УТВЕРЖДЕНО

приказом управления записи
актов гражданского состояния
Ставропольского края

от «___»_____г. № _____

ПОЛОЖЕНИЕ

о порядке организации и проведения работ по защите персональных данных в автоматизированных информационных системах управления записи актов гражданского состояния Ставропольского края

I. Общие положения

1. Настоящее положение о порядке организации и проведения работ по защите персональных данных в автоматизированных информационных системах управления записи актов гражданского состояния Ставропольского края (далее – Положение) определяет содержание и порядок осуществления мероприятий по защите информации в автоматизированных информационных системах управления записи актов гражданского состояния Ставропольского края (далее – АИС ЗАГС СК).

2. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом Феде-

ральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», руководящим документом Государственной технической комиссии Российской Федерации от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

3. Целью настоящего Положения является регулирование работ по защите информации и обеспечение функционирования АИС ЗАГС СК.

4. Информация, циркулирующая в АИС ЗАГС СК, связанная с персональными данными (далее – ПДн) и сведениями конфиденциального характера, подпадает под действие федеральных законов Российской Федерации, направленных на обеспечение конституционных прав граждан, на сохранение личной тайны и конфиденциальности информации.

II. Организация и проведение работ по обеспечению безопасности защищаемой информации

5. Под организацией обеспечения безопасности защищаемой информации при ее обработке в АИС ЗАГС СК понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности защищаемой информации, реализуемых в рамках создаваемой системы защиты информации (далее – СЗИ).

6. Безопасность защищаемой информации при ее обработке в АИС ЗАГС СК обеспечивает управление записи актов гражданского состояния Ставропольского края (далее – управление) или лицо (пользователь АИС ЗАГС СК), осуществляющее обработку защищаемой информации по поручению управления ЗАГС СК на основании заключаемого с этим лицом договора или соглашения, который должен предусматривать обязанности по обеспечению безопасности защищаемой информации при ее обработке в АИС ЗАГС СК.

7. Защита информации, содержащейся в АИС ЗАГС СК, обеспечивается путем выполнения управлением требований к организации защиты информации, содержащейся в АИС ЗАГС СК, и требований к мерам защиты информации.

8. Все носители информации, установленные на защищаемых автоматизированных рабочих местах (далее – АРМ), и хранящие конфиденциаль-

ную информацию, подлежат обязательному учёту в Журнале учета машинных носителей информации, содержащих персональные данные.

9. Порядок учета, хранения и обращения с машинными носителями информации устанавливается документом «Инструкция по порядку учета использования съемных носителей персональных данных в автоматизированных информационных системах управления записей актов гражданского состояния Ставропольского края».

10. Защита от компьютерных вирусов производится в соответствии с документом «Инструкция по антивирусной защите в автоматизированной информационной системе управления записи актов гражданского состояния Ставропольского края».

11. Парольная система защиты информации организуется в соответствии с Инструкцией по организации парольной защиты в автоматизированной информационной системе управления записи актов гражданского состояния Ставропольского края.

12. В целях обнаружения пожара в помещениях управления предусматриваются специальные автоматические устройства сигнализации возникновения пожара.

13. Для предотвращения и ликвидации пожара в помещениях сотрудники управления в зависимости от обстановки проводят мероприятия по спасению людей и оборудования, а также:

– доводят до конца, если позволяет обстановка, решение текущих задач;

– собирают и выносят машинные носители информации и журналы учета;

– отключают источники питания и вентиляцию;

– организуют защиту оборудования от попадания в него воды, копоти (с помощью пластиковых листов, чехлов и т.п.).

14. Размещение и установка технических средств в помещениях, где обрабатывается конфиденциальная информация, должны исключать возможность хищения устройств (блоков) технических средств и предотвращать бесконтрольное использование и визуальный просмотр обрабатываемых сведений лицами, не имеющими к ним отношения.

15. Допуск в помещения, где размещены технические средства, представителей для ремонта и уборки помещений осуществляется в присутствии лиц, осуществляющих эксплуатацию технических средств.

16. Для обеспечения безопасности защищаемой информации, содер-

жащейся в АИС ЗАГС СК, и организацию обработки защищаемой информации, управлением ЗАГС СК назначается структурное подразделение или должностное лицо (администратор безопасности), ответственное за обеспечение безопасности информации.

17. Для обеспечения защиты информации, содержащейся в АИС ЗАГС СК, проводятся следующие мероприятия:

– формирование требований к защите информации, содержащейся в АИС ЗАГС СК;

– разработка средств защиты информации (далее – СЗИ);

– внедрение СЗИ;

– аттестация АИС ЗАГС СК по требованиям защиты информации;

– обеспечение защиты информации, в ходе эксплуатации аттестованной АИС ЗАГС СК;

– обеспечение защиты информации при выводе из эксплуатации аттестованной АИС ЗАГС СК или после принятия решения об окончании обработки информации.

18. Для проведения мероприятий и работ по защите информации в ходе создания и эксплуатации АИС ЗАГС СК, при необходимости, привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 года. № 99-ФЗ «О лицензировании отдельных видов деятельности».

19. Для обеспечения защиты информации, содержащейся в АИС ЗАГС СК, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 года. № 184-ФЗ «О техническом регулировании».

20. СЗИ включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности защищаемой информации, уровня защищенности персональных данных, который необходимо обеспечить, класса государственной информационной системы и информационных технологий, используемых в АИС ЗАГС СК.

21. Для обеспечения безопасности информации в АИС ЗАГС СК применяются следующие меры:

– 21.1. организационные меры:

– инструктаж пользователей по правилам обеспечения безопасности информации;

– учет и хранение съемных носителей информации, и порядок их обращения, исключающие хищение, подмену и уничтожение;

– мониторинг и реагирование на инциденты информационной безопасности;

– контроль за соблюдением требований по обеспечению безопасности информации;

– ограничение доступа посторонних лиц к техническим средствам АИС ЗАГС СК, а также к носителям информации, содержащим защищаемую информацию;

– размещение технических средств в пределах контролируемой зоны;

– организация физической защиты помещений и технических средств, осуществляющих обработку информации;

– 21.2. технические меры:

– разграничение доступа пользователей АИС ЗАГС СК к информационным ресурсам;

– регистрация действий пользователей АИС ЗАГС СК;

– резервирование технических средств и носителей информации;

– использование защищенных каналов связи, при необходимости;

– предотвращение внедрения в АИС ЗАГС СК вредоносных программ и программных закладок;

– применение сертифицированных средств защиты информации.

III. Обязанности работников управления по обеспечению информационной безопасности

22. Практическая реализация мероприятий по защите информации и контроль за соблюдением безопасности информации в управлении возлагается на ответственного по защите информации, назначаемого приказом управления.

23. На ответственного по защите информации возлагается:

– осуществление контроля за выполнением приказов, инструкций в части обеспечения безопасности и защиты информации в управлении ЗАГС СК;

– своевременное создание и ведение баз эталонных копий программного обеспечения автоматизированных информационных систем;

– взаимодействие по вопросам обеспечения безопасности и защиты информации с органами государственной власти и контролирующими органами;

– разработка проектов приказов, распоряжений и инструкций по обеспечению защиты информации и осуществление контроля за выполнением требований указанных документов;

– анализ состояния работ по обеспечению защиты информации и выработка предложений по ее совершенствованию;

– выявление конфиденциальной информации и ее документальное

оформление в виде перечня сведений, подлежащих защите;

– осуществление контроля за сменой паролей в установленное время;

– контроль за хранением машинных носителей с общим программным обеспечением и пакетов прикладных программ, предназначенных для тиражирования;

– контроль за выполнением специальных требований по размещению технических средств, прокладке кабельных трасс и инженерных систем;

– инструктаж и консультирование работников управления по вопросам обеспечения защиты информации;

– участие в проведении расследований по фактам нарушения безопасности информации в управлении;

– организация учета и хранения машинных носителей информации, в соответствии с Инструкцией по порядку учета использования съемных носителей персональных данных.

24. На администратора безопасности ПДн возлагается:

– организация охраны служебных помещений;

– организация антивирусной защиты АИС ЗАГС СК;

– создание надлежащих условий, обеспечивающих безопасность сохранения машинных и бумажных носителей информации в помещениях;

– выбор и установка технических и общесистемных программных средств, совместно с ответственным по защите информации, удовлетворяющих требованиям настоящего Положения;

– разработка, при необходимости, инструкций, методических материалов по использованию разрешенных технологических и общесистемных программных средств с включением в них раздела, отражающего вопросы защиты информации.

– выполнять обязанности в соответствии с Инструкцией администратора безопасности персональных данных автоматизированной информационной системы управления записи актов гражданского состояния Ставропольского края.

25. Методическое руководство администратором безопасности ПДн осуществляет начальник отдела информатизации и защиты информации.

26. Ответственность за выполнение мероприятий по обеспечению защиты информации структурных подразделениях возлагается на руководителей подразделений.

27. Работник управления, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным АИС ЗАГС СК, несет персональную ответственность за свои дейст-

вия и обязан:

– Соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АИС ЗАГС СК;

– Выполнять правила работы со СЗИ на своем АРМ;

– Хранить в тайне свой пароль (пароли) в соответствии с Инструкцией по организации парольной защиты в автоматизированной информационной системе управления записи актов гражданского состояния Ставропольского края, с установленной периодичностью принимать меры по замене своего пароля (паролей);

– Действовать в соответствии с требованиями соответствующих документов по работе со средствами криптозащиты информации в случае предоставления ему права защиты (подтверждения подлинности и авторства) документов, передаваемых по технологическим цепочкам в АИС ЗАГС СК, при помощи электронной цифровой подписи;

– Немедленно вызывать ответственного по защите информации и ставить в известность руководителя структурного подразделения в случае подозрении компрометации личных ключей и паролей, а также при обнаружении:

– фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к защищенному АРМ;

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

– некорректного функционирования установленных на АРМ технических средств защиты;

28. Присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ в структурном подразделении.

29. Сотрудникам управления ЗАГС СК запрещается:

– использовать компоненты программного и аппаратного обеспечения АИС ЗАГС СК в неслужебных целях;

– передавать сведения конфиденциального характера по незащищенным каналам связи (факс, электронная почта и т.п.);

– несанкционированно копировать, распространять, изменять, использовать документы конфиденциального характера;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства;

– осуществлять обработку конфиденциальной информации в присутствии посторонних лиц, не допущенных к данной информации;

– записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.);

– оставлять включенной без присмотра свою ПЭВМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

– оставлять без личного присмотра на рабочем месте или где бы то ни было персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок необходимо поставить в известность ответственного по защите информации и руководителя своего структурного подразделения.

IV. Контроль обеспечения защиты информации в ходе эксплуатации АИС ЗАГС СК

30. Контроль (мониторинг) за обеспечением безопасности информации в АИС ЗАГС СК осуществляется путем проведения периодических контрольных мероприятий и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

31. В рамках проведения контрольных мероприятий выполняется следующее:

– контроль событий безопасности и действий пользователей в АИС ЗАГС СК;

– контроль (анализ) защищенности информации, содержащейся в АИС ЗАГС СК;

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

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

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

32. Контрольные мероприятия проводятся как периодически, так и внепланово по решению ответственного за обеспечение безопасности информации в АИС ЗАГС СК и в случае возникновения инцидентов информационной безопасности.

33. Внутренние проверки в АИС ЗАГС СК должны проводится в случае выявления следующих фактов инцидентов информационной безопасности:

– нарушение конфиденциальности, целостности, доступности информации;

– несоблюдение требований к обеспечению безопасности информации;

34. В ходе выявления инцидентов и реагирования на них осуществляются:

– определение лиц, ответственных за выявление инцидентов и реагирование на них;

– обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в АИС ЗАГС СК пользователями и администратором безопасности;

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

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению АИС ЗАГС СК и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

35. По результатам проведения внутренней проверки составляется отчет о результатах внутренней проверки режима защиты информации в соответствии с Приложение.

Заместитель начальника управления К.С.Попов

Приложение

к Положению о порядке организации и проведения работ по защите персональных данных в автоматизированных информационных системах управления записи актов гражданского состояния Ставропольского края

ОТЧЕТ

о результатах внутренней проверки режима защиты информации в автоматизированной информационной системе Управления ЗАГС Ставропольского края

Внутренняя проверка произведена на основании Положения по организации и проведению работ по обеспечению безопасности защищаемой информации при ее обработке в АИС ЗАГС К утвержденного приказом управления записи актов гражданского состояния Ставропольского края от «___» _____г. № _____.

Проверка проводилась «___» _____20__ г. по адресу:

_____
_____

В ходе проверки были проведены следующие мероприятия:

1.

_____
____

2.

_____
____

Результаты проведения проверки:

6.

_____
____

7.

_____
____

Необходимые мероприятия.

На основании проведения внутренней проверки режима защиты информации рекомендуется осуществить следующие мероприятия:

11.

_____
___
12.
_____
___

Подписи ответственных лиц, проводивших внутреннюю проверку режима защиты информации:

_____	_____	_____
(дата)	(подпись)	(расшифровка)
_____	_____	_____
(дата)	(подпись)	(расшифровка)
_____	_____	_____
(дата)	(подпись)	(расшифровка)