УТВЕРЖДЕНА

приказом управления записи
актов гражданского состояния
Ставропольского края

от «___»_____г. № _____

ИНСТРУКЦИЯ

администратора безопасности персональных данных обрабатываемых в автоматизированных информационных системах управления записи актов гражданского состояния Ставропольского края

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Полное наименование
АИС ЗАГС, Система	Автоматизированная информационная система Управления записей актов гражданского состояния Ставропольского края
АРМ	Автоматизированное рабочее место
ИБ	Информационной безопасность
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОРД	Организационно-распорядительная документация
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПК	Программный комплекс
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина
РФ	Российская Федерация
СИБ	Система информационной безопасности автоматизированной информационной системы Управления записей актов гражданского состояния Ставропольского края
СКЗИ	Средства криптографической защиты информации
СрЗИ	Средство защиты информации
УЗАГС СК	Управление записи актов гражданского состояния Ставропольского края

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

– В настоящем документе используются следующие термины и определения:

– Автоматизированная информационная система – совокупность программно-аппаратных средств, предназначенных для автоматизации деятельности, связанной с хранением, передачей и обработкой информации;

– Администратор безопасности Системы – сотрудник УЗАГС СК, в обязанности которого входит обеспечение штатного функционирования средств и системы защиты от несанкционированного доступа к защищаемой информации;

– АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным программным обеспечением) для выполнения определенной производственной задачи;

– Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности;

– Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз;

– Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

– Защита от НСД к информации – это деятельность, направленная на предотвращение несанкционированного доступа к защищаемой информации;

– Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

– Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

– Информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации;

– Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ;

– Машинный носитель конфиденциальной информации – материальный носитель, предназначенный для записи и воспроизведения конфиденциальной информации средствами вычислительной техники, а также сопрягаемыми с ними устройствами;

– Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы;

– Несанкционированный доступ – доступ к информации, нарушающий или обходящий установленные правила Системы с использованием штатных средств Системы или средств перехвата и обработки защищаемой информации в каналах связи Системы, не защищенных от НСД к информации организационно-техническими методами (за исключением средств перехвата и обработки побочных сигналов, сопровождающих функционирование Системы, технических средств Системы и программных средств скрытого информационного воздействия);

– Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации;

– Пользователь Системы – сотрудник УЗАГС СК, участвующий в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты;

– Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

– Разрешительная система доступа – таблица, отображающая правила разграничения доступа пользователей к защищаемой информации;

– Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;

– Средства антивирусной защиты – набор программ для обнаружения компьютерных вирусов, других вредоносных программ и лечения инфицированных файлов, а также для профилактики предотвращения заражения файлов или операционной системы вредоносным кодом;

– Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты информации;

– Средства криптографической защиты информации – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем и осуществлять криптографическое преобразование информации для обеспечения ее безопасности;

– Съемный машинный носитель конфиденциальной информации – машинный носитель информации, содержащий конфиденциальную информацию, который не входит в комплектность системного блока ПЭВМ, но может подключаться и отключаться;

– Угрозы безопасности конфиденциальной информации – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к конфиденциальной информации, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение конфиденциальной информации, а также иные неправомерные действия при их обработке в АИС ЗАГС.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая инструкция (далее – Инструкция) определяет основные требования к работе администратора безопасности Системы и разработана в соответствии с руководящими документами РФ, внутренними правилами, инструкциями и положениями УЗАГС СК.

2. Действие Инструкции распространяется на администратора безопасности Системы.

3. Администратор безопасности Системы подчиняется ответственному за обеспечение безопасности конфиденциальной информации при их обработке в АИС ЗАГС.

4. Администратор безопасности Системы отвечает за поддержание необходимого уровня безопасности конфиденциальной информации, обрабатываемой в АИС ЗАГС, на этапах ее эксплуатации и модернизации.

5. Администратор безопасности Системы выполняет работу по администрированию средств защиты информации и реализации принятой в отношении АИС ЗАГС политики безопасности.

6. При выполнении своих обязанностей администратор безопасности Системы должен:

– знать и соблюдать требования по защите информации;

– выполнять требования инструкции по обеспечению антивирусной защиты Системы и проведению антивирусного контроля;

– выполнять требования инструкции по организации парольной защиты в информационной системе;

– выполнять требования инструкции по эксплуатации используемых в Системе средств защиты информации;

– выполнять требования Инструкции.

7. Администратор безопасности Системы должен знать:

– действующее законодательство РФ в области ИБ;

– специализацию и особенности деятельности УЗАГС СК;

– методы и средства контроля охраняемых сведений, выявления каналов утечки информации;

– методы планирования и организации работ по защите информации;

– средства контроля и защиты информации, перспективы и направления их совершенствования;

– порядок пользования реферативными и справочно-информационными изданиями, а также другими источниками научно-технической информации;

– правила и нормы охраны труда, техники безопасности и противопожарной защиты.

8. Администратор безопасности Системы несет ответственность за обеспечение безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в АИС ЗАГС, а также за правильность использования и нормального функционирования системы информационной безопасности АИС ЗАГС.

9. Администратором безопасности Системы назначается лицо, имеющее высшее профессиональное образование в области защиты информации. Желательным условием при назначении администратора безопасности АИС ЗАГС является наличие опыта работы в сфере обеспечения защиты информации.

10. К администратору безопасности Системы, помимо квалификационных, предъявляются следующие требования:

– оконченное высшее техническое образование;

– знания основ теории баз данных;

– знания основных понятий и определений численных методов и математической статистики;

– знания принципов построения электронных вычислительных машин и их устройств;

– знания по периферийным устройствам электронных вычислительных машин, принципам их работы; механическим узлам, входящих в их состав;

– знания по конструкции персональных компьютеров, их составу, по компоновке;

– знания и опытом работы с современными операционными системами;

– знания и опыт адаптации программного обеспечения обработки информации к конкретным электронно-вычислительным машинам;

– навыки администрирования локальной вычислительной сети и образующего её активного сетевого оборудования;

– опыт работы с СрЗИ:

– СрЗИ «Secret Net 7»;
– СрЗИ «vGate R2»;
– СКЗИ «ViPNet SafeDisk-V 4.1»;
– ПАК «ViPNet Coordinator HW»;
– ПК «ViPNet Administrator»;
– ПК «ViPNet Client»;
– Средство антивирусной защиты «Kaspersky Endpoint Security»;

– Система предотвращения вторжений с функцией межсетевого экрана «StoneGate IPS»;

– ПК «Acronis Backup & Recovery 11»;

– СКЗИ «КриптоПро CSP», версии 3.6;

– Средство анализа защищенности «RedCheck».

11. Во время отсутствия администратора безопасности Системы (командировка, отпуск, болезнь и др.) его должностные обязанности выполняет работник управления, назначаемый в установленном порядке ответственным за обеспечение безопасности конфиденциальной информации при их обработке в АИС ЗАГС, и несущий полную ответственность за качественное, эффективное и своевременное их исполнение.

II. ФУНКЦИИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ СИСТЕМЫ

1. Администратор безопасности Системы осуществляет установку, настройку и сопровождение технических (программно-аппаратных) средств защиты, входящих в состав системы информационной безопасности АИС ЗАГС, а также выполняет, в рамках своих должностных обязанностей, определенных Инструкцией, организационные мероприятия по обеспечению безопасности конфиденциальной информации, включая ПДн.

2. Администратор безопасности Системы осуществляет настройку и сопровождение подсистемы идентификации/аутентификации, при этом:

– осуществляет управление идентификаторами пользователей, включающее:

– присвоение и выдачу идентификаторов пользователям;

– предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного периода времени;

– блокирование идентификатора пользователя после установленного времени неиспользования;

– осуществляет управление паролями пользователей, включающее:

– назначение и выдачу пользователям АИС ЗАГС паролей для доступа к информационным ресурсам Системы;

– установление характеристик пароля в соответствии с требованиями инструкции по организации парольной защиты в информационной системе;

– блокирование (прекращение действия) или замену утерянных, скомпрометированных или поврежденных средств аутентификации;

– обновление паролей с установленной периодичностью (не более чем через 120 дней);

– защиту парольной информации от неправомерного доступа к ней и модифицирования путем установления запрета на смену пароля пользователем Системы;

– осуществляет настройку идентификации/аутентификацию технических средств АИС ЗАГС.

3. Администратор безопасности Системы осуществляет настройку и сопровождение подсистемы управления доступом, при этом:

– осуществляет управление учетными записями пользователей, включающее:

– своевременное создание и удаление учетных записей пользователей АИС ЗАГС по запросу ответственного за обеспечение безопасности конфиденциальной информации при изменениях в списке сотрудников, допущенных к работе с защищаемыми информационными ресурсами (прием на работу, увольнение, перемещение сотрудника);

– верификацию пользователя при заведении учетной записи пользователя – проверку личности пользователя, уточнение в установленном порядке его должностных (функциональных) обязанностей по обработке объектов защиты;

– определение типа учетной записи, объединение учетных записей в группы (при необходимости);

– пересмотр и, при необходимости, корректировку учетных записей пользователей;

– блокирование учетных записей в случае необходимости;

– заведение, контроль использования и уничтожение временных и гостевых учетных записей;

– реализует полномочия доступа для каждого пользователя Системы к элементам защищаемых информационных ресурсов на основе разрешительной системы доступа к информационным (программным) ресурсам АИС ЗАГС;

– осуществляет настройку блокирования учетной записи пользователя при превышении установленного количества неуспешных попыток входа в информационную систему;

– осуществляет настройку блокирования сеанса доступа пользователя после установленного времени его бездействия (неактивности);

– ограничивает применение в АИС ЗАГС съемных носителей информации путем установления соответствующих настроек на блокировку подключения к ПЭВМ;

– выполняет требования по обеспечению безопасности информации при организации технического обслуживания средств обработки конфиденциальной информации АИС ЗАГС и отправке их в ремонт (контролирует затирание информации, содержащей конфиденциальные сведения, на машинных носителях информации с составлением соответствующего Акта).

4. Администратор безопасности Системы осуществляет настройку и сопровождение подсистемы регистрации и учета событий безопасности, при этом:

– проводит регулярный анализ (не реже одного раза в неделю) системного журнала СрЗИ от НСД для выявления попыток НСД к защищаемым ресурсам;

– производит еженедельное архивирование электронного журнала, обеспечивает хранение информации о событиях безопасности в течение установленного срока (минимум – в течение 6 месяцев);

– своевременно информирует руководство и ответственного за обеспечение

безопасности конфиденциальной информации о несанкционированных действиях персонала и участвует в расследовании попыток НСД;

– устанавливает в средствах защиты от НСД необходимое количество циклов очистки (обнуления, обезличивания) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей;

– обеспечивает защиту информации о событиях безопасности – хранение информации о событиях безопасности, исключающее доступ к ней пользователей АИС ЗАГС.

5. Администратор безопасности Системы осуществляет настройку и сопровождение подсистемы обеспечения целостности информационной системы и информации, при этом:

– периодически проверяет обеспечение целостности программных средств и обрабатываемой информации;

– периодически тестирует функции установленных в АИС ЗАГС средств защиты от НСД к информации, особенно при изменении полномочий пользователей;

– обеспечивает наличие в АИС ЗАГС дистрибутивов установленного ПО, в том числе дистрибутивов установленных в Системе программных средств защиты от НСД с резервными файлами настроек;

– восстанавливает программную среду, программные средства, программные СрЗИ от НСД и их настройки при сбоях в Системе;

– осуществляет настройку обнаружения и реагирования на поступление в Систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию АИС ЗАГС (защита от спама).

6. Администратор безопасности Системы осуществляет сопровождение подсистемы анализа защищенности, при этом:

– контролирует работоспособность, правильность функционирования программного обеспечения и средств защиты информации;

– контролирует соответствие настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в документе «Инструкция по эксплуатации используемых в Системе средств защиты информации»;

– устанавливает обновления программного обеспечения, включая программное обеспечение средств защиты информации, полученные из доверенных источников;

– восстанавливает работоспособность (правильность функционирования) и параметры настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов в соответствии с требованиями, приведенным в документе «Инструкция по эксплуатации используемых в Системе средств защиты информации»;

– контролирует состав технических средств, программного обеспечения и средств защиты информации (не реже одного раза в три месяца), при этом:

– проверяет сохранность наклеек с защитной и идентификационной информацией на корпусах ЭВМ;

– проверяет соответствие состава технических средств, программного обеспечения и средств защиты информации сведениям, приведенным в эксплуатационной документации;

– проверяет условия и сроки действия сертификатов соответствия на СрЗИ;

– при обнаружении несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации восстанавливает программную среду в соответствии с документально утвержденным составом ПО, участвует в работах по восстановлению исходной конфигурации технических средств;

– участвует в работах по внесению изменений в аппаратно-программную конфигурацию АИС ЗАГС, участвует в приемке новых программных средств;

– ведет учет изменений состава технических средств, программного обеспечения и средств защиты информации.

7. Администратор безопасности Системы осуществляет настройку и сопровождение подсистемы антивирусной защиты, при этом:

– осуществляет настройку средства антивирусной защиты информации в соответствии с инструкцией по обеспечению антивирусной защиты Системы и проведению антивирусного контроля;

– осуществляет периодические проверки (не реже одного раза в месяц) компонентов Системы (рабочих мест пользователей, серверов) на наличие вирусов;

– обеспечивает обновление баз данных признаков вредоносных компьютерных программ из доверенных источников (не реже одного раза в неделю);

– обеспечивает своевременное реагирование, выполнение действий при обнаружении вредоносных компьютерных программ и оповещение руководства.

8. Администратор безопасности Системы осуществляет настройку и сопровождение подсистемы межсетевого экранирования, включающая в себя функцию обнаружения вторжений, при этом:

– настраивает идентификацию/аутентификацию администратора МЭ при его локальных запросах на доступ;

– настраивает регистрацию входа (выхода) администратора МЭ в систему (из системы). В параметрах регистрируемых событий должны быть указаны:

– дата, время и код регистрируемого события;

– результат попытки осуществления регистрируемого события – успешная или неуспешная;

– идентификатор администратора МЭ, предъявленный при попытке осуществления регистрируемого события;

– настраивает правила фильтрации МЭ;

– настраивает регистрацию и учет фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации;

– обеспечивает восстановление свойств МЭ после сбоев и отказов оборудования;

– настраивает правила обнаружения вторжений (атак);

– настраивает уведомления о вторжениях.

9. Администратор безопасности Системы осуществляет сопровождение подсистемы криптографической защиты, при этом:

– осуществляет настройку СКЗИ в соответствии с требованиями нормативных документов по безопасности информации;

– реализует полномочия доступа пользователей к средству защиты канала передачи данных, генерирует и выдает пользователям, допущенным к работам с СКЗИ, пароли для доступа к СКЗИ;

– своевременно выявляет попытки посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– ведет Журнал учета средств криптографических средств защиты информации.

10. Администратор безопасности Системы осуществляет настройку и сопровождение подсистемы защиты среды виртуализации, при этом:

– осуществляет настройку идентификации/аутентификации субъектов доступа и объектов доступа в виртуальную инфраструктуру, в том числе администраторов управления средствами виртуализации;

– осуществляет настройку регистрации событий безопасности в виртуальной инфраструктуре.

11. Администратор безопасности Системы осуществляет методическое руководство работой пользователей Системы в вопросах обеспечения безопасности конфиденциальной информации, при этом:

– проводит обучение пользователей перед началом работы в АИС ЗАГС правилам и мерам защиты конфиденциальных данных, в частности:

– ознакомление пользователей под роспись с содержанием основных нормативно-методических документов в области обеспечения безопасности конфиденциальной информации, а также организационно-распорядительной документацией АИС ЗАГС;

– инструктаж пользователей Системы по правилам работы с используемыми техническими средствами и системами защиты информации;

– обучение навыкам выполнения операций в рамках назначенных им должностных обязанностей в части организации обработки и обеспечении безопасности конфиденциальной информации;

– осуществляет периодические проверки (не реже одного раза в год) знаний пользователями положений нормативной и организационно-распорядительной документации по вопросам обеспечения безопасности конфиденциальной информации, правил работы со средствами защиты информации;

– выявляет ошибки и некорректную работу пользователей Системы с элементами АИС ЗАГС и средствами защиты;

– оказывает помощь пользователям Системы в части применения средств защиты и консультирует по вопросам введенного режима защиты;

– контролирует соблюдение пользователями политики разграничения доступа к ресурсам Системы, а также требований организационно-распорядительной документации, регламентирующей обеспечение безопасности конфиденциальной информации.

12. При обнаружении нарушения установленного порядка доступа к информационным ресурсам Системы со стороны зарегистрированного пользователя Системы, администратор безопасности Системы обязан приостановить доступ такого пользователя до выяснения причин и принятия решения по данному вопросу.

13. Администратор безопасности обязан периодически представлять отчет ответственному за обеспечение безопасности конфиденциальной информации о состоянии защиты АИС ЗАГС и о нештатных ситуациях на объектах Системы и допущенных пользователями нарушениях относительно установленных требований по защите информации.

14. После получения запроса ответственного за обеспечение безопасности конфиденциальной информации на создание или изменение учетной записи пользователя, администратор безопасности Системы создает/изменяет учетную запись и формирует перечень паролей доступа пользователей к ресурсам АИС ЗАГС, который направляет соответствующим пользователям. Указанные сведения должны направляться с соблюдением требований к работе с документами, содержащими конфиденциальные сведения.

15. При изменении обязанностей или полномочий пользователя по запросу ответственного за обеспечение безопасности конфиденциальной информации администратором безопасности Системы осуществляется своевременная корректировка реализованных прав доступа к информационным (программным) ресурсам АИС ЗАГС.

16. Администратору безопасности Системы запрещается:

– используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации;

– использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий;

– передавать третьим лицам тем или иным способом имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки рабочих мест;

– производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы Системы, блокированию доступа, потере информации без санкции руководства и предупреждения пользователей;

– передавать свои идентификаторы и пароли доступа администратора безопасности Системы другим лицам. Администратор безопасности Системы несет

личную ответственность за их сохранность.

17. Администратор безопасности Системы в пределах своей компетенции осуществляет взаимодействие с подразделениями и лицами, участвующими в информационных технологических процессах, направляет запросы и получает необходимую информацию из других подразделений организации для согласования работ по обработке конфиденциальной информации.

III. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ СИСТЕМЫ

18. Администратор безопасности информации имеет право:

– доступа в помещения, где установлена АИС ЗАГС, обрабатывающая конфиденциальную информацию;

– требовать прекращения обработки в случае нарушения установленного порядка работ или нарушения функционирования СрЗИ от НСД и расследования фактов НСД;

– участвовать в анализе ситуаций, касающихся функционирования средств защиты от НСД и расследования фактов НСД;

– в случае выявления нарушений в СИБ, принимать меры к сотрудникам, допустивших нарушения, и немедленно информировать ответственного за обеспечение безопасности конфиденциальной информации при их обработке в АИС ЗАГС;

– проводить гласные и негласные проверки состояния защиты информации в Системе;

– принимать экстренные меры по ликвидации последствий выявленных нарушений;

– разрабатывать предложения по совершенствованию системы защиты от НСД в Системе;

– вносить предложения по всем вопросам своей работы руководителю организации.

IV. ОТВЕТСТВЕННОСТЬ

19. Администратор безопасности Системы несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в АИС ЗАГС, состояние и поддержание установленного уровня защиты конфиденциальной информации, обрабатываемой в АИС ЗАГС.

20. Ответственность за ознакомление администратора безопасности Системы с Инструкцией несет ответственный за обеспечение безопасности конфиденциальной информации при их обработке в АИС ЗАГС.

21. Администратор безопасности Системы несет ответственность за несоблюдение требований Инструкции в соответствии с действующим законодательством и локальными нормативными актами УЗАГС СК.

Заместитель начальника управления К.С.Попов