ГБОУ РХ «Черногорская школа-интернат»

СОГЛАСОВАНО на общем собрании трудового коллектива Протокол № ___ от «___»____2022 г.	УТВЕРЖДАЮ и. о. директора _____С.И. Бутенко Приказ № ___от «___»____2022 г.

ИНСТРУКЦИЯ № 12
по обеспечению безопасности персональных данных

1. Обязанности ответственного за обеспечение безопасности персональных данных информационных систем персональных данных (далее – Ответственный) в ГБОУ РХ «Черногорская школа-интернат» (далее – ОУ)

1.1. Идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1)

Ответственный создает, удаляет и блокирует учетные записи пользователей для осуществления аутентификации пользователя с использованием аутентификации аппаратно-программного средства защиты от несанкционированного доступа (Электронный замок «Соболь»).

1.2. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации (ИАФ.4)

Ответственный является ответственным за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации аппаратно-программного средства защиты от несанкционированного доступа (Электронный замок «Соболь»).

1.3. Управление доступом субъектов доступа к объектам доступа. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13)

Меры по реализации защищенного удаленного доступа субъектов доступа к объектам доступа внутри сети реализуются при помощи подсистемы защиты информационной системы, её средств и систем связи и передачи данных (ЗИС) средствами криптографической защиты. Меры по реализации защищенного удаленного доступа субъектов через внешние информационно-телекоммуникационные сети в информационную систему реализуются при помощи Подсистемы межсетевого экранирования, подсистемы криптографической защиты, обнаружения вторжений.

1.4. Управление доступом субъектов доступа к объектам доступа. Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) (УПД.16)

Ответственный обеспечивает взаимодействие с внешними информационными системами в целях межведомственного электронного взаимодействия, исполнения государственных и муниципальных функций, формирования базовых государственных информационных ресурсов и выполнение следующих функции:

предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям в соответствии с «Положение о разграничении прав доступа к персональным данным» (матрица доступа), УПД.2;

выполнение требований и регламентов взаимодействия с информационными системами сторонних организаций.

1.5. Управление доступом субъектов доступа к объектам доступа. Обеспечение доверенной загрузки средств вычислительной техники (УПД.17)

Правила и процедуры обеспечения доверенной загрузки средств вычислительной техники регламентируются в соответствии с эксплуатационной документацией на программные и аппаратно-программного средства доверенной загрузки и защиты от несанкционированного доступа.

1.6. Ограничение программной среды. Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения(ОПС.2)

Администратор Системы осуществляет контроль и управление установкой (инсталляцией) компонентов программного обеспечения информационной системы.

Компоненты программного обеспечения (состава и конфигурации), подлежащие установке перечислены в разделе (ОПС.3)

Техническая реализация контроля управления установкой осуществляется встроенным функционалом СЗИ и средствами групповых политик контроллера домена.

1.7. Ограничение программной среды. Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов (ОПС.3)

Компоненты программного обеспечения (состава и конфигурации), подлежащие установке в информационной системе после загрузки операционной системы:

конфигурации, предусматривающие включение в домен;

пакет Microsoft office;

браузер

архиватор

приложение для просмотра PDF, FoxitReader

специализированное программное обеспечения для сканирования документов

драйверы для периферийных устройств

сертифицированные средства защиты инофрмации

антивирусное программное обеспечение.

Данный перечень может дополняться ответственным за обеспечение безопасности персональных данных. Техническая реализация запрета на установку осуществляется встроенным функционалом СЗИ и средствами групповых политик контроллера домена.

1.8. Защита машинных носителей информации. Учет машинных носителей информации (ЗНИ.1)

Ответственный обеспечивает учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации. Учету подлежат:

съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера. Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации. Учет

встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в Журнале учета мобильных технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом. Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или Журнал учета мобильных технических средств указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации. Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш- накопители, съемные жесткие диски).

1.9. Защита машинных носителей информации. Управление доступом к машинным носителям информации (ЗНИ.2)

Ответственный за организацию обработки персональных данных определяет (утверждает) перечень должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим:

съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках);

в Перечне отражается предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций);

1.10. Защита машинных носителей информации. Контроль использования интерфейсов ввода (вывода) (ЗНИ.5)

В случае отсутствия необходимости в использовании машинных носителей информации Ответственным применяются меры, исключающих возможность использования запрещенных интерфейсов ввода (вывода).

В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода), могут применяться:

опечатывание интерфейсов ввода (вывода);

использование механических запирающих устройств;

удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода);

применение средств защиты информации, обеспечивающих контроль

использования интерфейсов ввода (вывода).

Для проведения мероприятий по контролю использования интерфейсов ввода (вывода) Ответственный пользуется перечнем должностных лиц, имеющих физический доступ к машинным носителям информации.

1.11. Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) (ЗНИ.8)

Уничтожение (стирание) информации на машинных носителях исключает возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации. Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации возлагается на Ответственного. Для выполнения данных процедур Ответственным используется средство контроля защищенности от несанкционированного

доступа сертифицированная программа поиска и гарантированного уничтожения информации на дисках TERRIER (версия 3.0). Эксплуатационная документация и формуляр поставляются вместе с средством контроля защищенности от несанкционированного доступа.

1.12. Определение событий безопасности, подлежащих регистрации, и сроков их хранения (РСБ.1)

Ответственный в настройках СЗИ от НСД подсистемы РСБ определяет следующий перечень событий безопасности, подлежащий обязательному регистрированию:

вход (выход), а также попытки входа субъектов доступа в АРМ и АИС ОУ и загрузки (остановки) ОС;

подключение машинных носителей информации и вывод информации на носители информации;

запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой ПДн;

попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

попытки удаленного доступа.

1.13. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации (РСБ.2)

Ответственный в настройках СЗИ от НСД подсистемы РСБ в соответствии с эксплуатационной документацией определяет следующие состав и содержание информации о событиях безопасности при регистрации входа (выхода) субъектов доступа:

дата и время входа (выхода) в (из) АИС ОУили загрузки (остановки) ОС;

результат попытки входа (успешная или неуспешная);

результат попытки загрузки (остановки) ОС АРМ и серверов (успешная или неуспешная);

идентификатор, предъявленный при попытке доступа.

Ответственный в настройках СЗИ от НСД подсистемы РСБ в соответствии с эксплуатационной документацией определяет следующие состав и содержание информации о событиях безопасности при регистрации подключения машинных носителей информации и вывода информации на носители информации:

дата и время подключения машинных носителей информации и вывода информации на носители информации;

логическое имя (номер) подключаемого машинного носителя информации;

идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

Ответственный в настройках СЗИ от НСД подсистемы РСБ в соответствии с эксплуатационной документацией определяет следующие состав и содержание информации о событиях безопасности при регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой ПДн:

дата и время запуска;

имя (идентификатор) программы (процесса, задания);

идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание);

результата запуска (успешного, неуспешного).

Ответственный в настройках СЗИ от НСД подсистемы РСБ в соответствии с эксплуатационной документацией определяет следующие состав и содержание информации о событиях безопасности при регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам:

дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная);

идентификатор субъекта доступа (устройства);

спецификация защищаемого файла (логическое имя, тип).

Ответственный в настройках СЗИ от НСД подсистемы РСБ в соответствии с эксплуатационной документацией определяет следующие состав и содержание информации о событиях безопасности при регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним:
дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная);
идентификатор субъекта доступа (устройства);
спецификация защищаемого объекта доступа (логическое имя (номер).
Ответственный в настройках СЗИ от НСД подсистемы РСБ в соответствии с эксплуатационной документацией определяет следующие состав и содержание информации о событиях безопасности при регистрации попыток удаленного доступа к АИС ОУ :
дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная);
идентификатор субъекта доступа (устройства);
используемый протокол доступа;
используемый интерфейс доступа и (или) иная информация о попытках удаленного доступа к АИС _____ .
1.14. Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти (РСБ.4)
Ответственный осуществляет восстановление после сбоев функционала регистрации событий безопасности СЗИ от НСД в соответствии с эксплуатационной документацией.
1.15. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5)
Ответственный должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности СЗИ от НСД и реагирование на них.
Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии с РСБ.1, и с периодичностью, установленной в ОУ для АИС ОУ, и обеспечивающей своевременное выявление признаков инцидентов безопасности в АИС ОУ.
В случае выявление признаков инцидентов безопасности в АИС ОУ осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности
1.16. Генерирование временных меток и (или) синхронизация системного времени в информационной системе
Ответственный с помощью средств МЭ ПАК «ViPNetCoordinatorHW» проводит аудит корректности работы внутренних системных часов АРМ пользователей и серверов АИС ОУ.
1.17.Защита информации о событиях безопасности
Доступ к записям аудита и функциям управления механизмами регистрации (аудита) СЗИ от НСД должен предоставляться только уполномоченным должностным лицам.
Действия пользователей, администратора системы и Ответственного регламентируются инструкцией по организации антивирусной защиты.
1.18. Выявление, анализ и устранение уязвимостей информационной системы (АН3.1)
Процедуры выявления (поиска), анализа и устранения уязвимостей на комплексе СВТ АИС ОУ проводятся как в автоматическом режиме, так и ответственным сотрудником оператора с утвержденной периодичностью. В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей. Процедура обновления

Системного ПО на АРМ проводится в автоматическом режиме не реже 1 раза в неделю. Процедура обновления Системного ПО на серверах проводится в ручном режиме ежемесячно. Процедура обновления баз данных СОВ проводится ежедневно в автоматическом режиме. Ответственный взаимодействует с разработчиками АИС ОУ для определения анализа уязвимостей. Ответственным за проведение процедур анализа и устранения уязвимостей является Ответственный.

1.19. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации (АН3.2)

Процедуры контроля установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и базовое программное обеспечение на комплексе СВТ АИС _____ проводятся как в автоматическом режиме, так и ответственным сотрудником оператора с утвержденной периодичностью.

Ответственным за процедуру контроля установки обновлений является Ответственный. Ответственный проводит ежеквартальный контроль установки обновлений, который состоит из проверки соответствия версий общесистемного, прикладного и специального программного обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

После проведения данных процедур ответственный фиксирует результат проведения контроля в журнал событий информационной безопасности.

1.20. Контроль состава технических средств, программного обеспечения и средств защиты информации (АН3.4)

Процедуры контроля состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация) проводится Ответственным один раз в год.

При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;

контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

После проведения данных процедур ответственный фиксирует результат проведения контроля в журнал событий информационной безопасности.

1.21. Контроль целостности ПО, включая ПО средств защиты информации

Ответственный в настройках СЗИ от НСД в соответствии с эксплуатационной документацией для подсистемы ОЦЛ включает контроль:

целостности ПО СЗИ, включая их обновления, по наличию имен (идентификаторов) и по контрольным суммам компонентов СЗИ в процессе загрузки и динамически в процессе работы ОС;

целостности компонентов прикладного ПО, участвующего в обработке ПДн, по наличию имен (идентификаторов) компонентов ПО и по контрольным суммам в процессе загрузки ОС;
применения средств разработки и отладки программ в составе программных средств ОС и АИС ОУ.
Ответственный ежеквартально осуществляет тестирование функций безопасности СЗИ, в том числе с помощью тест-программ, имитирующих попытки НСД, и специальных программных средств, в соответствии с АН3.1 и АН3.2.
1.22. Обеспечение возможности восстановления ПО, включая ПО СЗИ, при возникновении нештатных ситуаций.
Для обеспечения возможности восстановления ПО АИС ОУ и ПО СЗПДн в ОУ разработана инструкция по резервированию и восстановлению работоспособности при возникновении нештатных ситуаций, которая предусматривает:
восстановление ПО АИС ОУ, в том числе ПО СЗИ, из резервных копий (дистрибутивов) ПО согласно эксплуатационной документации;
восстановление и проверка работоспособности СЗПДн, обеспечивающая необходимый уровень защищенности ПДн;
возврат ОС на АРМ и серверах в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование.
При невозможности восстановить работоспособность ПО из резервных копий, администратору системы и Ответственному подлежит произвести переустановки необходимого ПО, входящего в состав АИС ОУ, и ПО СЗИ соответственно, согласно эксплуатационной документации.
Перед выполнением данных действий администратору системы и Ответственному необходимо произвести резервное копирование БД АИС ОУ и настроек ПО СЗИ соответственно, если это представляется возможным.
1.23. Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)
Ответственный в настройках МЭ в соответствии с эксплуатационной документацией для подсистемы ОЦЛ включает следующие механизмы защиты:
фильтрацию по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным или эвристическим методами;
фильтрацию на основе информации об отправителе электронного сообщения, в том числе с использованием «черных» списков запрещенных отправителей или «белых» списков разрешенных отправителей.
Администратор безопасности осуществляться обновление базы «черных» или «белых» списков еженедельно и проводит контроль целостности обновленных баз.
1.24. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование (ОДТ.3)
Ответственный осуществляет контроль безотказного функционирования технических средств, обнаружение и локализацию отказов функционирования, принимает мер по восстановлению отказавших средств и их тестирование.
Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования информационной системы путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия "ответов", визуального контроля, контроля трафика, контроля "поведения" системы или иными методами). При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению

отказавших средств тестирование в соответствии с эксплуатационной документацией. События заносятся в журнал событий информационной безопасности.

1.25. Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2). Контроль и управление физическим доступом к техническим средствам (ЗТС.3)

Для АИС в ОУ приняты следующие меры, по обеспечению организации контролируемой зоны:

утверждены границы контролируемой зоны ОУ;

обеспечен доступ на территорию контролируемой зоны лицам, ответственным за обработку персональных данных в АИС ОУ, в соответствии с Порядком доступа сотрудников ОУ в помещения, в которых ведется обработка персональных данных.

с сотрудниками осуществляющими системно-техническое обслуживание программного обеспечения и оборудования АИС ОУ подписаны обязательства о неразглашении информации, содержащей персональные данные.

В ОУ используется контрольно пропускной режим. Осуществляется видеоконтроль, утверждено Положение о СКУД.

1.26. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4)

Работы по размещению устройств вывода (отображения) информации осуществляются с участием Ответственного. Во время работы должны быть соблюдены требования, исключающие несанкционированный просмотр экранов мониторов автоматизированных рабочих мест пользователей, мониторов консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанелей, видеостен и других средства визуального отображения защищаемой информации, печатающих устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональных устройств.

Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

2. Обязанности администратора системы АИС

2.1. Идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1)

Администратор Системы создает, удаляет и блокирует учетные записи пользователей для осуществления аутентификации пользователя с использованием паролей. В АИС ОУ при помощи средств операционной системы обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

2.2. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных (ИАФ.2)

Администратор Системы до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) осуществляет процедуру занесения идентификационных данных новых устройств в фильтры таблицы имен устройств/ID/IP/MAC адресов, на межсетевых экранах, осуществлять поддержание данных таблиц в актуальном состоянии.

2.3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (ИАФ.3)

Администратор Системы является ответственным за создание, присвоение и уничтожение идентификаторов пользователей в СУБД. Функциональные возможности

сертифицированной СУБД используются для осуществления идентификации пользователей и (или) устройств, в том числе блокирования, исключения повторного использования и удаление. Подробный перечень мер по выполнению требований ИАФ.1 и ИАФ.3 представлен в «Инструкции по организации парольной защиты».

Управление доступом субъектов доступа к объектам доступа. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации (УПД.11)

При необходимости Администратором Системы может быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации. Данные функциональные возможности реализуются путем разрешения (запрета) действий пользователей, разрешенных до идентификации и аутентификации (гостевые учетные записи) при помощи локальной (групповой доменной) политики безопасности.

Перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации:

Локальный вход на АРМ под гостевой учетной записью.

Запуск браузера, доступ к разрешенным сайтам в Интернете.

(Данный пункт предусматривает типовое рабочее место общественного доступа)

2.4. Управление доступом субъектов доступа к объектам доступа. Регламентация и контроль использования в информационной системе мобильных технических средств (УПД.15)

В ИСПДн разрешены к использованию только учтенные мобильные технические средства. Администратор Системы ведет журнал учета мобильных технических средств, съемных машинные носителей информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативных вычислительных устройств и устройств связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства), выданных сотрудникам, и осуществляет регулярный контроль использования только учтенных мобильных технических средств.

2.5. Периодическое резервное копирование информации на резервные машинные носители информации (ОДТ.4). Обеспечение возможности восстановления информации с резервных копий в течение установленного времени (ОДТ.5)

В АИС ОУ проводится еженедельное полное резервное копирование всех СУБД, и ежедневные инкрементные резервные копии в ночное время.

Ответственным за осуществление резервного копирования в АИС ОУ является Администратор Системы.

В составе комплекса СВТ АИС ОУ входит программно аппаратный комплекс резервного копирования, состоящий из ленточной библиотеки и позволяющий выполнять следующие функции:

суммарный объем резервируемых данных принять как 1 ТБ.

предполагаемый прирост объема резервируемых данных составляет около 50% в год.

система обеспечивает время восстановления данных любой из действующих подсистем в течение 24-х часов.

возможность создания резервных копий данных всех эксплуатируемых информационных систем;

возможность создания иерархических резервных копий с различными показателями по скорости восстановления и стоимости хранения;

защита от несанкционированного доступа (НСД), компоненты подсистемы защиты от НСД обеспечивают идентификацию и аутентификацию администраторов с проверкой его полномочий и прав доступа.

События, связанные с восстановление данных из резервных копий заносятся в журнал событий информационной безопасности.

2.6. Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации (ОДТ.7)

Администратор системы осуществляет контроль состояния и качества предоставления провайдером вычислительных ресурсов (мощностей), в том числе по передаче информации, предусматривающий:

контроль выполнения провайдером требований о защите информации, установленных законодательством Российской Федерации и условиями договора (соглашения), на основании которого уполномоченное лицо обрабатывает информацию или предоставляет вычислительные ресурсы (мощности);

мониторинг состояния и качества предоставления провайдером вычислительных ресурсов (мощностей);

мониторинг состояния и качества предоставления провайдером услуг по передаче информации.

Условия, права и обязанности, содержание и порядок контроля должны определяться в договоре (соглашении), заключаемом между оператором и уполномоченным лицом на предоставление вычислительных ресурсов (мощностей) или передачу информации с использованием информационно-телекоммуникационных сетей связи.

События, связанные нарушением состояния и качества предоставления провайдером вычислительных ресурсов (мощностей) заносятся в журналсобытий информационной безопасности.