ПРИЛОЖЕНИЕ № 1
к приказу директора МБОУ СОШ им. Героя
Советского Союза Э.Асхарова с.Зильги
№ 83.2 от «05» сентября 2022 г.

ПОЛИТИКА
обеспечения информационной безопасности муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания

Раздел I
Общие положения

Политика обеспечения информационной безопасности (далее – Политика) муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания (далее – Учреждение) определяет порядок и процедуры обеспечения безопасности информации, обрабатываемой в сегменте информационной системы Министерства образования и науки Республики Северная Осетия-Алания в муниципальном бюджетном образовательном учреждении «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания (далее – сегмент ИС).

Настоящая Политика регламентирует следующие организационные и технические мероприятия обеспечения информационной безопасности:

— порядок использования информационных ресурсов Учреждения и предоставления доступа к ним;

— порядок антивирусной защиты информации;

— порядок парольной защиты;

— порядок обеспечения отказоустойчивости информационных ресурсов;

— порядок обеспечения сетевой безопасности;

— порядок проведения аудита информационной безопасности.

Настоящая Политика разработана в соответствии с:

— Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

— Федеральным законом от 27.07.2008 № 152-ФЗ «О персональных данных»;

— Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

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

Раздел II
Порядок инвентаризации, учёта и эксплуатации средств вычислительной техники

Проведение инвентаризации и учёта является необходимым аспектом обеспечения безопасности информации. Учёту подлежат:

— автоматизированные рабочие места пользователей (далее - АРМ);

— съемные машинные носители информации (формы журналов учёта съемных носителей информации приведены в приложении № 1 к настоящей Политике);

— системное и прикладное программное обеспечение, используемое в СВТ;

— средства защиты информации.

Учёт машинных носителей информации, встроенных в корпуса АРМ, ведётся в составе этих технических средств.

Средства вычислительной техники и средства защиты информации учитываются в Техническом паспорте сегмента ИС.

Пользователь средства вычислительной техники сегмента ИС – сотрудник Учреждения, которому предоставляется доступ к информации, содержащейся в сегменте ИС, а также обрабатываемой техническим средством.

Администратор средства вычислительной техники сегмента ИС – сотрудник Учреждения или иное уполномоченное лицо, которое обеспечивает установку, настройку, конфигурацию (в том числе изменение прав доступа) к средству вычислительной техники.

Доступ к информации – возможность получения информации и её использования.

Каждый пользователь, обеспеченный АРМ, получает аутентификационную информацию (персональное сетевое имя (имя пользователя), пароль). Сведения о правах доступа пользователей к сегменту ИС отражаются администратором сегмента ИС согласно разработанной Матрице доступа.

Работа на АРМ пользователям разрешена только с разрешённым программным обеспечением и сетевыми ресурсами.

До ввода аутентификационной информации, пользователям запрещаются любые действия с сегментом ИС и средствами вычислительный техники.

Самостоятельная установка программного обеспечения пользователями на АРМ запрещена. Установка и удаление любого программного обеспечения производится только администратором сегмента ИС Учреждения или администратором ИС.

Самостоятельное изменение пользователями аппаратной конфигурации АРМ, а также подключение к АРМ мобильных устройств передачи информации (сотовые телефоны, usb-модемы, и пр.) запрещено. Изменение (модификация) аппаратной конфигурации АРМ производится только администратором сегмента ИС Учреждения.

АРМ подлежат опечатыванию/опломбированию (с целью недопущения бесконтрольного изменения аппаратных конфигураций). Опечатывание осуществляется только администратором сегмента ИС. Пользователи АРМ обязаны следить за сохранностью данных пломб и в случае их нарушений – незамедлительно сообщать о данном событии, администратору сегмента ИС.

На АРМ осуществляется установка пароля на доступ к базовой системе ввода-вывода (BIOS).

На АРМ пользователей должно быть запрещено использование технологий беспроводной передачи данных (в частности, 802.11xWi-Fi, 802.15.1 Bluetooth, 802.22 WRAN, IrDA и иных беспроводных соединений).

При работе АРМ должен обеспечиваться контроль работоспособности (неотключения) программного обеспечения средств защиты информации. Настройка программного обеспечения и средства защиты информации должна осуществляться в соответствии с требованиями эксплуатационной документации на них.

Порядок внесения изменений в состав программного обеспечения и аппаратных характеристик АРМ и серверов информационных систем приведён в разделе VI настоящей Политики. Все изменения документально фиксируются.

При необходимости отлучиться от АРМ, пользователь обязан, во избежание осуществления несанкционированного доступа к ресурсам АРМ, принудительно заблокировать АРМ посредством функционала операционной системы или используемого средства защиты информации от несанкционированного доступа, межсетевого экранирования уровня хоста.

Передача работниками электронных документов внутри Учреждения производится с использованием учтённых съёмных носителей информации, а также посредством общих папок, средств электронной почты. Иные способы передачи запрещены.

Информация об использовании пользователями сегмента ИС средств вычислительной техники протоколируется и, при необходимости, может быть предоставлена директору Учреждения.

Раздел III
Порядок использования служебной электронной почты

Электронная почта Учреждения (служебная электронная почта) предназначена исключительно для использования в служебных целях – сотрудникам запрещено вести частную переписку с использованием средств служебной электронной почты (к частной переписке относится переписка, не связанная с исполнением сотрудником своих должностных обязанностей). Использование служебной электронной почты для частной переписки сотрудником, является нарушением трудовой дисциплины.

Сотрудникам запрещается использование своего адреса служебной электронной почты для подписки на рассылки и другие сервисы, а также при регистрации на любых сайтах, расположенных в сети Интернет (при использовании АРМ, подключенных к сети Интернет, не входящих в сегмент ИС).

Все почтовые сообщения, переданные или принятые с использованием служебной электронной почты, принадлежат Учреждению и являются неотъемлемой частью его производственного процесса.

При работе с электронной почтой пользователь должен учитывать следующие принципиальные положения:

— электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;

— электронная почта не является средством передачи информации, обеспечивающим конфиденциальность передаваемой информации. Передачу конфиденциальной информации вне локальной сети необходимо осуществлять только в зашифрованном виде;

— электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

В целях повышения уровня безопасности при работе со служебной электронной почтой, при получении входящей корреспонденции:

— необходимо избегать перехода по ссылкам, содержащимся во входящих электронных сообщениях, полученных от недостоверных источников;

— не открывать вложения электронной почты, полученные от недостоверных источников;

— проверять адреса отправителей электронной почты с целью предотвращения подделки адреса отправителя путём замены адреса на схожий, но с подменными символами (например, путём замены букв цифрами – замена «ivanov@mail.ru» на «ivanov@ma1l.ru», где вместо буквы «i» используется цифра «1»);

— проверять расширения вложенных файлов, при этом особое внимание следует обращать на так называемые «исполняемые файлы» с расширением «.exe», «.js», «.cmd», «.bat».

Раздел IV
Порядок использования съёмных носителей информации

Под съёмными носителями информации понимаются, оптические диски, флэш-накопители, внешние накопители на жёстких дисках и иные переносные устройства хранения информации.

Под использованием съёмных носителей информации понимается их подключение к АРМ с целью приёма/передачи информации.

Допускается использование только учтённых носителей информации, которые являются собственностью Учреждения и подвергаются регулярной ревизии и контролю.

Учёт съёмных носителей информации и факт их выдачи осуществляется в журнале учёта съёмных носителей информации (формы журналов учёта приведены в приложении № 1 к настоящей Политике), который ведётся администратором сегмента ИС. При этом съёмные носители информации должны быть соответствующим образом промаркированы.

Хранение съёмных носителей информации должно осуществляться в сейфах, запираемых металлических шкафах. Перечень мест хранения съёмных носителей информации должен быть заранее определён, при этом, определяются ответственные лица за обеспечение сохранности съёмных носителей информации (форма учёта мест хранения съёмных носителей информации приведена в приложении № 1 к настоящей Политике).

Съёмные носители информации, пришедшие в негодность или отслужившие установленный срок, а также съемные носители информации, которые не подлежат очистке, подлежат уничтожению. Уничтожение съёмных носителей с защищаемой информации осуществляется комиссией. По результатам уничтожения носителей составляется акт и сведения заносятся в соответствующий журнал (форма акта приведены в приложении № 2 к настоящей Политике).

В следующих случаях должно быть обеспечено гарантированное уничтожение (стирание) информации, исключающее возможность восстановления защищаемой информации, со съёмного носителя:

— после его приобретения;

— при его первичном подключении к сегменту ИС;

— при передаче в сторонние организации (в том числе перед и после возвращения из ремонта или перед передачей в утилизацию).

Гарантированное уничтожение информации обеспечивается администратором информационной безопасности посредством функционала средства подсистемы защиты информации от несанкционированного доступа.

Пользователи обязаны:

— использовать носители информации исключительно для выполнения своих служебных обязанностей;

— обеспечивать физическую безопасность носителей информации всеми разумными способами;

— извещать администратора сегмента ИС о фактах утраты (кражи) носителей информации.

При использовании съёмных носителей информации пользователям запрещено:

— использовать носители информации в личных целях;

— передавать носители информации другим лицам;

— оставлять съёмные носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

Любое взаимодействие (обработка, приём/передача информации) с сегментом ИС посредством использования неучтённых (личных) носителей информации, рассматривается как несанкционированное (за исключением случаев, заранее оговорённых и согласованных с администратором сегмента ИС).

Вынос съемных носителей информации для использования их за пределами контролируемой зоны Учреждения должен согласовываться с администратором сегмента ИС.

Раздел V
Порядок предоставления доступа к информационным ресурсам (системам) и средствам обработки информации

Права доступа пользователей к сегменту ИС и СВТ предоставляются объёме минимально необходимых полномочий для выполнения ими своих должностных обязанностей.

К работе с сегментом ИС и СВТ допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности (ознакомившиеся с организационно-распорядительной документацией, регламентирующей процессы обработки и защиты информации, в том числе персональных данных).

Необходимость доступа пользователя к сегменту ИС и СВТ определяет директор Учреждения на основании должностных (трудовых) обязанностей сотрудника.

Основанием для предоставления прав доступа пользователя к сегменту ИС и СВТ является заявка директора Учреждения, согласованная администратором ИС, и администратором сегмента ИС.

Права доступа пользователей к сегменту ИС назначаются администратором ИС в установленном порядке.

Оповещение администратора ИС об изменении и (или) блокировании прав доступа пользователей к сегменту ИС осуществляется администратором сегмента ИС, в следующих случаях:

— выявления нарушений пользователем исполнения установленных нормативными правовыми актами Учреждения требований по обработке и обеспечению безопасности информации (в том числе персональных данных);

— в период отпуска пользователя – по заявке директора Учреждения;

— изменения должностных обязанностей работника (перевода на другую должность);

— увольнения работника

Ответственность за своевременное уведомление администратора ИС об увольнении администратора сегмента ИС несёт директор Учреждения.

В случае увольнения работника также изымаются предоставленные ему съёмные носители информации.

Раздел VI
Порядок внесения изменений в программное обеспечение и технические средства

Все изменения программного обеспечения и технических средств (АРМ) должны быть санкционированы и проводиться только на основании заявок директора Учреждения.

Право изменения конфигурации системных и прикладных программных средств, программных и программно-аппаратных средств защиты информации, а также в отношении аппаратных средств АРМ пользователей сегмента ИС – предоставляется администратору сегмента ИС Учреждения;

Изменение конфигурации аппаратно-программных средств защищённых АРМ кем-либо, кроме администратора сегмента ИС Учреждения запрещено.

Установка (обновление) программного обеспечения СВТ производится с эталонных копий программных средств, хранящихся у администратора сегмента ИС или у администратора ИС.

Обновление программного обеспечения осуществляется в т.ч. по результатам проведения внутреннего инструментального аудита информационной безопасности (сканирование средством анализа защищённости).

Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода.

Действия по изменению программного обеспечения фиксируются в Реестре разрешённого к использованию в сегменте ИС программного обеспечения (форма реестра приведена в приложении № 4 к настоящей Политике). Реестр ведётся администратором сегмента ИС при содействии администратора ИС.

Раздел VII
Порядок предоставления удалённого доступа пользователей к сегменту ИС

Под удалённым доступом к сегменту ИС понимаются все виды доступа, осуществляемые по внешним каналам связи (проводной (коммутируемой), широкополосной) и с использованием устройств доступа, расположенных за пределами контролируемой зоны Учреждения.

Удалённый доступ к сегменту ИС предоставляется:

— системному администратору ИС;

— администратору информационной безопасности ИС;

— подрядным организациями, осуществляющим поддержку функционирования ИС на основании заключенных государственных контрактов.

Решение о предоставлении удалённого доступа системному администратору ИС должно быть обосновано служебной необходимостью и согласовано с администратором информационной безопасности ИС.

Сотрудникам Учреждения, не предоставляется удалённый доступ к сегменту ИС.

Для удалённого доступа к сегменту ИС должны применяться средства криптографической защиты информации, обладающие действующими сертификатами ФСБ России по требованиям, предъявляемым к средствам криптографической защиты информации.

Раздел VIII
Порядок действий в ходе эксплуатации информационной системы, аттестованной по требованиям безопасности информации

Аттестованная информационная система по требованиям безопасности информации – информационная система, успешно прошедшая процедуру оценки соответствия требований, предъявляемых к установленному классу защищённости информационной

системы (далее – аттестация), на которую в установленном порядке организацией, имеющей лицензию ФСТЭК России на деятельность по технической защите информации (далее – Лицензиат ФСТЭК России), выдан соответствующий Аттестат соответствия информационной системы требованиям безопасности информации (далее – Аттестат соответствия).

Администратор сегмента ИС обеспечивает поддержание базовой конфигурации сегмента ИС и системы защиты информации Учреждения (структуры системы защиты, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с аттестатом соответствия сегмента ИС требованиям безопасности информации.

Виды возможных изменений в состав и структура аттестованного по требованиям безопасности информации сегмента ИС и необходимые действия со стороны её обладателя:

№ п/п	Вид изменений	Порядок необходимых действий
1	Окончание срока действия аттестата соответствия	Необходимо проведение аттестации (повторно) сегмента ИС с выдачей Аттестата соответствия
2	Повышение класса защищённости сегмента ИС	
3	Увеличение состава угроз сегмента ИС, связанное с добавлением новых информационных технологий в сегмент ИС	Необходимо проведение дополнительных аттестационных испытаний сегмента ИС (контроль эффективности) в рамках действующего аттестата соответствия: администратор сегмента ИС отправляет уведомительное письмо Лицензиату ФСТЭК России, выдавшему Аттестат соответствия, в котором указываются планируемые изменения, а также их причину; по результатам анализа планируемых изменений, Лицензиат ФСТЭК России принимает решение о необходимости проведения дополнительных аттестационных испытаний сегмента ИС и определяет порядок проверки эффективности системы защиты информации в рамках вносимых изменений, о чём извещает администратора сегмента ИС о принятом решении и последующих совместных действиях по внесению изменений; администратор сегмента ИС проводит работы в рамках вносимых изменений и, при необходимости, привлекает исполнителей, имеющих соответствующий уровень квалификации, из числа сотрудников организаций, обладающих необходимыми лицензиями ФСТЭК России и ФСБ России на осуществление видов деятельности, связанных с защитой информации; лицензиат ФСТЭК России проводит дополнительные аттестационные испытания сегмента ИС; дополнительные аттестационные испытания сегмента ИС проводятся по Программе и методикам, согласованным с администратором сегмента ИС и утверждённым лицензиатом ФСТЭК России; по результатам дополнительных аттестационных испытаний лицензиатом ФСТЭК России оформляются протокол проведённых испытаний и заключение. Положительные результаты дополнительных
4	Изменение состава средств защиты информации, указанных в аттестате соответствия, на новые, не указанные в аттестате	
5	Добавление в состав аттестованного сегмента ИС новых АРМ и/или серверов	
6	Переустановка средств защиты информации с аттестованных АРМ на новые АРМ с последующим их добавлением в состав аттестованной сегмента ИС	
7	Переустановка установленных средств защиты информации, указанных в Аттестате соответствия, на аттестованных АРМ в пределах сегмента ИС	

		аттестационных испытаний дают право на обработку защищаемой информации в сегменте ИС с учётом внесённых изменений; копия уведомительного письма с перечнем планируемых изменений конфигурации сегмента ИС, извещение от лицензиата ФТСЭК России, Программа и методики дополнительных аттестационных испытаний и отчётная документация по результатам испытаний хранятся администратором сегмента ИС вместе с комплектом аттестационных документов на сегмент ИС
8	Понижение класса защищённости сегмента ИС (уменьшение числа актуальных угроз, объёма обрабатываемых данных, снижение требований к характеристикам безопасности и пр.)	Аттестат соответствия сохраняет своё действие
9	Исключение из состава аттестованной сегмента ИС некоторых АРМ	Аттестат соответствия сохраняет свое действие: оператор информационной системы пишет уведомительное письмо лицензиату ФСТЭК России, в котором указывает планируемые изменения, а также их причину; лицензиат ФСТЭК России рассматривает вносимые изменения в конфигурацию сегмента ИС и извещает администратора сегмента ИС о возможности внесения данных изменений; администратор сегмента ИС самостоятельно проводит работы по внесению изменений в состав аттестованного сегмента ИС; копия уведомительного письма с составом планируемых изменений конфигурации сегмента ИС и извещение от лицензиата ФСТЭК России хранятся администратором сегмента ИС вместе с комплектом аттестационных документов
10	Замена периферийного оборудования АРМ сегмента ИС: монитора, принтера, сканера и т.п.	
11	Перемещение АРМ аттестованного сегмента ИС в пределах контролируемой зоны	
12	Удаление, установка, переустановка на аттестованных АРМ прикладного программного обеспечения, не связанного с обработкой защищаемой информации	
13	Удаление, установка, переустановка на аттестованных АРМ и (или) серверах программного обеспечения, предназначенного для обработки защищаемой информации (без повышения класса защищённости информационной системы)	
14	Увольнение ответственных работников	

Раздел IX
Организация мероприятий по антивирусной защите информации

К использованию допускаются только лицензионные средства антивирусной защиты информации, имеющие действующие сертификаты соответствия ФСТЭК России, предъявляемые к средствам антивирусной защиты, приобретенные у разработчиков (официальных поставщиков) данных средств.

Установка средств антивирусной защиты информации на автоматизированные рабочие места и сервера должна осуществляться только с сертифицированных ФСТЭК России дистрибутивов, приобретённых у разработчиков (официальных поставщиков) данных средств.

Средства антивирусной защиты информации должны использоваться на всех автоматизированных рабочих местах сегмента ИС и обеспечивать выполнение следующих требований:

— возможность обнаружения как можно большего числа известных вредоносных программ, в том числе вирусов, деструктивного кода (макровирусов, объектов ActiveX, апплетов языка Java и других), а также максимальную готовность быстрого реагирования на появление новых видов вирусных угроз;

— своевременное уведомление о необходимости обновления антивирусных баз и их последующее обновление из доверенных источников. Контроль целостности обновлений антивирусных баз должен обеспечиваться функционалом антивирусного средства;

— обеспечивать соответствие системных требований средства к платформам, характеристикам и комплектации применяемой вычислительной техники;

— иметь документацию, необходимую для практического применения и освоения средства, на русском языке;

— обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком средства.

При функционировании средств антивирусной защиты информации на компонентах информационных систем обязательно выполнение следующих требований:

— антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы и другие), получаемая и передаваемая посредством каналов связи (в том числе по электронной почте), а также съёмных носителей информации (CD/DVD-диски, флэш-накопители и т.п.);

— определение автоматической реакции средства антивирусной защиты информации при обнаружении компьютерных вирусов и другого вредоносного программного обеспечения;

— систематическая проверка содержимого жестких дисков АРМ;

— проверка в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съёмных носителей информации, сетевых подключений (в том числе к сетям общего пользования) и других внешних источников) при загрузке, открытии или исполнении таких файлов;

— поддержание антивирусных баз в актуальном состоянии и их своевременное распространение на АРМ сегмента ИС;

— запрет деактивации средств антивирусной защиты информации пользователями информационных систем;

— деактивация средств антивирусной защиты информации на АРМ сегмента ИС только для проведения профилактических мероприятий и по согласованию с администратором сегмента ИС.

Раздел X
Порядок формирования и использования аутентификационной информации

Для обеспечения возможности однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами каждому пользователю формируется имя пользователя.

Имя пользователя должно отождествляться с учетной записью пользователя в сегменте ИС (при наличии технической возможности).

Использование гостевых учётных записей запрещено.

Локальная учётная запись администратора операционной системы Windows (Администратор) предназначена только для служебного использования администратором при настройке систем и не может быть использована для повседневной работы.

Сотрудники обязаны хранить в секрете персональные пароли доступа к информационным ресурсам (системам) и средствам обработки информации и не передавать их другим лицам. Передача личного пароля пользователя третьим лицам возможна только в следующих случаях:

— в случае необходимости при проведении проверочных мероприятий (внутренний аналитический аудит), которые требуют знания пароля пользователя, допускается раскрытие значений своего пароля проверяющему сотруднику. По окончанию проверочных работ сотрудники самостоятельно производят немедленную смену значений «раскрытых» паролей;

— в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имён и паролей сотрудников (в их отсутствие) допускается изменение паролей администратором сегмента ИС. Сотрудники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, создать их новые значения в соответствии с требованиями раздела XI настоящей Политики.

Хранение сотрудником (администратором, пользователем) аутентификационной информации допускается только в личном сейфе (запираемом шкафу, ящике) либо в сейфе (запираемом шкафу, ящике) администратора сегмента ИС. При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

При доступе к средствам обработки информации (серверам, активному сетевому оборудованию, средствам защиты информации) запрещается использование аутентификационной информации, заданной производителем «по умолчанию».

После получения доступа к информационному ресурсу (системе), средству обработки информации пользователь при первом входе в систему должен сменить пароль доступа (в случае наличия технической возможности), на пароль, удовлетворяющий требованиям настоящей Политики.

При вводе аутентификационной информации (пароля) должно обеспечиваться исключение отображения вводимой парольной информации (например, осуществляется замена вводимых символов условными знаками «-», «*» или иными знаками). В случае отсутствия технической возможности реализации данного требования пользователь самостоятельно создает условия защиты, вводимой аутентификационной информации.

Запрещается передача аутентификационной информации пользователям при помощи почтовых сообщений, либо по иным открытым каналам связи.

В случае компрометации аутентификационных данных сотрудники должны незамедлительно сообщить об этом событии, являющемся инцидентом информационной безопасности, администратору сегмента ИС.

Предусматривается периодическая плановая (в соответствии с установленным сроком) и внеплановая смена паролей. Внеплановая немедленная смена пароля обязательна в случае его компрометации. Также, внеплановая смена пароля и (или) блокирование учётной записи пользователя производится в случае прекращения его полномочий, непосредственно после окончания последнего сеанса работы данного пользователя.

Должностным лицам запрещается разглашать пароли, ставшие известными им в ходе служебной деятельности по обеспечению функционирования сегмента ИС.

Для доступа к сегменту ИС следующими категориями лиц применяются средства двухфакторной аутентификации:

— администратор сегмента ИС;

— администратор ИС;

— администратора информационной безопасности ИС.

Раздел XI
Требования к качеству аутентификационной информации и мер по обеспечению её безопасности

К аутентификационной информации пользователей и администраторов информационных ресурсов (систем) и средств обработки информации определены следующие требования:

№ п/п	Параметр качества пароля	Администратор	Пользователь
1	Минимальная длина пароля в символах	8	6
2	Максимальная длина пароля в символах	не ограничена	не ограничена
3	Содержание в пароле букв верхнего и нижнего регистра	да	да
4	Содержание в пароле специальных символов (@, #, $, &, * и т.п.) и цифр (при наличии технической возможности)	обязательно	обязательно
5	Содержание в пароле личных имён, фамилий, кличек домашних животных, номеров телефонов, дат рождения, географических названий, именований АРМ и т.п.	запрещено	запрещено
6	Содержание в пароле общепринятых сокращений (Admin, Administrator, ViPNet, Cisco, User, UserID и т.д.)	запрещено	запрещено
7	Использование дополнительных средств идентификации (аппаратных идентификаторов)	обязательно	рекомендуется
8	Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки	5	8
9	Блокировка сеанса доступа в информационную систему после времени бездействия (неактивности) пользователя (минут)	5	15
10	Исключение возможности отображения информации о сеансе пользователя на экране монитора после блокировки сеанса	обязательно	обязательно
11	Блокировка программно-технического средства или учётной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации	30	15
12	Блокировка учётной записи после	60	90

№ п/п	Параметр качества пароля	Администратор	Пользователь
	периода неиспользования (дней)		
13	Минимальное отличие нового пароля от предыдущего (в позициях)	4	3
14	Количество уникальных паролей, устанавливаемых подряд (в течение установленного срока смены паролей)	не менее 5	не менее 3
15	Максимальный срок действия пароля	60 дней	90 дней
16	Минимальный срок действия пароля	нет	нет

Раздел XII
Контроль физического доступа и защита технических средств

Режим обеспечения безопасности помещений, в которых размещаются компоненты сегмента ИС и осуществляется обработка персональных данных (далее – Помещения) должен быть организован таким образом, чтобы препятствовать возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

Ограждающие конструкции Помещений, должны предполагать существенные трудности для нарушителя по их преодолению. Пример: металлические решетки на окнах, металлическая дверь, надёжные замки, система контроля и управления доступом и т.д.

Помещения должны быть оснащены надёжными входными дверьми с замками, а также средствами опечатывания помещений по окончании рабочего дня.

Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, должны быть оборудованы металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

Доступ сотрудников в Помещения должен быть организован согласно перечню лиц, допущенных в Помещения. Перечень сотрудников, доступ которых разрешен в Помещения, размещается на внутренней стороне двери этого помещения.

В Помещениях определяются места хранения материальных носителей персональных данных и лиц, ответственных за их сохранность.

Доступ посторонних лиц в Помещения, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица из числа сотрудников, допущенных в Помещение. При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с персональными данными и другой защищаемой информацией. Такими мерами являются: размещение мониторов, исключающее или существенно затрудняющее просмотр отображаемой информации; размещение документации на бумажных носителях, исключающее просмотр информации на них (документация убирается в папки, ящики тумбочек/столов, либо переворачивается лицевой стороной вниз, либо накрывается сверху непрозрачными объектами, закрывающими область текста).

В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведется обработка персональных данных, должны быть надёжно закрыты, материальные носители должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

Доступ в серверные помещения посторонних лиц допускается по согласованию с директором Учреждения.

Двери серверных помещений должны быть оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытие только для санкционированного прохода.

Уборка Помещений происходит только под контролем сопровождающего лица из числа сотрудников, допущенных в Помещение.

Нахождение в Помещении посторонних лиц без сопровождающего запрещено.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с директора Учреждения.

Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении сотрудника, допущенного в Помещение.

При необходимости повышенного уровня обеспечения безопасности Помещений могут использоваться системы видеонаблюдения и системы контроля и Учреждения доступом.

Для помещений, в которых размещаются компоненты сегмента ИС (средства обработки информации), должна обеспечиваться контролируемая зона[1]).

Границы контролируемой зоны сегмента ИС отражаются в Техническом паспорте сегмента ИС.

Учёт доступа в помещения может реализовываться путём:

— использования систем контроля и управления доступом;

— использования систем охраны помещений;

— использования систем видеонаблюдения;

— опечатывания помещений и контроля выдачи ключей от помещений;

— реализации иных мер, предусмотренных контрольно-пропускным режимом.

Должна обеспечиваться защита технических средств от внешних воздействий[2], включающая:

— обеспечение выполнения норм и правил пожарной безопасности – для всех помещений размещения технических средств;

— обеспечение необходимых для эксплуатации технических средств, условий по степени запылённости воздуха – для всех помещений размещения технических средств;

— обеспечение выполнения норм и правил устройства и технической эксплуатации электроустановок, а также соблюдение параметров электропитания и заземления технических средств (в т. ч. использование для АРМ, активного сетевого оборудования, средств защиты информации, выполненных в виде программно-аппаратных комплексов, кратковременных резервных источников питания (достаточных для обеспечения правильного (корректного) завершения работы технического средства, устройства в случае отключения основного источника питания) и (или) долговременных резервных источников питания в случае длительного отключения основного источника питания и

---

[1] *Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и лиц, не имеющих постоянного допуска (не являющихся работниками), а также посторонних транспортных, технических и иных материальных средств. Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.*

[2] *Внешние воздействия – воздействия окружающей среды, нестабильности электроснабжения, кондиционирования и иные внешние факторы.*

необходимости продолжения выполнения техническим средством установленных функциональных задач[3].

Раздел XIII
Обеспечение отказоустойчивости технических средств

Обеспечение отказоустойчивости технических средств осуществляется путём:

— выполнения требований раздела XII настоящей Политики;

— контроля пороговых значений основных показателей функционирования технических средств (степени загрузки: процессорных мощностей, дискового пространства, оперативной памяти, каналов связи и пр.);

Резервирование машинных носителей информации, находящихся в составе АРМ пользователей сегмента ИС, в случае необходимости, может осуществляться Администратором сегмента ИС.

Резервирование важных файлов и каталогов пользователей сегмента ИС осуществляется Администратором сегмента ИС, по заявке.

Резервное копирование должно проводиться только на учтенные машинные носители информации. При проведении копирования необходимо сделать запись в журнале учета проведения резервного копирования (форма журнала приведена в приложении № 5).

Раздел XIV
Обеспечение резервного копирования и восстановления информации

Резервному копированию подлежат:

— защищаемая информация (информационные ресурсы: файлы и каталоги, базы данных информационных систем);

— параметры настройки, конфигурации и журналы аудита средств защиты информации.

Резервное копирование может осуществляться следующими способами:

— посредством функционала программного обеспечения (прикладного программного обеспечения; функционала средств защиты информации) с их последующим сохранением на места размещения резервных копий (хранилища данных, съёмные носители информации) - тип 1 (автоматически или вручную);

— посредством копирования защищаемой информации на места размещения резервных копий (хранилища данных, съёмные носители информации) – тип 2 (вручную).

Резервные копии запрещается хранить в одном месте с резервируемыми данными.

В случае хранения резервных копий на съёмных носителях информации они должны быть учтены и храниться в соответствии с разделом IV настоящей Политики. Съёмный носитель с резервной копией должен быть подписан и содержать как минимум следующую информацию:

— перечень информационных ресурсов, резервные копии которых хранятся на данном носителе;

---

[3] *В качестве кратковременных резервных источников бесперебойного питания могут применяться ИБП, в качестве кратковременных резервных источников бесперебойного питания могут применяться дизельные или бензиновые генераторные установки, а также резервные линии электропитания.*

— год, месяц, число, время создания резервной копии.

Не допускается хранение резервных копий в местах, не предусмотренных для этого. Характеристики процесса резервного копирования определяются администратором сегмента ИС.

Учёт проведения резервного копирования должен осуществляться автоматизированными средствами (в случае наличия технической возможности) или в «Журнале учёта проведения резервного копирования» (форма журнала приведена в приложении № 5). Данный журнал может вестись в электронном виде.

Восстановление защищаемой информации из резервных копий осуществляется в случае её утраты или повреждения вследствие несанкционированного доступа к ней, воздействия вирусов, программных ошибок, ошибок работников или аппаратных сбоев.

Восстановление данных из резервных копий должно осуществляться в максимально сжатые сроки, ограниченными техническими возможностями.

В зависимости от характера и уровня повреждения информационного ресурса (сегмента ИС) восстанавливается либо весь массив резервных данных, либо отдельные поврежденные или уничтоженные файлы и папки.

Все действия по восстановлению защищаемой информации должны быть учтены в «Журнале учёта восстановления информации» (форма журнала приведена в приложении № 6 к настоящей Политике).

Ответственность за резервирование и восстановление защищаемой информации несет администратор сегмента ИС.

Резервное копирование параметров настройки, конфигурации, а также журналов аудита средств защиты информации, осуществляется администратором сегмента ИС.

Раздел XV
Порядок обеспечения сетевой безопасности

Средства, используемые в составе ЛВС для обеспечения необходимого уровня безопасности информации, должны обеспечивать:

— доступность, целостность и конфиденциальность информационных ресурсов;

— защиту каналов передачи данных и управления, их доступность;

— защиту сетевого трафика от несанкционированного внешнего и внутреннего доступа;

— защищённый удалённый доступ в сегмент ИС;

— простоту используемых технологий защиты информации и их эксплуатации;

— прозрачность используемых средств и механизмов защиты для пользователей.

С целью обеспечения выполнения указанных требований в составе ЛВС должны применяться следующие технологии сетевой безопасности:

— обнаружение и предотвращение вторжений;

— криптографическая защита информации.

С целью минимизации возможных точек доступа к сетям связи общего пользования использование технологий беспроводной передачи данных в сегменте ИС Учреждения запрещено.

Используемые средства межсетевого экранирования должны иметь соответствующие действующие сертификаты соответствия, выданные ФСТЭК России.

Средства обнаружения вторжений должны иметь в своем составе следующие компоненты:

— компоненты регистрации событий безопасности (датчики);

— компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы);

— базу решающих правил (базу сигнатур), содержащую информацию о характерных признаках компьютерных атак.

Средствами обнаружения вторжений должен реализовываться следующий функционал:

— использование сигнатурных и эвристических методов для анализа сетевого трафика, журналов ОС и приложений на предмет нештатных ситуаций, а также попыток проведения вторжений;

— защита от атак на сетевые протоколы на различных уровнях модели OSI;

— возможность анализа собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени;

— централизованное управление (администрирование) компонентами средств, установленными в различных сегментах ИС;

— обновление (из доверенных источников) базы решающих правил;

— контроль целостности обновлений базы решающих правил;

— уведомление о необходимости обновления и непосредственном обновлении базы решающих правил.

С целью выполнения указанных требований могут применяться программные средства обнаружения вторжений уровня хоста – на внутренних узлах сегментов информационных систем.

Используемые средства обнаружения вторжений должны иметь соответствующие действующие сертификаты соответствия, выданные ФСТЭК России.

Раздел XVI
Порядок проведения внутреннего аудита информационной безопасности

Внутренний аудит заключается в оценке выполнения требований нормативных документов по обеспечению безопасности и защищённости информации, обрабатываемой Учреждением.

Внутренний аудит представляет собой непрерывную и неотъемлемую часть деятельности, по обеспечению информационной безопасности сегмента ИС.

Внутренний аудит может проводиться:

— с использованием сертифицированных ФСТЭК России автоматизированных средств контроля (анализа) защищённости и соответствия требованиям – инструментальный аудит;

— без использования автоматизированных средств – аналитический аудит.

Внутренний аудит может быть плановый, проводимый с целью проверки степени выполнения Учреждением требований по обеспечения информационной безопасности, и внеплановый.

Внеплановый внутренний аудит может проводиться в случае:

— наличия косвенных подтвержденных сведений о нарушениях сотрудниками Учреждения требований к обеспечению информационной безопасности;

— многократных инцидентов нарушения информационной безопасности, случившихся в Учреждении;

— подготовки к контролю со стороны уполномоченных федеральных органов, регулирующих деятельность в сфере обработки и защиты информации.

Внеплановый внутренний инструментальный аудит может проводиться после появления информации об уязвимости и соответствующем обновлении баз средств контроля (анализа) защищённости.

Внутренний аналитический аудит проводится в целях проверки:

— назначения лиц, ответственных за защиту информации;

— определения соответствия состава и структуры программно-технических средств, обрабатывающих защищаемую информацию (в т.ч. средств защиты информации), документированному составу и структуре средств, разрешённых для обработки такой информации;

— соответствия реального уровня полномочий по доступу к сегменту ИС, внутренним документам;

— правильности применения средств защиты информации;

— организации хранения носителей информации и допуска в помещения, в которых размещены средства обработки информации и осуществляется обработка защищаемой информации;

— выполнения требований к условиям размещения технических средств, обрабатывающих защищаемую информацию, в служебных помещениях;

— выполнения требований, предъявляемых к порядку обработки и защиты персональных данных;

— проверки знания пользователями требований руководящих документов, технологических инструкций, предписаний, актов, заключений и уровень овладения технологией безопасной обработки информации, описанной в этих документах.

Структура плана проведения внутреннего аналитического аудита приведена в приложении № 7.

Для проведения внутреннего аналитического аудита, директора Учреждения, назначается рабочая группа (комиссия) по проведению аудита информационной безопасности.

Члены комиссии имеют право:

— осматривать помещения, в которых производится обработка конфиденциальной информации;

— получать доступ к техническим средствам, участвующим в обработке информации;

— просматривать настройки средств защиты информации;

— проводить беседы и консультации с сотрудниками Учреждения, требовать от них предоставления письменных объяснений, справок, отчётов по вопросам, относящимся к предмету аудита.

По результатам внутреннего аналитического аудита:

— комиссией в двухнедельный срок составляется акт о результатах внутреннего аудита Учреждения, выявленных недостатках и нарушениях, а также разрабатывается план устранения выявленных в ходе проведения внутреннего аналитического аудита информационной безопасности недостатков (форма плана приведена в приложении № 8 к настоящей Политике), который передается на согласование директору Учреждения;

— директор Учреждения, при необходимости, вносит изменения в данный план и контролирует реализацию его пунктов;

— лица, назначенные ответственными за реализацию пунктов Плана, в согласованный срок отчитывается о результатах проделанной работы.

Внутренний инструментальный аудит проводится в целях:

— выявления (поиска) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (системном и прикладном), в программном обеспечении средств защиты информации, с правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также с

корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

— контроля, установленного на АРМ ПО, разрешённого к использованию в информационных системах Учреждения;

— контроля установки обновлений программного обеспечения;

— проверки выполнения требований, установленных организационно-распорядительными документами Учреждения, регламентирующими процессы обработки и защиты информации.

— наблюдения за действиями пользователей информационных систем с целью контроля соблюдения ими норм и требований обеспечения безопасности информации, установленных в Учреждении;

— получения актуальных и объективных данных о текущем состоянии обеспечения безопасности сегмента ИС (в том числе от внешних угроз со стороны потенциальных злоумышленников);

— контроля возникновения и устранения уязвимостей и ошибок конфигурации информационных систем;

— оценки и отражения в отчётах текущего уровня защищённости информационных ресурсов (систем), средств обработки информации, динамики его изменения;

— разработки рекомендаций по повышению уровня безопасности информационных ресурсов (систем), средств обработки информации.

Устранение выявленных уязвимостей осуществляется администратором ИС. Устранение выявленных уязвимостей должно осуществляться, в том числе, путём установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств или применения комплекса компенсирующих мер (например, дополнительная настройка средств защиты информации, изменение режима и порядка использования средств вычислительной техники).

В ходе внутреннего аудита быть получена объективная и полная информация по состоянию обеспечения информационной безопасности.

Внутренний аудит считается оконченным после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

Каждый год комиссией на основании сведений, полученных в ходе проведения аудитов информационной безопасности, разрабатываются рекомендации, в которых отражаются необходимые корректирующие воздействия, направленные на совершенствование процессов обеспечения информационной безопасности (анализ причин возникновения выявленных недостатков и предложения по исключению подобных недостатков в будущем), а также, при необходимости, предложения по корректировке организационно-распорядительной документации, регламентирующей процессы обработки и защиты информации (в т.ч. Моделей угроз безопасности информации).

Раздел XVII
Порядок проведения внешнего аудита информационной безопасности

Внешний (экспертный) аудит проводится в целях оценки соответствия эффективности применяемых мер защиты установленным требованиям законодательства Российской Федерации и (или) выявления недостатков в системе защиты информации.

Внешний аудит может проводиться в виде:

— тестирования информационной системы на проникновение;

— аттестации по требованиям безопасности информации.

Тестирование информационных систем на проникновение, в данном случае, должно осуществляться в режимах «чёрного» или «серого» ящика. Необходимость проведения тестирования на проникновения определяется директором Учреждения совместно с администратором информационной безопасности сегмента ИС.

Аттестация сегмента ИС должна проводиться не реже чем раз в три года. Аттестация сегмента ИС должна проводиться в соответствии с требованиями, утверждёнными национальным стандартом ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний» и требованиями Приказа ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

Приложение № 1
к Политике обеспечения информационной безопасности муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания

ФОРМЫ УЧЁТА
съёмных носителей информации, мест их хранения

Форма журнала учёта съёмных носителей информации

№ п/п	Дата, регистрационный номер съёмного носителя информации	Учётный номер, откуда поступил	Серийный номер (при наличии)	Тип съёмного носителя информации	Отметка об уничтожении съёмного носителя информации
1	2	3	4	5	5

Форма журнала учёта выдачи съёмных носителей информации

№ п/п	Регистрационный номер съёмного носителя информации	Тип съёмного носителя информации	Дата выдачи	Расписка в получении (ФИО и подпись)	Место хранения съёмного носителя информации	Расписка в обратном приёме (ФИО, подпись и дата)
1	2	3	4	5	5	6

Форма журнала учёта утилизации съёмных носителей информации

№ п/п	Тип съёмного носителя информации	Учётный номер носителя информации	Обоснование уничтожения носителя информации	Дата уничтожения	Номер акта утилизации	Ф.И.О. и подпись исполнителя	Ф.И.О. и подпись ответственного за обеспечение безопасности, и обработку конфиденциальной информации
1	2	3	4	5	6	7	8

Форма учёта мест хранения съёмных носителей информации и лиц, ответственных за их сохранность

№ п/п	Наименование структурного подразделения	Место хранения (номер помещения)	Ответственное лицо (ФИО, должность)	Подпись
1	2	3	4	5

Приложение № 2
к Политике обеспечения информационной безопасности муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания

ФОРМА
Акта утилизации съёмных носителей информации

АКТ
утилизации съёмных носителей информации

Комиссия в составе:
Председатель комиссии: _____;
члены комиссии: _____;
_____,

произвела отбор съёмных носителей информации и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации подлежит гарантированному уничтожению и составила настоящий акт о том, что произведена утилизация носителей конфиденциальной информации в составе:

№ п/п	Тип носителя	Регистрационный номер носителя	Примечание
1	2	3	4

Всего подлежит уничтожению _____ (_____) носителей.
(цифрами) (прописью)

Хранящаяся на указанных носителях информация уничтожена путём:
_____

Перечисленные носители уничтожены путём
_____
_____ .

Председатель комиссии: _____ / _____
личная подпись инициалы фамилия

Члены комиссии: _____ / _____
личная подпись инициалы фамилия

_____ / _____
личная подпись инициалы фамилия

Приложение № 3
к Политике обеспечения информационной безопасности муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания

ФОРМЫ МАТРИЦ ДОСТУПА
к информационным ресурсам, информационным системам и средствам обработки информации

Матрица доступа к объектам файловой системы (файлам, каталогам), информационным системам

№ п/п	Пользователь	Роль	Учетное имя	Доступ к настройкам СЗИ	Доступ к файлам журналов	Конфиденциальные данные в виде файлов и каталогов	Конфигурационные файлы СЗИ НСД	Каталоги и файлы данных ОС
1.								
2.								

Матрица доступа к средствам защиты информации

№ п/п	Наименование средства защиты информации	Ф.И.О., должность администратора подсистемы	Роль	Доступ к журналам аудита средства	Доступ к настройкам средства	Доступ к возможности деактивации функционала средства	Сведения, доступные пользователям ИС о конфигурации средства
1	2	3	4	5	6	7	8

Приложение № 4

к Политике обеспечения информационной безопасности муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания

ФОРМА РЕЕСТРА
программного обеспечения, разрешённого к использованию в сегменте ИС

Реестр программного обеспечения, разрешённого к использованию в муниципальном бюджетном образовательном учреждении «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания

№ п/п	Дата включения в реестр	Производитель ПО	Название ПО	Область применения (назначение) ПО	Количество лицензий	Особенности лицензирования
1	2	3	4	5	6	7
Системное программное обеспечение						
Прикладное программное обеспечение общего назначения						
Прикладное программное обеспечение специализированного назначения[4)]						

[1)] Под прикладным программным обеспечением специализированного назначения понимается программное обеспечение, используемое для обработки защищаемой информации

Приложение № 5
к Политике обеспечения информационной безопасности муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания

ФОРМА ЖУРНАЛА
проведения резервного копирования информации

ЖУРНАЛ
проведения резервного копирования информации

№ п/п	Наименование информационной ресурса/системы	Схема резервного копирования	Время и дата резервного копирования	Произвёл резервное копирование	
				Фамилия, инициалы	Подпись
1	2	3	4	5	6

Приложение № 6
к Политике обеспечения информационной безопасности муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания

ФОРМА ЖУРНАЛА
проведения восстановления информации

ЖУРНАЛ
проведения восстановления информации

№ п/п	№ инцидента ИБ	Наименование информационной ресурса/системы	Источник резервной копии с указанием схемы резервного копирования	Время и дата восстановления	Произвёл восстановление	
					Фамилия, инициалы	Подпись
1	2	3	4	5	6	7

Приложение № 7
к Политике обеспечения информационной безопасности муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания

ФОРМА СТРУКТУРЫ ПЛАНА
проведения внутреннего аналитического аудита информационной безопасности

ПЛАН
проведения ежегодного внутреннего аналитического аудита

№ п\п	Объект проверки	Результат проверки	Примечание
1	**Назначение ответственных лиц**		
1.1	Проверка назначения администратора сегмента ИС		
2	**Инвентаризация и учёт средств обработки информации**		
2.1	Проверка наличия заполненных форм учёта средств вычислительной техники и степени их актуальности:		
2.1.1	учёта автоматизированных рабочих мест		
2.1.2	учёта съёмных носителей информации		
2.1.3	учёта средств защиты информации		
2.2	Проверка наличия разработанных технических паспортов на сегмент ИС и степени их актуальности		
2.3	Проверка наличия разработанных описаний технологического процесса обработки информации в сегменте ИС и степени их актуальности		
3	**Эксплуатация и предоставление прав доступа к сегменту ИС, средствам вычислительной техники**		
3.1	Проверка наличия заявок на предоставление (изменение) прав доступа к информационным ресурсам (системам), средствам обработки информации, матриц доступа и их соответствие реально имеющимся правам		
3.2	Проверка перечня используемых для доступа к АРМ учётных записей пользователей с фактическими использованными для доступа к АРМ		

№ п\п	Объект проверки	Результат проверки	Примечание
3.3	Выборочная проверка отсутствия активных (незаблокированных) учётных записей уволенных сотрудников		
3.4	Выборочная проверка наличия минимальных прав доступа у учётных записей пользователей		
3.5	Проверка на АРМ пользователей наличия информации (в т. ч. в истории интернет-браузеров), не относящейся к служебным обязанностям		
3.6	Проверка состава используемого на АРМ пользователей программного обеспечения (в соответствии с Реестром разрешённого к использованию ПО)		
3.7	Проверка наличия печатей (пломб) на АРМ и серверах		
3.8	Проверка наличия установленных на АРМ и серверах паролей на доступ к BIOS		
3.9	Проверка работоспособности на АРМ и серверах средств защиты информации		
3.10	Проверка наличия действующих сертификатов соответствия ФСТЭК России, выданных на используемые средства защиты информации		
3.11	Проверка настроек программного обеспечения и средств защиты информации требованиям эксплуатационной документации (в том числе актуальность антивирусных баз, и баз решающих правил СрЗИ)		
3.12	Проверка АРМ и серверов на предмет подключения к ним мобильных устройств передачи информации (в ретроспективе), а также неучтённых съёмных носителей информации		
4	**Учёт и использование съёмных носителей информации**		
4.1	Проверка журнала учёта выдачи съёмных носителей информации с фактическим наличием у сотрудников данных съёмных носителей		
4.2	Проверка наличия перечня мест хранения съёмных носителей, назначения ответственных за них лиц и степени их актуальности		
4.3	Проверка съёмных носителей информации на предмет наличия информации, не связанной с исполнением служебных обязанностей		
4.4	Проверка выполнения уничтожения (стирания) информации со съёмных носителей информации		
4.5	Проверка выполнения порядка уничтожения съёмных носителей информации		
5	**Эксплуатация аттестованных по требованиям безопасности информации информационных систем**		
5.1	Проверка наличия аттестата соответствия на информационные системы,		

№ п\п	Объект проверки	Результат проверки	Примечание
	выданного лицензиатом ФСТЭК России, и срока его действия		
5.2	Проверка выполнения порядка действий в ходе эксплуатации аттестованной информационной системы		Проверяется в случае обнаружения расхождений между техническим паспортом информационной системы сведениями, указанными в аттестационной документации, и реальным состоянием информационной системы
6	**Использование аутентификационной информации при доступе к информационным ресурсам и средствам обработки информации**		
6.1	Проверка формата задания имён доступа пользователей установленным требованиям		
6.2	Проверка отсутствия гостевых учётных записей для доступа к АРМ, серверам, активному сетевому оборудованию, средствам защиты информации		
6.3	Выборочная проверка реализации требований, установленных к качеству аутентификационной информации и мер по обеспечению её безопасности		После проверок исполнения требований к качеству пароля (приводящие к его санкционированной компрометации), пользователь должен продемонстрировать установленный пароль на доступ, после чего незамедлительно его сменить
6.4	Отсутствие сохранённых паролей доступа как на средствах программного обеспечения, так и на бумажных носителях (вне отведённых для этого мест)		
6.5	Проверка исполнения требований, предъявляемых к учету и использованию дополнительных средств аутентификации		При их использовании
7	**Организация доступа в помещения обработки информации и выполнение требований, установленных к таким помещениям**		
7.1	Проверка наличия перечня помещений, в которых разрешена обработка конфиденциальной информации (в т. ч. персональных данных) и степени его актуальности		

№ п\п	Объект проверки	Результат проверки	Примечание
7.2	Проверка наличия перечня лиц, допущенных в помещения обработки конфиденциальной информации, степени его актуальности		Проверка наличия перечней для каждого помещения, а также в ходе проведения аудита проверяется степень исполнения данного требования при доступе в помещения
7.3	Проверка реализации требований, предъявляемых к помещениям обработки конфиденциальной информации:		
7.3.1	наличие ограждающих конструкций, предполагающих существенные трудности для нарушителей по их преодолению (металлические решётки на окнах, металлическая дверь, система контроля и управления доступом и т.д.)		
7.3.2	надёжные входные двери с замками, а также средствами опечатывания помещений		
7.3.3	окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, оборудованы металлическими решётками или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения		
7.4	Проверка наличия перечня мест хранения материальных носителей персональных данных и ответственных лиц, степени актуальности данного перечня		
8	**Защита технических средств от внешних воздействий**		
8.1	Способ реализации учёта доступа в помещения		Указывается реализованный способ
8.2	Проверка наличия средств обеспечения температурно-влажностного режима серверных помещений		
8.3	Проверка наличия средств обеспечения бесперебойного резервного питания для АРМ		
9	**Обеспечение отказоустойчивости технических средств**		
9.1	Проверка резервирования средств обработки информации, имеющих высокую критичность и способа резервирования		Указать способ резервирования
10	**Резервное копирование защищаемой информации**		
10.1	Проверка наличия заполненного перечня информационных ресурсов,		

№ п\п	Объект проверки	Результат проверки	Примечание
	подлежащих резервному копированию, его полноту и степень актуальности		
10.2	Проверка ведения журнала проведения резервного копирования информации		
10.3	Проверка ведения журнала восстановления информации		
10.4	Проверка мест хранения резервных копий		
11	**Обработка персональных данных**		
11.1	Проверка наличия размещённых на информационном Интернет-портале Учреждения Правил обработки персональных данных		При наличии информационного Интернет-портала Учреждения
11.2	Проверка степени актуальности уведомления об обработке персональных данных, поданных в Роскомнадзор		
11.3	Проверка наличия перечня обрабатываемых персональных данных и степени его актуальности		
11.4	Проверка наличия перечня должностей, замещение которых предусматривает осуществление обработки персональных данных, степени его актуальности		
11.5	Проверка соблюдения требований по учёту и реагированию на запросы субъектов персональных данных		
11.6	Соблюдение условий и порядка обработки персональных данных граждан, обратившихся в Учреждение		
11.7	Соблюдение процедур, направленных на предотвращение и выявление нарушений законодательства РФ в сфере персональных данных		
12	**Нормативно-методическое обеспечение системы защиты информации**		
12.1	Проверка наличия модели угроз безопасности информации и степени её актуальности с учётом используемых технологий обработки информации (срок актуальности документа не может превышать 3 лет)		
12.2	Проверка наличия технической и проектной документации по созданию/развитию системы защиты информации		
12.3	Проверка ознакомления сотрудников с нормативными документами, регламентирующими процессы обработки и защиты информации (в т.ч. персональных данных)		Может проводиться в формате тестирования или анкетирования с установленным перечнем контрольных вопросов

Приложение № 8
к Политике обеспечения информационной безопасности муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа имени Героя Советского Союза Энвера Ахсарова с. Зильги» Правобережного района Республики Северная Осетия-Алания

ФОРМА ПЛАНА
устранения недостатков, выявленных в ходе проведения внутреннего аналитического аудита информационной безопасности

ПЛАН
устранения недостатков, выявленных в ходе проведения внутреннего аналитического аудита информационной безопасности

№ п/п	Нарушение / недостаток	Мероприятия по устранению	Срок исполнения	Ответственные за исполнение
1	2	3	4	5