕМ СВЯЗИ И ПЕРЕДАЧИ ДАННЫХ

19.1. Назначение и область действия правил защиты ИС ее средств, систем связи и передачи данных

19.1.1. В ИС осуществляется разделение полномочий на администраторские и пользовательские. Пользовательские полномочия (права) используются исключительно для обработки информации, администраторские полномочия (права) используются исключительно для настройки параметров ОС, ПО и СрЗИ ИС. Настройка средств защиты информации разрешается исключительно локальным доступом к АРМ ИС.

19.1.2. При технологической необходимости удалённый доступ к АРМ ИС КГКОУ ШИ 3 может быть разрешен директором КГКОУ ШИ 3, по представлению Администратора ИБ, для проведения работ исключительно на разовой основе, после проведения таких работ удалённый доступ блокируется.

19.1.3. Использование технологии мобильного кода (Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация, VBScript и т.п.) разрешается исключительно в служебных целях.

19.2. Правила и процедуры обеспечения защиты информации при ее передаче по каналам связи, имеющим выход за пределы КЗ

19.2.1. Защита систем связи и передачи данных заключается в обеспечении безопасности защищаемой информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

19.2.2. Запрещается передача защищаемой информации по открытым каналам связи за пределы контролируемой зоны без применения сертифицированных по требованиям безопасности средств криптографической защиты информации (СКЗИ).

19.3. Правила и процедуры применения видеокамер, микрофонов и иных периферийных устройств

19.3.1. В ИС запрещено применение видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно или которые имеют возможность управления через компоненты программного обеспечения,

установленных на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы).

19.4. Правила и процедуры применения беспроводных соединений

19.4.1. В ИС запрещено применять беспроводные соединения, за исключением следующих случаев:

– технологией работы в ИС предусмотрено использование беспроводных технологий;

– между узлами беспроводной сети обеспечивается шифрование трафика сертифицированными ФСБ России средствами криптографической защиты.

19.4.2. Обеспечивается защита беспроводных точек доступа при подключении вариантом hot-spot (через точку доступа) следующими механизмами:

– блокировка широковещательных передач узлом доступа (режим скрытого идентификатора сети).

– фильтрация доступа клиентов сети по MAC-адресам по «белому списку».

– использование сложного ключа доступа к сети (более 8 символов, отвечает требованиям к сложности, периодическая смена и др.);

– использование в качестве метода аутентификации и шифрования технологию WPA. Рекомендуется применять технологию WPA корпоративного уровня (WPA 2 Enterprise).

19.5. Правила и процедуры защиты мобильных технических средств

19.5.1. К мобильным техническим средствам, в рамках настоящей Политики, относятся портативные вычислительные устройства и устройства связи с возможностью обработки информации (например: ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).

19.5.2. Мобильные технические средства, используемые в ИС должны рассматриваться как отдельный сегмент ИС (мобильный сегмент).

19.5.3. В качестве мер обеспечения безопасности информации, обрабатываемой в мобильном сегменте, службой ИТ должны быть реализованы, в том числе, следующие меры:

– очистка (удаление) информации в мобильном техническом средстве после завершения сеанса удаленного доступа к защищаемой информации или принятие иных мер, исключающих несанкционированный доступ к хранимой защищаемой информации;

– уничтожение съемных машинных носителей информации, которые не подлежат очистке;

– выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации).

19.5.4. Запрет возможности автоматического запуска (без команды пользователя) в ИС ПО на мобильных технических средствах.

20.ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ И РЕАЛИЗАЦИИ ПРОГРАММ ПО ОБУЧЕНИЮ И ПОВЫШЕНИЮ ОСВЕДОМЛЕННОСТИ В ОБЛАСТИ ИБ

20.1.1. В ходе организации программ по обучению и повышению осведомленности в области ИБ осуществляются:

– работа с персоналом и клиентами в направлении повышения осведомленности и обучения в области ИБ, санкционированная руководством КГКОУ ШИ 3;

– разработка планов, программ обучения и повышения осведомленности в области ИБ. По результатам выполнения указанных планов должна осуществляться проверка полученных знаний. В планах обучения и повышения осведомленности должны быть установлены требования к периодичности обучения и повышения осведомленности;

– ведение перечня свидетельств программ обучения и повышения осведомленности в области ИБ. В частности, такими свидетельствами могут являться:

- документы (журналы), подтверждающие прохождение руководителями и работниками КГКОУ ШИ 3 обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых;
- документы, содержащие результаты проверок обучения работников КГКОУ ШИ 3;
- документы, содержащие результаты проверок осведомленности в области ИБ на КГКОУ ШИ 3.

21. ОТВЕТСТВЕННОСТЬ

21.1.1. Ответственность за соблюдение настоящей Политики возлагается на всех работников Оператора, на которых распространяются эта Политика.

21.1.2. Лица, виновные в нарушении настоящей Политики и требований законодательства в области информационной безопасности, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность

21.1.3. Ответственность за осуществление общего контроля выполнения требований Политики несет Ответственный за организацию обработки персональных данных и Администратор ИБ.

21.1.4. С настоящей Политикой знакомятся под подпись все работники КГКОУ ШИ 3, на которых распространяется действие этой Политики.

22. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящая Политика является внутренним документом Оператора.

Требования настоящей Политики могут развиваться другими внутренними нормативными документами КГКОУ ШИ 3, которые дополняют и уточняют ее.

22.1. Изменения и пересмотр документа

22.1.1. Политика пересматривается, изменяется и дополняется по мере необходимости, но не реже одного раза в три года.

22.1.2. Проверка и пересмотр настоящей Политики осуществляется в следующих случаях:

– при внедрении новой техники и (или) технологий;

– при внедрении новых СрЗИ, существенно изменяющих порядок работы с ними;

– в случае изменения процессов обработки и защиты информации в ИС;

– при выявлении новых угроз безопасности информации и определении необходимости реализации дополнительных защитных мер;

– по результатам анализа материалов расследования нарушений требований законодательства об обеспечении безопасности информации;

– при повышении уровня защищенности;

– по требованию представителей ФСБ России и ФСТЭК России.

22.1.3. Настоящая Политика подлежит обязательному пересмотру в случае изменения законодательства Российской Федерации в области защиты информации.

22.1.4. Политика подлежит полному пересмотру при изменении перечня решаемых задач, состава ТС и программных средств ИС на КГКОУ ШИ 3, приводящих к существенным изменениям технологии обработки информации.

22.1.5. Политика подлежит частичному пересмотру в остальных случаях.

22.1.6. В зависимости от изменяющихся условий деятельности КГКОУ ШИ 3 проводится корректировка правил и процедур по защите информации.

22.1.7. Вносимые изменения не должны противоречить другим разделам Политики.

22.1.8. Ответственность за своевременные изменения и корректировки настоящей Политики возлагается на Администратора ИБ и Ответственного за организацию обработки персональных данных.

22.1.9. С приказом о внесении изменений (дополнений) в настоящую Политику знакомятся под расписку все работники КГКОУ ШИ 3, на которых распространяется действие этой Политики.

22.2. Порядок утверждения

22.2.1. Политика вступает в силу с момента его утверждения директором КГКОУ ШИ 3 и действует бессрочно, до замены ее новой Политикой. Все изменения в Политику вносятся на основании решения руководителя Оператора в установленном порядке.

22.2.2. С настоящей Политикой знакомятся под подпись все работники КГКОУ ШИ 3, на которых распространяется действие этой Политики.

Приложение № 1
к Политики по обеспечению
информационной безопасности
от «___» _____ 201__ г. № ____

Форма Журнала

учета инцидентов информационной безопасности

№ п/п	Номер инцидента	Описание инцидента	Дата и время регистрации инцидента	Дата и время закрытия инцидента	Действия по реагированию на инцидент	Ф. И. О. Администратора ИБ	Подпись Администратора ИБ
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1.							
2.							
3.							
…							
N							

Приложение № 2
к Политики по обеспечению
информационной безопасности
от «___» _____ 201__ г. № ____

Форма Журнала

учета изменений в конфигурации

№ п/п	Дата и время внесения изменения	Цель проведения изменения	Отчет об проведения изменения	Компоненты, затронутые изменением	Ф. И. О. лица, проводившего изменение	Подпись лица, проводившего изменение	Ф. И. О. Администратора ИБ	Подпись Администратора ИБ
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1.								
2.								
3.								
…								
N								

Приложение № 3
к Политики по обеспечению
информационной безопасности
от «___» _____ 201__ г. № ____

Форма Журнала
учета машинных носителей информации (МНИ)

№ п/п Рег. № МНИ	Наименование МНИ	Заводской номер	ФИО сотрудника, поставившего МНИ на учет	Отметка о выдаче		Отметка о получении		Отметка о возврате			Отметка об уничтожении			Примечания
				ФИО сотрудника, выдавшего МНИ	Дата выдачи	ФИО сотрудника, получившего МНИ	Дата получения	Дата возврата	сотрудника, вернувшего МНИ (получатель из	Роспись сотрудника, получившего МНИ	Дата уничтожения	ФИО сотрудника, уничтожившего МНИ	Номер акта уничтожения МНИ	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1.														
2.														
…														
N														

Приложение № 4
к Политики по обеспечению
информационной безопасности
от «___» _____ 201__ г. № ____

Форма Журнала

вывода из эксплуатации технических средств (ТС)

№ п/п	Заводской номер	Наименование программно-технического средства	Место установки (использования)	Причина вывода из эксплуатации	Ответственное должностное лицо (Ф. И. О., дата, подпись)
1	2	3	4	5	6
1.					
2.					
3.					
…					
N					

Лист ознакомления
с политикой по обеспечению информационной безопасности
Краевого государственного казенного общеобразовательного учреждения для детей-сирот и детей, оставшихся без попечения родителей, реализующее адаптированные основные общеобразовательные программы «Школа-интернат № 3»

№ п/п	Фамилия, имя, отчество	Дата ознакомления	Подпись