ЗАО «РАМЭК-ВС»

НА СЛУЖБЕ БИЗНЕСА
И ГОСУДАРСТВА

RAMDOC
powered by Open Text

Защита персональных данных в информационных системах персональных данных на базе продуктов Open Text.
Использование RAMDOC Power by Open Text - сертифицированного решения на базе Open Text в информационных системах ПДн.

Содержание

О чем пойдет речь?

- Система электронного документооборота **RAMDOC Power by Open Text** и платформа **Open Text** – преимущества и сертификация.
- Нормативная база в области защиты персональных данных.
- Классификация ИСПДн.
- Контролирующие органы и ответственность.
- Этапы создания СЗПДн.

Система электронного документооборота RAMDOC Power by Open Text

Возможности и преимущества системы RAMDOC

- Система электронного документооборота **RAMDOC** - предназначена для организации электронного документооборота и делопроизводства в государственных органах и крупных коммерческих компаниях на основе действующего законодательства и стандартов РФ

- **RAMDOC** позволяет организовать единое информационное пространство обработки документов, с полным учетом сложившейся практики нумерации, классификации и контроля исполнения документов

- **RAMDOC** разработана на базе семейства продуктов OpenText ECM Suite 2010, разработки компании Open Text и поддерживает различную архитектуру аппаратных средств (с одним, с двумя или тремя серверами, кластерную архитектуру, кластерную архитектуру с балансировкой нагрузки и др.)

- **RAMDOC** представляет удобную схему администрирования, позволяющую реализовать централизованное управление всеми компонентами

- **RAMDOC** имеет развитую защиту от несанкционированного доступа, включающую систему идентификаторов и паролей, разграничение прав доступа к объектам и функциям, создание ролей пользователей, хранения и передачи информации с различными метками конфиденциальности

Система электронного документооборота RAMDOC Power by Open Text

Сертификация системы RAMDOC

В настоящее время уже успешно завершены испытания и проводятся заключительные мероприятия по получению сертификата на систему RAMDOC в системе сертификации ФСТЭК России.

- на соответствие требованиям Руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по **4 уровню контроля** и технических условий РАМГ.50123-01 ТУ, а также оценки возможности использования в автоматизированных системах до класса защищенности **1Г** включительно и **в информационных системах обработки персональных данных до 1 класса** включительно.

Наличие данного сертификата позволит:

- использовать встроенные в систему **RAMDOC** механизмы защиты информации для выполнения большинства требований к системе защиты от несанкционированного доступа ИСПДн до класса **К1** включительно, что позволит привести ИСПДн на основе **RAMDOC в соответствие ФЗ-152.**

Сертификация платформы Open Text

Сертификация платформы Open Text

В основе продукта RAMDOC лежит платформа Open Text в составе пакетов Open Text CLM package 2012 и Shared Services Suite, включающих все основные модули Open Text, в том числе непосредственно сама платформа Enterprise Library Services.

- Таким образом сертификат на RAMDOC распространяется на входящую в его состав платформу Open Text.

Наличие данного сертификата позволит:

- использовать встроенные в платформу Open Text механизмы защиты информации для выполнения большинства требований к системе защиты от несанкционированного доступа ИСПДн до класса **К1** включительно, что позволит **привести ИСПДн, построенные на платформе Open Text 2010, в соответствие ФЗ-152.**

Основные положения ФЗ от 27 июля 2006 г. 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

1) Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация;

2) Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

3) Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

Статья 25. п.3. с учетом принятых поправок «Информационные системы персональных данных, созданные до дня вступления настоящего Федерального закона, должны были быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 июля 2011 года.»

Нормативная база

Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ
«О персональных данных» с изменениями от 17.12.2010 г.

Постановление правительства РФ от 17 ноября 2007 г. № 781
«Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. №55/86/20 г. Москва
«Об утверждении порядка проведения классификации информационных систем персональных данных»

Документы ФСТЭК России

«Базовая модель угроз безопасности ПДн при их обработке в информационных системах персональных данных»

«Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах персональных данных»

«Положение о методах и способах защиты в информационных системах защиты персональных данных»

Документы ФСБ России

«Методические рекомендации по обеспечению с помощью криптографических средств безопасности ПДн при обработке в информационных системах персональных данных с использованием автоматизации»

«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств , предназначенных для защиты информации, не содержащих сведений составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных».

Классификация типовых ИСПДн

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных. Определяются следующие категории обрабатываемых в информационной системе персональных данных (ХПД):

Категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

Категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

Категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;

Категория 4 – обезличенные и (или) общедоступные персональные данные.

Классификация типовых ИСПДн

Класс типовой информационной системы определяется в соответствии с таблицей.

Хпд \ Хнпд	3 (менее 1 000)	2 (от 1 000 до 100 000)	1 (более 100 000)
Категория 4 (Обезличенные ПДн)	К4	К4	К4
Категория 3 (однозначная идентификация субъекта ПДн)	К3	К3	К2
Категория 2 (однозначная идентификация субъекта ПДн+ доп.информация)	К3	К2	К1
Категория 1 (сведения о состояние здоровья, интимной жизни, вероисповедании субъекта и т.д.)	К1	К1	К1

Классификация ИСПДн

По результатам анализа исходных данных информационной системе присваивается один из следующих классов:

Класс 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

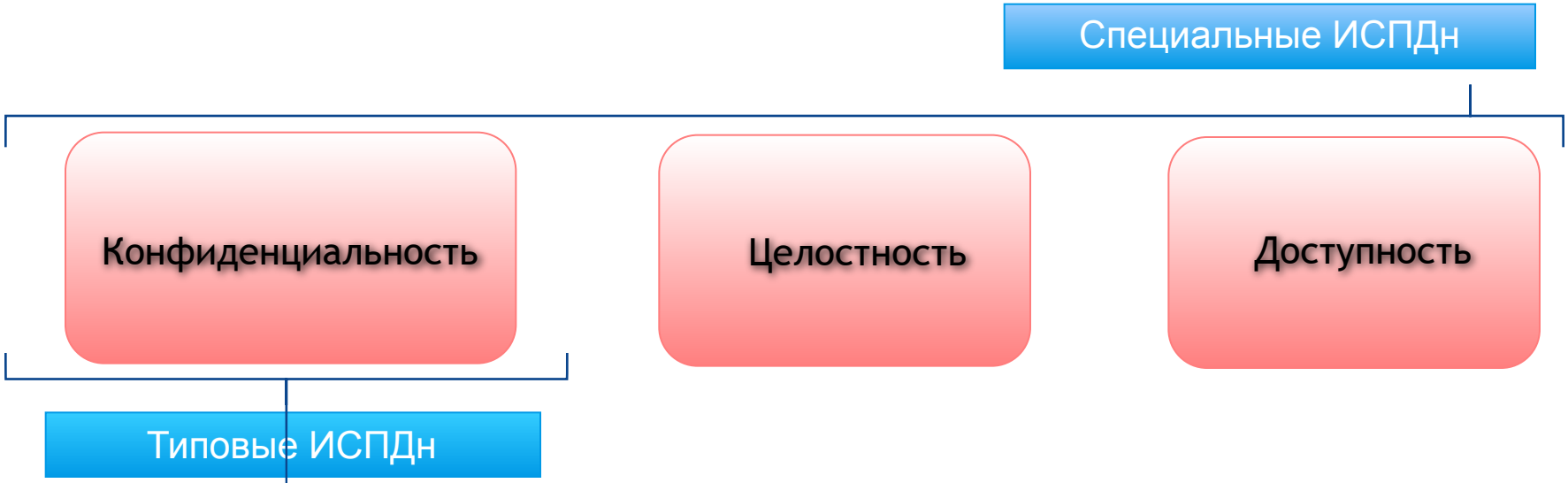
Класс 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

Класс 3 (К3) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

Класс 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Классификация специальных информационных систем персональных данных

Специальные информационные системы - информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).



По результатам анализа исходных данных класс специальной информационной системы определяется на основе **модели угроз безопасности персональных данных.**

RAMDOC
powered by Open Text

Контролирующие органы

Роскомнадзор	**Государственный контроль достаточности принятых мер по обеспечению безопасности ПДн**
ФСТЭК РФ ФСБ РФ	**Разработка методов и способов защиты информации в информационных системах ПДн в пределах полномочий**
Оператор*	**Обеспечение безопасности ПДн при их обработке путем выполнения требований к системе защиты.** ***Выполнение требований может быть поручено уполномоченному лицу, имеющему разрешительные документы на этот вид деятельности***

Ответственность

Лица, виновные в нарушении требований закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Кодекс об административных правонарушениях (КоАП РФ)	Статьи: **13.11, 13.12, 13.13, 13.14, 5.27, 5.39, 19.4, 19.5, 19.6, 19.7, 19.20, 20.25**	• Штраф до 500 тыс. руб.; • Приостановление деятельности на срок до 90 суток; • Дисквалификация должностного лица на срок от одного года до трех лет.
Трудовой кодекс (ТК РФ)	Статьи: **237, 195, 90, 81**	• Денежная компенсация за причиненный моральный вред; • Увольнение.
Уголовный кодекс (УК РФ)	Статьи: **137, 140, 171**	• Штраф до 300 тыс. руб.; • Арест до 6-ти месяцев; • Лишение права занимать должность на срок до 5-ти лет;

Организационные мероприятия

Разовые

- Сбор и анализ исходных данных
- Разработка модели угроз
- Разработка модели нарушителя
- Классификация ИСПДн
- Разработка организационно-распорядительной документации (приказы, изменения в инструкции, положение по защите ПДн и др.)

Периодические

- Физическая охрана в помещениях ИСПДн
- Ведение журналов учета (допуска к работе, съемных носителей и др.)
- Обучение сотрудников

Технические мероприятия

Защита от НСД

- Управление доступом
- Регистрация и учет
- Обеспечение целостности
- Криптографическая защита
- Антивирусная защита
- Обнаружение вторжений
- Анализ защищенности

Защита от утечки по техническим каналам

- Создание активных электромагнитных помех
- Звукоизоляция ограждающих конструкций (при речевой обработке ПДн)
- Исключение просмотра информации

Требования к оператору или привлекаемой организации

Федеральный закон РФ №128-ФЗ от 8 августа 2001 года «О лицензировании отдельных видов деятельности»

Лицензии ФСТЭК России

Лицензии ФСБ России

Наличие специалистов имеющих профильное образование или прошедших обучение (повышение квалификации)

Наличие необходимой нормативно-методической и руководящей документации

Наличие необходимого материально-технического обеспечения

Постановление Правительства РФ № 504 от 15.08.2006г. «О лицензировании деятельности по технической защите конфиденциальной информации» (ПП №504) дает определение (п.2 Положения) ТЗКИ – под ТЗКИ «понимается комплекс мероприятий и(или) услуг по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней». п. 12 Постановления Правительства РФ № 781 от 17.11.2007 г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» указывает десять мероприятий, часть мероприятий (например, установка и ввод в эксплуатацию СЗИ) действительно являются деятельностью по ТЗКИ, и, в соответствии с ФЗ-128 эта деятельность лицензируется.

Этапы создания СЗПДн

Предпроектная стадия

- Перечень ПДн
- Архитектура ИСПДн
- Перечень угроз безопасности ПДн
- Класс ИСПДн
- Техническое задание на СЗПДн

Стадия проектирования

- Технический проект
- Разработка организационно-распорядительной документации
- Эксплуатационная документация
- Строительно-монтажные работы

Стадия ввода в действие

- Внедрение системы защиты персональных данных
- Опытная эксплуатация
- Приемо-сдаточные испытания
- Оценка соответствия

Этапы создания СЗПДн

1 Аудит информационной системы персональных данных, анализ соответствия нормативным требованиям

- *Получение исходных качественных и количественных параметров для организации проектирования;*
- *Оценка состояния системы по параметрам соответствия с требованиями руководящих документов ФСТЭК и ФСБ России.*

→ Отчет об обследовании (концепция)

2 Разработка требований безопасности информационной системы персональных данных

- *Классификация ИСПДн;*
- *Формирование модели угроз безопасности;*
- *Разработка требований по безопасности;*
- *Проведение экспертизы в регулирующих органах (по желанию заказчика).*

→ Техническое задание на проектирование

3 Разработка системы защиты персональных данных

- *Проектирование системы защиты;*
- *Разработка организационно-распорядительной документации;*
- *Отработка процессов функционирования системы, проведение испытаний и доводка на макетах и стендах (по желанию заказчика)*

→ Технический проект

RAMDOC
powered by Open Text

Этапы создания СЗПДн

4 Внедрение проектных решений *(установка, пуско-наладка аппаратных средств, инсталляция и настройка СПО)*

→ Действующая система защиты информации

- *Разработка разрешительной документации системы доступа, организационно-распорядительной документации, технической документации на объект в части касающейся защиты ПДн;*
- *Проведение испытаний на соответствие требований безопасности информации, включая экспертное обследование объекта информатизации, исследований на предмет утечки по техническим каналам, комплексные испытания защищенности.*

5 Испытание СЗИ объектов информатизации

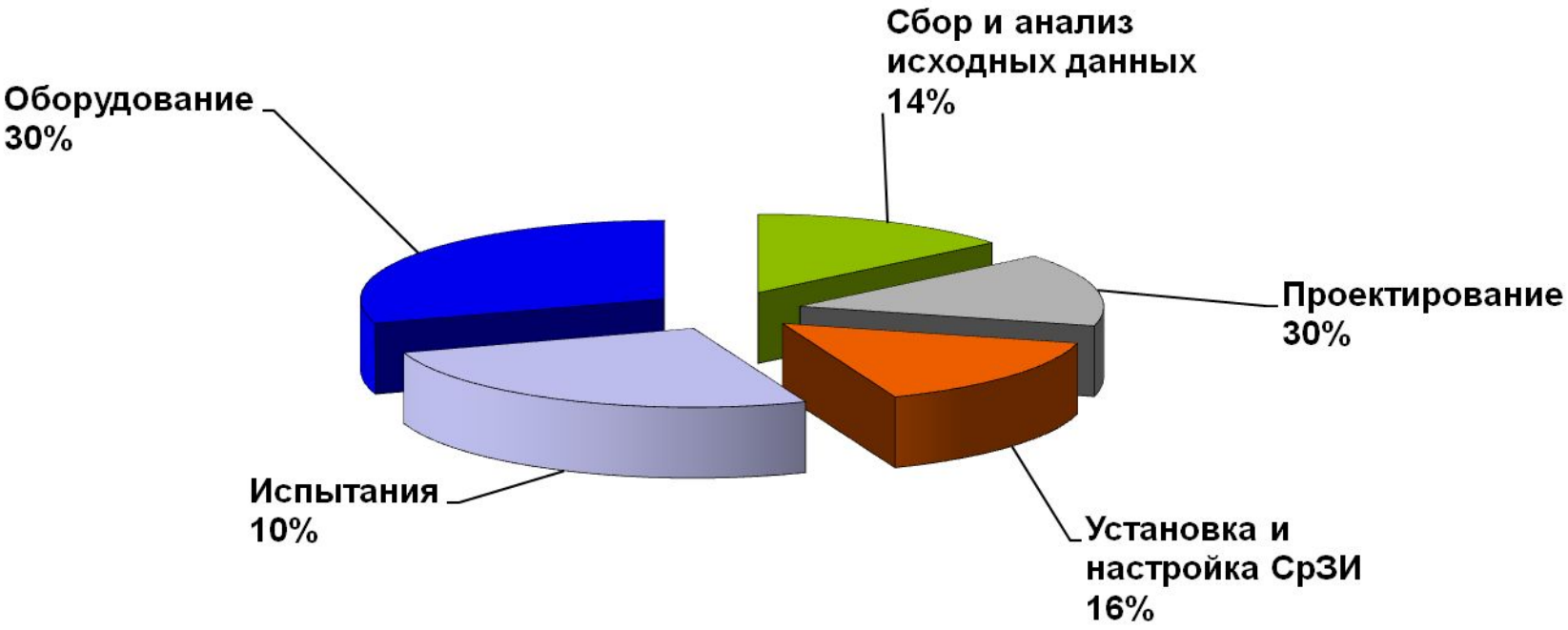
→ Заключение о соответствии

6 Сервисное обслуживание

→ Оперативное восстановление системы, периодический контроль

RAMDOC
powered by Open Text

Структура затрат на СЗПДн



Что нас ждет ?

Возможно:

- Устранение выявленных противоречий в подзаконных актах, нормативных и руководящих документах;
- Пересмотр требований к операторам по наличию соответствующих лицензий.

Что делать?

- Ответственно подойти к выполнению требований закона;
- **Самостоятельно и с привлечением специализированных организаций приступить к реализации мероприятий обеспечивающих выполнение требований Закона.**

СПАСИБО ЗА ВНИМАНИЕ !

Волков Дмитрий Валерьевич,
зам. нач. отдела комплексных систем безопасности
Телефон: (495) 221-17-18 * доб. 2605.

Московское представительство
Адрес: 109316, Москва, Волгоградский пр. 2
Тел.: (495) 221-17-18, Факс: (495) 221-17-18

Директор департамента информационной безопасности
ШИБКОВ СЕРГЕЙ ИЛЬИЧ
(495) 221-17-18 * доб. 2642, моб. +7 (925)729-95-56

- Отдел комплексных систем безопасности
- Зам. нач. отдела Волков Дмитрий Валерьевич
  (495) 221-17-18 * доб. 2605, моб. +7 (925) 011-28-48

- Отдел НИОКР
- Начальник отдела Варакин Юрий Васильевич
  (495) 221-17-18 * доб. 2602, моб. +7 (925)294-25-17

- Отдел аттестации объектов информатизации
- Начальник отдела Морозкин Андрей Борисович
  (495) 221-17-18 * доб. 2689, моб. +7 (925)010-40-84

- Отдел специальной экспертизы
- Начальник отдела Букреев Игорь Алексеевич
  (495) 221-17-18 * доб.2606, моб. +7 (925)010-40-85

- Испытательная лаборатория
- Начальник ИЛ Тимохин Сергей Иванович
  (495) 221-17-18 * доб.2690