ПРИЛОЖЕНИЕ № 1

УТВЕРЖДЕНА

распоряжением

администрации Новоминского сельского поселения Каневского района

от 01.12.2020 № 69-р

Политика   
обеспечения информационной безопасности

в информационных системах администрации Новоминского сельского поселения Каневского района

# Раздел I

# Общие положения

Политика обеспечения информационной безопасности (далее – Политика) в информационных системах администрации Новоминского сельского поселения Каневского района (далее – Администрация) определяет порядок и процедуры обеспечения безопасности информации, обрабатываемой в информационных системах администрации Новоминского сельского поселения Каневского района (далее – ИС).

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

* порядок использования ИС и предоставления доступа к ней;
* порядок антивирусной защиты информации;
* порядок парольной защиты;
* порядок обеспечения отказоустойчивости информационных ресурсов;
* порядок обеспечения сетевой безопасности;
* порядок проведения аудита информационной безопасности;
* порядок управления событиями безопасности информации;
* порядок эксплуатации средств криптографической защиты информации (далее – СКЗИ).

Настоящая Политика разработана в соответствии с:

* Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
* Приказом ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* Приказом ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* приказом ФСБ России от 10.06.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
* приказом ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

# 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 (форма журналов учёта съемных носителей информации приведены в приложении № 1 к настоящей Политике);
* системное и прикладное программное обеспечение, используемое в средствах вычислительной техники;
* средства защиты информации.

Для всех информационных систем должны быть разработаны и поддерживаться в актуальном состоянии Технический паспорт и Описание технологического процесса обработки 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 ИС.

Пользователь – сотрудник Администрации, которому предоставляется доступ к ин­формации, содержащейся в ИС, а также обра­батываемой техническим средством.

Администратор ИС – сотрудник Администрации или иное уполномоченное лицо, которое обеспечивает установ­ку и настройку программного обеспечения (далее – ПО), а также конфигурацию (в том числе изменение прав доступа) к средству вычислительной техники.

Администратор ИБ – сотрудник Администрации, который осуществляет мониторинг и аудит средств защиты информации, используемых в ИС Администрации.

Ответственный пользователь СКЗИ – сотрудник Администрации, который обеспечивает и несет ответственность за соблюдение условий эксплуатации средств криптографической защиты информации в ИС Администрации.

Оператор ИС – физическое или юридическое лицо, которому принадлежит информационная система, взаимодействующая с ИС Администрации или иное уполномоченное лицо, осуществляющее деятельность по ее эксплуатации.

Доступ к информации – возможность получения информации и её использования.

Для управления учётными записями пользователей, разграничения прав доступа к ИС, используется сертифицированное СЗИ от НСД.

Пользователю для работы в ИС предоставляется АРМ.

Каждый пользователь, обеспеченный АРМ, получает аутентификационную информацию (персональное сетевое имя (имя пользователя), пароль). Сведения о правах доступа пользователей к ИС отражаются Администратором ИС согласно разработанной Матрице доступа (Форма Матрицы доступа приведена в приложении №2 к настоящей Политике).

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

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

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

АРМ подлежат опечатыванию/опломбированию (с целью недопущения бесконтрольного изменения аппаратных конфигураций). Опеча­тывание осуществляется только администратором ИС. Пользователи АРМ обязаны следить за сохранностью данных пломб и в случае их нарушений – незамедлительно сообщать о данном событии, администратору 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 802.11x Wi-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 ИС приведён в разделе V 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.

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

Информация о работе пользователей в ИС протоколируется и, при необходимости, может быть предо­ставлена руководителю.

# Раздел III

# 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 и подвергаются регулярной ревизии и контролю.

Учёт съёмных носителей информации осуществляется в журнале учёта съёмных носителей информации (форма журналов учёта приведены в приложении № 1 к настоящей Политике), который ведётся администратором 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.

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 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 ИС 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 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 ИС посредством использования неучтённых (лич­ных) носителей информации, рассматривается как несанкционированное (за ис­ключением случаев, заранее оговорённых и согласованных с администратором ИС).

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

# Раздел IV

# Порядок обеспечения доступа к ИС

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

К работе с ИС 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 ИС определяет руководитель его структурного подразделения на основании должностных (трудовых) обязанно­стей сотрудника.

Основанием для предоставления прав доступа пользователя к ИС является заявка руководителя его структурного подразделения, согласованная Администратором ИС, и Оператором ИС.

Права доступа пользователей к ИС назначаются Администратором ИС в установленном порядке.

Оповещение Оператора ИС об изменении и (или) блокировании прав доступа пользователей к ИС осуществляется Администратором ИС, в следующих слу­чаях:

* выявления нарушений пользователем исполнения установленных норма­тивными правовыми актами Администрации требований по обработке и обеспечению безопасности информации (в том числе персональных данных);
* изменения должностных обязанностей работника (перевода на другую должность);
* увольнения работника.

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

# Раздел V

# Порядок внесения изменений в программное и аппаратное обеспечение

Все изменения программного и аппаратного обеспечения должны быть санкционированы.

Право изменения конфигурации системных и прикладных программных средств, а также в отношении аппаратных средств АРМ пользователей ИС – предоставляется администратору ИС.

Право изменения конфигурации программных и программно-аппаратных средств защиты ин­формации – предоставляется администратору ИБ.

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

Установка (обновление) программного обеспечения АРМ производится с эталонных копий программных средств, хранящихся 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 ИС программного обеспе­чения (форма реестра приведена в приложении № 3 к настоящей Политике). Реестр ведётся Администратором ИС.

# Раздел VI

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

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

|  |  |  |
| --- | --- | --- |
| № п/п | Вид изменений | Порядок необходимых действий |
| 1 | Повышение класса защищённости ИС | Необходимо проведение аттестации (повторно) ИС с выдачей Аттестата соответствия |
| 2 | Увеличение состава угроз ИС, связанное с добавлением новых информационных технологий в ИС |
| 3 | Изменение состава средств защиты информации, указанных в аттестате соответствия, на новые, не указанные в аттестате | Необходимо проведение дополнительных аттестационных испытаний ИС (контроль эффективности) в рамках действующего аттестата соответствия:  администратор ИБ отправляет уведомительное письмо Лицензиату ФСТЭК России, выдавшему Аттестат соответствия, в котором указываются планируемые изменения, а также их причину (форма письма приведена в приложении № 4 к настоящей Политике);  по результатам анализа планируемых изменений, Лицензиат ФСТЭК России принимает решение о необходимости проведения дополнительных аттестационных испытаний ИС и определяет порядок проверки эффективности системы защиты информации в рамках вносимых изменений, о чём извещает администратора ИБ о принятом решении и последующих совместных действиях по внесению изменений;  администратор ИБ 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 ИС;  дополнительные аттестационные испытания ИС проводятся по Программе и методикам, согласованным с администратором ИБ и утверждённым лицензиатом ФСТЭК России;  по результатам дополнительных аттестационных испытаний лицензиатом ФСТЭК России оформляются протокол проведённых испытаний и заключение. Положительные результаты дополнительных аттестационных испытаний дают право на обработку защищаемой информации в ИС с учётом внесённых изменений;  копия уведомительного письма с перечнем планируемых изменений конфигурации ИС, извещение от лицензиата ФСТЭК России, Программа и методики дополнительных аттестационных испытаний и отчётная документация по результатам испытаний хранятся администратором ИС вместе с комплектом аттестационных документов на ИС |
| 4 | Добавление в состав аттестованного ИС новых АРМ |
| 5 | Переустановка средств защиты ин­формации с аттестованных АРМ на новые АРМ с последующим их добавлением в состав аттестованного ИС |
| 6 | Переустановка установленных средств защиты информации, указанных в Аттестате соответствия, на аттестованных АРМ в пределах ИС |
| 7 | Понижение класса защищённости ИС (уменьшение числа актуальных угроз, объёма обрабатываемых данных, снижение требований к характеристикам безопасности и пр.) |
| 8 | Исключение из состава аттестованной ИС некоторых АРМ | Аттестат соответствия сохраняет своё действие |
| 9 | Замена периферийного оборудования АРМ ИС: монитора, принтера, сканера и т.п. | 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 ИС и извещает администратора ИС о возможности внесения данных изменений;  администратор ИС самостоятельно проводит работы по внесению изменений в состав аттестованного ИС;  копия уведомительного письма с составом планируемых изменений конфигурации ИС и извещение от лицензиата ФСТЭК России хранятся администратором ИС вместе с комплектом аттестационных документов |
| 10 | Перемещение АРМ аттестованного ИС в пределах контролируемой зоны |
| 11 | Удаление, установка, переустановка на аттестованных АРМ прикладного программного обеспечения, не связанного с обработкой защищаемой информации |
| 12 | Удаление, установка, переустановка на аттестованных АРМ и (или) серверах программного обеспечения, предназначенного для обработки защищаемой информации (без повышения класса защищённости информационной системы) |
| 13 | Увольнение ответственных работников |

# Раздел VII

# Порядок организации 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 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 ИС;
* запрет деактивации средств антивирусной защиты информации пользова­телями информационных систем;
* деактивация средств антивирусной защиты информации на АРМ ИС только для проведения профилактических меро­приятий и по согласованию с администратором ИБ.

# Раздел VIII

# 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 ИС.

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 ИС. Сотрудники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, создать их новые значения в соответ­ствии с требованиями раздела IX настоящей Политики.

Хранение сотрудником (администратором, пользователем) аутенти­фикационной информации допускается только в личном сейфе (запираемом шкафу, ящике) либо в сейфе (запираемом шкафу, ящике) администратора ИБ. 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 ИС, 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 ИБ.

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 ИС.

# Раздел IX

# Требования к качеству аутентификационной информации и мер по обеспечению её безопасности

К аутентификационной информации пользователей и администрато­ров 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 периода не­использования (дней) | 60 | 90 |
| 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 X

# Контроль физического доступа и защита технических средств

Режим обеспечения безопасности помещений, в которых размещаются компоненты 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 перечня 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.

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

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

Границы контролируемой зоны ИС отражаются в Техническом паспорте 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]](#footnote-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 необходимости продолжения выполнения техническим средством установленных функциональных задач[[3]](#footnote-3).

# Раздел XI

# Обеспечение отказоустойчивости технических средств

Обеспечение отказоустойчивости технических средств осуществляется путём:

* выполнения требований раздела X настоящей Политики;
* контроля пороговых значений основных показателей функционирования технических средств (степени загрузки: процессорных мощностей, дискового пространства, оперативной памяти, каналов связи и пр.);
* обеспечения резервирования технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы;
* осуществления контроля безотказного функционирования технических средств;
* обнаружения и локализации отказов функционирования, принятия мер по восстановлению отказавших средств и их тестирования.
* выполнения периодического резервного копирования информации на резервные машинные носители информации;
* обеспечения надежного хранения резервных копий информации;
* обеспечения надежного хранения эталонных дистрибутивов.

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

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

Резервное копирование должно проводиться только на учтенные машинные носители информации.

# Раздел XII

# Порядок обеспечения 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 III 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;
* год, месяц, число, время создания резервной копии.

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

Учёт проведения резервного копирования должен осуществляться автоматизированными средствами (в случае наличия технической возможности). 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.

Ответственность за резервирование и восстановление защищаемой информации несет Администратор ИС.

Резервное копирование параметров настройки, конфигурации, а также журналов аудита средств защиты информации, осуществляется Администратором ИБ.

# Раздел XIII

# Порядок обеспечения сетевой безопасности

Локально-вычислительная сеть (далее – ЛВС) подлежит защите от воздействий (как внутренних, так и внешних), которые могут привести к:

* нарушению непрерывности функционирования информационных процессов;
* нарушению конфиденциальности защищаемой информации;
* нарушению целостности защищаемой информации.

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

* доступность, целостность и конфиденциальность информационных ре­сурсов;
* защиту сетевого трафика от перехвата;
* простоту используемых технологий защиты информации и их эксплуата­ции;
* прозрачность используемых средств и механизмов защиты для пользова­телей.

Для обеспечения выполнения указанных требований в составе ЛВС могут применяться средства обнаружения вторжений, межсетевого экранирования и криптографической защиты информации.

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

Средствами межсетевого экранирования должен обеспечиваться следующий функционал:

* идентификация сетевых устройств по IP-адресам и (или) MAC-адресам;
* аутентификация сетевых устройств, по одному из протоколов: Remote Authentication Dial-In User Service (RADIUS); Lightweight Directory Access Protocol (LDAP); Kerberos;
* фильтрация информационных потоков по протоколам (например, TCP, UDP, IP), портам и адресам назначения, а также определение маршрутов передачи информации;
* завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного администратором временного интервала неактивности сетевого соединения).

С целью выполнения указанных требований могут применяться:

* программные и программно-аппаратные средства межсетевого экранирования уровня периметра сети – на внешней границе информационной системы;
* программные средства межсетевого экранирования уровня хоста – на внутренних узлах информационной системы (АРМ).

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:

* протоколирование нештатных ситуаций, а также попыток проведения вторжений и предотвращение угроз в журнале регистраций событий, а также предоставление отчетов;
* 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;
* 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 и программно-аппаратные средства обнаружения вторжений уровня периметра сети – на внешней границе информационной системы;
* 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.

Средства криптографической защиты информации, передаваемой по каналам связи, должны применяться в случае, если:

* передача защищаемой информации, в том числе персональных данных, осуществляется по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче защищаемой информации по информационно-телекоммуникационным сетям общего пользования; удаленном доступе и средствам обработки информации, в том числе для администрирования);
* хранение защищаемой информации осуществляется на носителях информации, несанкционированный доступ к которым по стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

С целью выполнения указанных требований могут применяться программные и (или) программно-аппаратные средства криптографической защиты информации (в том числе средства электронной подписи) – на внутренних узлах сегментов информационных систем (АРМ пользователей и серверах информационных систем).

# Раздел XIV

# Порядок проведения внутреннего аудита информационной безопасности

Внутренний аудит заключается в оценке выполнения требований нормативных документов по обеспечению безопасности и защищённости информации, обрабатываемой в ИС. Внутренний аудит представляет собой непрерывную и неотъемлемую часть деятельности, по обеспечению информационной безопасности 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 Администрацией требований по обеспечения информационной безопасности, и внеплановый.

Внеплановый внутренний аудит может проводиться в случае:

* наличия косвенных подтвержденных сведений о нарушениях сотрудниками требований к обеспечению информационной безопасности;
* многократных инцидентов нарушения информационной безопасности, случившихся в Администрации;
* 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 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.

Для проведения внутреннего аналитического аудита, руководителем организации, 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 ИС, 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 ИС, выявленных недостатках и нарушениях, а также разрабатывается план устранения выявленных в ходе проведения внутреннего аналитического аудита информационной безопасности недостатков, который передается на согласование руководителю организации;
* руководитель организации, 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 ИС;
* контроля установки обновлений программного обеспечения;
* проверки выполнения требований, установленных организационно-распорядительными документами Администрации, регламентирующими процессы обработки и защиты информации.
* наблюдения за действиями пользователей ИС с целью контроля соблюдения ими норм и требований обеспечения безопасности информации, установленных в Администрации;
* получения актуальных и объективных данных о текущем состоянии обеспечения безопасности 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 СВТ).

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.

# Раздел XV

# 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,
* контроля эффективности применяемых мер в аттестованной информационной системе.

Тестирование информационных систем на проникновение может осуществляться в режимах «чёрного» или «серого» ящика. Необходимость проведения тестирования на проникновения определяется Администратором ИБ.

Аттестация ИС должна проводиться в соответствии с требованиями, утверждёнными национальными стандартами ГОСТ РО 0043-003-2012 и ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

# Раздел XVI

# Порядок управления событиями безопасности информации

К событиям безопасности информации, подлежащих регистрации в ИС, относятся:

* изменение (в том числе: замена, добавление или изъятие) состава средств обработки информации;
* замена и (или) модификация аппаратной конфигурации средств обработки информации;
* осуществление действий со съёмными носителями информации;
* вынос за пределы контролируемой зоны средств вычислительной техники;
* передача средств вычислительной техники и их компонентов в сторонние организации;
* предоставление аутентификационной и ключевой информации на доступ к средствам обработки защищаемой информации (в том числе по использованию служебной электронной почты и сети Интернет);
* изменение прав доступа к средствам обработки защищаемой информации;
* изменение и (или) компрометация аутентификационной или ключевой информации;
* аутентификация и идентификация пользователей информационной системы (в том числе неуспешная);
* удалённый доступ к средствам обработки защищаемой информации (с указанием протокола доступа);
* действия, совершаемые с защищаемой информацией;
* завершение сеансов работы пользователей информационных ресурсов (систем) и средств обработки защищаемой информации;
* вывод на печать защищаемой информации;
* отключение/перезагрузка или приостановление работы средств обработки защищаемой информации;
* изменение параметров настроек средств обработки защищаемой информации;
* изменение состава и версий программного обеспечения (в том числе баз сигнатур средств антивирусной защиты информации и средств обнаружения вторжений);
* сбои и отказы работоспособности средств обработки защищаемой информации;
* достижение пороговых значений основных показателей функционирования технических средств (степени загрузки: процессорных мощностей, дискового пространства, оперативной памяти, каналов связи и пр.);
* восстановление работоспособности средств обработки защищаемой информации;
* архивирование, резервирование и восстановление защищаемой информации;
* выполнение операций, связанных с эксплуатацией и администрированием средств обработки защищаемой информации).

Перечень типов событий безопасности информации, подлежащих регистрации, должен пересматриваться в том числе по результатам контроля (мониторинга) обеспечения уровня защищённости информации, содержащейся в информационных системах, но не реже чем 1 раз в 2 года.

При регистрации событий безопасности информации регистрации подлежат следующие характеристики событий безопасности информации:

* тип события безопасности информации;
* дата и время события безопасности информации;
* идентификационная информация источника события безопасности информации;
* результат события безопасности информации (успешно или неуспешно);
* субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности информации.

Администратором ИБ должен обеспечиваться непрерывный сбор событий безопасности информации, генерируемых компонентами информационных систем и средствами защиты информации.

Регистрация, учёт и хранение событий безопасности информации должны обеспечиваться Администратором ИБ, срок хранения событий безопасности информации должен составлять не менее 12 месяцев.

Сведения о событиях безопасности информации подлежат защите от неправомерного доступа, уничтожения или модифицирования. Доступ к данным сведениям должен быть ограничен, кроме уполномоченных на это лиц.

Мониторинг событий информационной безопасности может осуществляться как с использованием средств автоматизации (средств, относящихся к средствам сбора и корреляции событий безопасности информации – SIEM), так и без использования таковых.

Мониторинг и анализ событий безопасности информации осуществляется Администратором ИБ в части средств обеспечения функционирования ИС (системного и прикладного программного обеспечения, активного сетевого оборудования) и средств системы обеспечения информационной безопасности.

Периодичность мониторинга и анализа событий безопасности составляет не реже 1 раза в месяц.

К инцидентам информационной безопасности относятся следующие категории негативных событий (группы событий) безопасности информации:

* разглашение защищаемой информации лицами, имеющими право доступа к ней (передача защищаемой информации третьим лицам, не имеющим права доступа к ней; передача защищаемой информации по открытым каналам связи; обработка защищаемой информации на незащищённых технических средствах; публикация защищаемой информации в средствах массовой информации; копирование защищаемой информации на неучтённые съёмные носители информации; утрата съёмных и (или) бумажных носителей информации или передача их лицам, не имеющим права доступа к ним);
* неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации (несанкционированное изменение, копирование защищаемой информации);
* ошибки обслуживающего персонала при эксплуатации информационных систем;
* дефекты, сбои, отказы программного обеспечения и аварии технических средств и систем обеспечения их отказоустойчивого функционирования;
* природные явления, стихийные бедствия (пожары, наводнения, землетрясения, грозовые разряды).

При обнаружении инцидента информационной безопасности (или события безопасности информации, имеющего признаки инцидента) должен быть незамедлительно проинформирован Администратор ИБ (средствами служебной электронной почты и посредством телефонной связи).

Сообщение о случившемся инциденте информационной безопасности должно содержать следующую информацию:

* Ф.И.О., должность работника, выявившего инцидент информационной безопасности;
* время обнаружения инцидента информационной безопасности;
* описание инцидента информационной безопасности.

На каждый инцидент информационной безопасности Администратором ИБ формируется карточка инцидента информационной безопасности (в соответствии с приложением № 5 к Политике).

До момента полного заполнения карточки инцидента информационной безопасности и, соответственно, закрытия инцидента информационной безопасности она своевременно заполняется и ведётся в электронном виде, после чего распечатывается и хранится на бумажном носителе.

# Раздел XVII

# Порядок эксплуатации СКЗИ

В процессе эксплуатации СКЗИ должны выполняться следующие процедуры:

* + - учет СКЗИ;
    - учет пользователей СКЗИ;
    - обеспечение эксплуатации СКЗИ в соответствии с требованиями;
    - контроль соблюдения условий эксплуатации СКЗИ;
    - хранение, выдача, замена и уничтожение СКЗИ;
    - реализация необходимых мероприятий при утере и компрометации СКЗИ.

Учет СКЗИ осуществляет ответственный пользователь СКЗИ в журнале учета СКЗИ, эксплуатационной и технической документации к ним в соответствии с приложением № 7.

Учет пользователей СКЗИ осуществляет ответственный пользователь СКЗИ путем создания и ведения лицевых счетов пользователей СКЗИ в соответствии с приложением № 8.

Условия использования СКЗИ в ИС должны периодически, но не реже 1 раза в год, проверяться на соответствие требованиям эксплуатации СКЗИ.

Проверки осуществляются комиссионно. Состав комиссии, сроки и порядок ее работы назначает ответственный за организацию обработки персональных данных.

Результаты проверок оформляются Актом результатов проверки условий использования СКЗИ по форме Приложения 6 к Политике. В Акте результатов проверки условий использования СКЗИ должны быть отражены результаты проверки по следующим пунктам:

* состояние и актуальность журнала учета СКЗИ;
* состояние и актуальность журнала учета пользователей СКЗИ;
* соответствие технического состояния СКЗИ и сопрягаемых с СКЗИ ТС требованиям эксплуатационной документации на СКЗИ, ИС и систему защиты информации;
* знание и выполнение пользователями правил хранения, выдачи и уничтожения СКЗИ;
* знание и выполнение пользователями правил защиты СКЗИ.

В случае потери или компрометации СКЗИ ответственный за организацию обработки персональных данных назначает внеплановую проверку условий использования СКЗИ.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи ответственный пользователь СКЗИ должен немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

При обнаружении недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения ответственный пользователь СКЗИ организует срочные меры к их розыску.

Начальник общего отдела администрации

Новоминского сельского

поселения

Каневского

района Л.Е.Власенко

# Приложение № 1

# к Политике обеспечения информационной безопасности в информационных системах администрации Новоминского сельского поселения Каневского района

Форма

Журнал 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 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Приложение № 2

# к Политике обеспечения информационной безопасности в информационных системах администрации Новоминского сельского поселения Каневского района

Форма

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование подразделения, должность | Ф.И.О., пользователя | Имя АРМ пользователя | Учетная запись | Наименование информационной системы, учетная запись пользователя, его роль (права доступа) | Объекты файловой системы (права доступа) |
| ИС | наименование объекта1 (путь) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 |  |  |  |  |  | - |
| 2 |  |  |  |  |  | - |
| 3 |  |  |  |  |  | - |

# Приложение № 3

# к Политике обеспечения информационной безопасности в информационных системах администрации Новоминского сельского поселения Каневского района

Форма

Реестр программного обеспечения, разрешённого к использованию в ИС

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Дата включения в реестр | Название ПО | Версия, не ниже |
| 1 | 2 | 3 | 4 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Приложение № 4

# к Политике обеспечения информационной безопасности в информационных системах администрации Новоминского сельского поселения Каневского района

ФОРМА

Уведомление лицензиата ФСТЭК России о планируемых изменениях информационной системы, аттестованной по требованиям безопасности

|  |  |
| --- | --- |
|  | Директору ООО «ТСС»  Сергиеву В.В.  350061, Краснодарский край, г. Краснодар, ул. Благоева, 24/1, лит. А1 |

Уважаемый Виктор Викторович!

Уведомляем Вас о внесении следующих изменений в состав и настройку информационной системы администрации Новоминского сельского поселения Каневского района, аттестат № «*Номер аттестата соответствия*» от «*Дата выдачи аттестата соответствия*», размещенной по адресу: «*Адрес размещения компонентов информационной системы*».

|  |  |  |
| --- | --- | --- |
| № | Состав и причина изменений | Дата внесения изменений |
| *1* | *Обновление сертифицированного средства защиты информации от несанкционированного доступа Secret Net Studio 8 до версии «8.5.5329»* | *«Дата»* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Приложение № 5

# к Политике обеспечения информационной безопасности в информационных системах администрации Новоминского сельского поселения Каневского района

КАРТОЧКА

инцидента информационной безопасности № \_\_\_\_

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование характеристики инцидента информационной безопасности (далее - ИБ): | Описание |

| 1 | 2 | 3 |
| --- | --- | --- |
| 1. Общие сведения об инциденте ИБ | | |
| 1.1. | Номер записи согласно Журналу учёта инцидентов ИБ |  |
| 1.2. | Дата и время возникновения инцидента ИБ |  |
| 1.3. | Дата и время регистрации инцидента ИБ |  |
| 1.4. | Источник информации об инциденте ИБ | работник или техническое средство |
| 1.5. | Ф.И.О. и должность работника, обнаружившего инцидент ИБ |  |
| 1.6. | Контактные данные работника, обнаружившего инцидент |  |
| 1.7. | Наименование технического средства, при использовании которого обнаружен инцидент ИБ |  |
| 1.8. | Описание инцидента ИБ |  |
| 2. Содержание инцидента ИБ | | |
| 2.1. | Сведения о нарушении установленных организационно-распорядительными документами требований по обеспечению ИБ | «нет» «наименование документа, регламентирующего требование; № пункта документа» |
| 2.2. | Данные о нарушителе требований по обеспечению ИБ | «нет» «Фамилия И.О., должность нарушителя» |
| 2.3. | Категория инцидента ИБ | «случайный» «преднамеренный» |
| 2.4. | Тип инцидента ИБ | «свершившийся» «попытка осуществления инцидента ИБ» «подозрение на инцидент ИБ» |
| 3. Воздействие инцидента на информационные системы и средства обработки защищаемой информации | | |
| 3.1. | Типы объектов (систем), затронутых инцидентом | «файлы/базы данных, содержащие защищаемую ин-формацию» «автоматизированные рабочие места» «серверы информационных систем» «активное сетевое оборудование» «средства защиты информации» «носители информации (в том числе бумажные носители)» «системное/прикладное программное обеспечение» «линии и сети передачи данных» «помещения, здания, сооружения, инженерные сети и коммуникации» |
| 3.2. | Нарушенные свойства безопасности: | «конфиденциальность», «целостность», «доступность» |
| 3.3 | Область распространения и действия инцидента ИБ | «пределы одной информационной системы» «пределы отдельного структурного подразделения» |
| 3.4. | Критичность инцидента ИБ | «высокая», «средняя», «низкая» |
| 4. Локализация и устранение последствий инцидента ИБ | | |
| 4.1. | Информирование об инциденте ИБ | «дата и время информирования и кому сообщено» |
| 4.2. | Назначение ответственного лица за локализацию инцидента ИБ | «дата и время, Ф.И.О., должность ответственного лица» |
| 4.3. | Планируемый срок локализации инцидента ИБ | «планируемый срок, определённый ответственным лицом» |
| 4.4. | Сведения о локализации инцидента ИБ | «дата и время, описание предпринятых действий» |
| 4.5. | Назначение ответственного лица за устранение последствий инцидента ИБ | «дата и время, Ф.И.О., должность ответственных лиц» |
| 4.6. | Планируемый срок устранения последствий инцидента ИБ | «планируемый срок, определённый ответственным лицом» |
| 4.7. | Сведения об устранении последствий инцидента ИБ | «дата и время, описание предпринятых действий» |
| 5. Расследование инцидента ИБ и реализация корректирующих мер | | |
| 5.1. | Сведения о комиссии по расследованию инцидента ИБ | «дата и время назначения комиссии, состав ее членов» |
| 5.2. | Сведения о причинах возникновения инцидента ИБ | «описание» |
| 5.3. | Сведения о лицах, понесших ответственность за инцидент ИБ | «Ф.И.О., должность лица, вид ответственности» |
| 5.4. | Степень вероятности повторного возникновения инцидента ИБ | «нет», «минимальная», «средняя», «высокая» |
| 5.5. | Перечень корректирующих мер, направленных на предупреждение повторного возникновения инцидента | «описание» |

Дата, время закрытия инцидента ИБ: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ф.И.О., подпись администратора ИБ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Приложение № 6

# к Политике обеспечения информационной безопасности в информационных системах администрации Новоминского сельского поселения Каневского района

Акт **№ \_\_\_\_\_\_\_\_**

проверки соблюдения условий использования

средств криптографической защиты информации

Дата составления: «\_\_\_\_» \_\_\_\_\_\_\_ 201\_\_ г.

Место проведение проверки: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Комиссия в составе:

Председатель

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В соответствии с требованиями «Политики обеспечения информационной безопасности информационной системы администрации Новоминского сельского поселения Каневского района» проведена проверка соблюдений условий использования средств криптографической защиты информации в информационной системе администрации Холмского сельского поселения Абинского райна.

В ходе проведения проверки определялись:

* + состояние и актуальность журнала учета СКЗИ;
  + состояние и актуальность журнала учета пользователей СКЗИ;
  + соответствие технического состояния СКЗИ и сопрягаемых с СКЗИ ТС требованиям эксплуатационной документации на СКЗИ, ИС и систему защиты информации;
  + знание и выполнение пользователями правил хранения, выдачи и уничтожения СКЗИ;
  + знание и выполнение пользователями правил защиты СКЗИ;
  + случаи компрометации СКЗИ и действия по устранению причин и последствий компрометации СКЗИ;
  + состояние помещений с установленными или хранящимися в них СКЗИ и состояние режима доступа в эти помещения;
  + наличие и состояние хранилищ СКЗИ и режим доступа к ним.

Выявленные нарушения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ЗАКЛЮЧЕНИЕ комиссии:

Соблюдений условий использования средств криптографической защиты информации СООТВЕТСТВУЕТ (НЕ СООТВЕТСТВУЕТ) *(нужное подчеркнуть)* требованиям к условиям использования СКЗИ в информационной системе администрации Новоминского сельского поселения Каневского района.

Председатель комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Приложение № 7

# к Политике обеспечения информационной безопасности в информационных системах администрации Новоминского сельского поселения Каневского района

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Наименование СКЗИ | Регистрационные номера СКЗИ | | Номера экземпляров ключевых документов | | Отметка о получении | | | | Отметка о выдаче | | | |
| От кого получены | | | Дата и номер сопроводительного письма | Ф.И.О. пользователя СКЗИ | | Дата и расписка в получении | |
| 1 | 2 | 3 | | 4 | | 5 | | | 6 | 7 | | 8 | |
| *1* | *VipNet Client 4.3* | *123-456789* | | *1* | | *ООО «БИС»* | | | *12.12.2020 г. Договор № 1234562* | *[И.О. Фамилия администратора информационной безопасности]* | | *(подпись)* | |
|  |  |  | |  | |  | | |  |  | |  | |
|  |  |  | |  | |  | | |  |  | |  | |
|  |  |  | |  | |  | | |  |  | |  | |
|  |  |  | |  | |  | | |  |  | |  | |
|  |  |  | |  | |  | | |  |  | |  | |
|  |  |  | |  | |  | | |  |  | |  | |
| Отметка о подключении (установке) СКЗИ | | | | | | | Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов | | | | | | Примечание | |
| Ф.И.О. пользователя СКЗИ, производившего подключение (установку | | | Дата подключения (установки) и подписи лиц, произведших подключение (установку) | | Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ | | Дата изъятия (уничтожения) | Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение) | | | Номер акта или расписка об уничтожении | |
| 9 | | | 10 | | 11 | | 12 | 13 | | | 14 | | 15 | |
| *[Краткое наименование организации]* | | | *01.01.2020 г.* | | *Инв. № 00023* | |  |  | | |  | | *Пример заполнения* | |
|  | | |  | |  | |  |  | | |  | |  | |
|  | | |  | |  | |  |  | | |  | |  | |
|  | | |  | |  | |  |  | | |  | |  | |
|  | | |  | |  | |  |  | | |  | |  | |
|  | | |  | |  | |  |  | | |  | |  | |
|  | | |  | |  | |  |  | | |  | |  | |
|  | | |  | |  | |  |  | | |  | |  | |

# Приложение № 8

# к Политике обеспечения информационной безопасности в информационных системах администрации Новоминского сельского поселения Каневского района

Лицевой счет пользователя СКЗИ

Пользователь \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование СКЗИ | Регистрационные номера СКЗИ | Номера экземпляров ключевых документов | Дата получения | Примечание |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

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* [↑](#footnote-ref-1)
2. *Внешние воздействия – воздействия окружающей среды, нестабильности электроснабжения, кондиционирования и иные внешние факторы* [↑](#footnote-ref-2)
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* [↑](#footnote-ref-3)