ТЕХЦЕНТР
ЗАЩИТА ИНФОРМАЦИИ И ОБЪЕКТОВ

Разработка систем защиты персональных данных, обрабатываемых в библиотечных информационных системах

Докладчик: кандидат технических наук,
технический директор ООО «Техцентр»
КУЗНЕЦОВ Андрей Владимирович

ООО «Техцентр
Контактные телефоны:
8 (812) 300-14-00
8 (812) 394-78-89
8 (812) 300-24-00

Российское законодательство в области защиты персональных данных

Федеральный Закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (в ред. Федеральных законов от 25.11.2009 N 266-ФЗ т 27.12.2009 N 363-ФЗ).

Обязанности операторов персональных данных

Предоставление сведений о наличии ПДн субъекту в доступной форме (статья 14 ФЗ).

Предоставление субъекту по его просьбе информации, касающейся обработки ПДн (статья 18 ФЗ).

Принятие организационных и технических мер для защиты ПДн при их обработке (статья 19 ФЗ).

Безвозмездное предоставление субъекту возможности ознакомления с ПДн, внесение в них изменения, уничтожение или блокирование ПДн, а также уведомление об этом субъекта (статья 20 ФЗ).

ФЗ №152 «О персональных данных». (Статья 25)

Информационные системы *(включая системы информационного взаимодействия)* персональных данных, созданные до 1 января 2011 года, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 июля 2011 года.

Операторы, которые осуществляют обработку персональных данных до дня вступления в силу настоящего Федерального закона и продолжают осуществлять такую обработку после дня его вступления в силу, обязаны направить в уполномоченный орган по защите прав субъектов персональных данных, за исключением случаев, предусмотренных частью 2 статьи 22 настоящего Федерального закона, уведомление, предусмотренное частью 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2008 года.

РИСКИ НЕИСПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Неисполнение требований Закона «О персональных данных» влечет для Предприятий и Учреждений риски следующего характера:

Гражданские иски со стороны клиентов или работников;

Приостановление или прекращение обработки персональных данных;

Привлечение Предприятия (Учреждения) и (или) ее руководителя **к административной, уголовной, гражданской, дисциплинарной и иным видам ответственности;**

Приостановление действия или аннулирование лицензий на основной вид деятельности Предприятия (Учреждения);

Репутационные риски;

Риски недобросовестной конкуренции (приостановления деятельности Предприятия (Учреждения) с подачи конкурентов при имеющихся нарушениях правил защиты персональных данных).

ЭТАПЫ РАБОТ ПО СОЗДАНИЮ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Предпроектная стадия

Задачи предпроектной стадии:

- обследование информационной системы персональных данных;
- определение угроз безопасности, а также формирование частной модели нарушителя;
- выдача рекомендаций по классификации информационной системы персональных данных;
- формирование общих и специальных требований в виде проекта Технического задания с целью создания системы защиты информации ИСПДн.

На этапе Предпроектной стадии разрабатываются:

- «Отчет об обследовании информационной библиотечной системы как информационной системы персональных данных»;
- Проект «Акта классификации информационной системы персональных данных»;
- «Модель угроз безопасности персональных данных»;
- «Техническое задание на создание системы защиты информации информационной системы персональных данных».

ЭТАПЫ РАБОТ ПО СОЗДАНИЮ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Стадия проектирования

Основной задачей стадии проектирования является разработка и обоснование технических решений и оформление проектной документации на систему защиты информации.

На этапе проектирования разрабатываются:

- СЗИ ИСПДн. Ведомость технического проекта;
- СЗИ ИСПДн. Пояснительная записка к Техническому проекту;
- СЗИ ИСПДн. Ведомость покупных изделий;
- СЗИ ИСПДн. Схема организационной структуры;
- Комплект рабочей документации на СЗИ ИСПДн.

ЭТАПЫ РАБОТ ПО СОЗДАНИЮ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Стадия ввода в эксплуатацию системы защиты информации

На этапе ввода в эксплуатацию системы защиты информации осуществляется:

- поставка аппаратно-программных средств защиты информации СЗИ ИСПДн, выбранных в качестве проектных технических решений;
- установка и настройка средств защиты информации;
- разработка и оформление организационно-распорядительной документации;
- аттестация объектов информатизации (при необходимости).

В состав разрабатываемой организационно-распорядительной документации входят:

- Инструкция администратора безопасности информации СЗИ ИСПДн;
- Инструкция по эксплуатации средств защиты информации СЗИ ИСПДн;
- Инструкция по организации парольной защиты в СЗИ ИСПДн;
- Инструкция по антивирусной защите СЗИ ИСПДн;
- Описание технологического процесса обработки информации в ИСПДн;
- Разрешительная система доступа к информационным ресурсам ИСПДн;
- Положение о защите персональных данных.

ТИПОВЫЕ РЕШЕНИЯ ПО ЗАЩИТЕ ИСПДн

1. Решение по защите персональных данных, обрабатываемых на автономном рабочем месте (автономной ЛВС) без подключения к сети связи общего пользования:

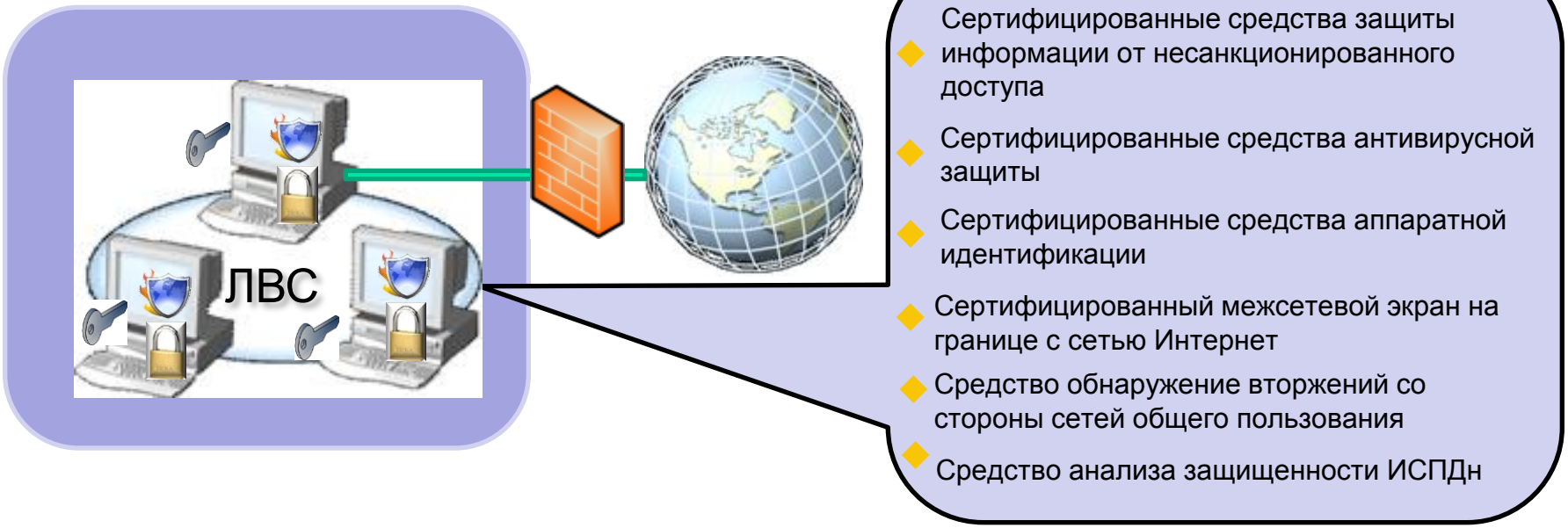
- Сертифицированное ФСТЭК России средство защиты информации от несанкционированного доступа
- Сертифицированное ФСТЭК России средство антивирусной защиты

Стоимость аппаратно-программных средств защиты информации и работ по защите автономного АРМ составит:

- от 8 500 рублей для приобретения средств защиты;
- от 2 000 рублей – установка и настройка средств защиты.

ТИПОВЫЕ РЕШЕНИЯ ПО ЗАЩИТЕ ИСПДн

2. Решение по защите персональных данных, обрабатываемых в локальной вычислительной сети при наличии подключения к сети связи общего пользования:

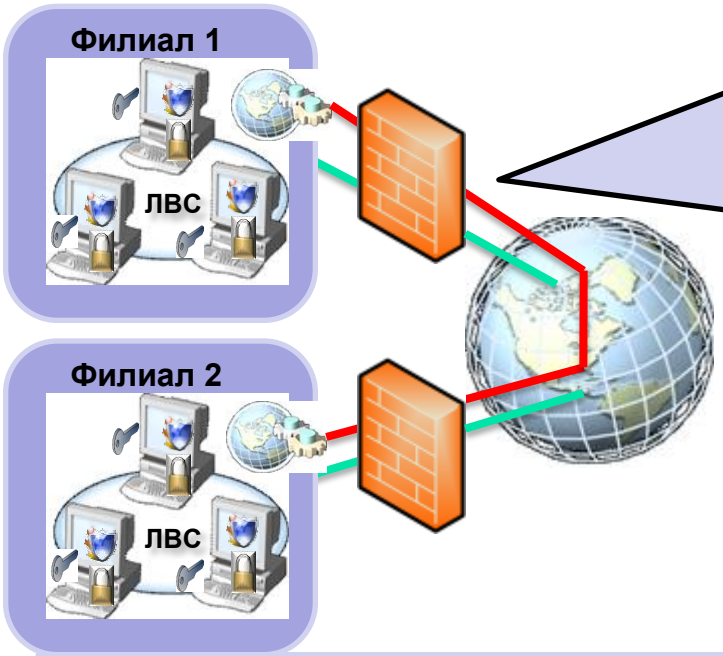


Стоимость аппаратно-программных средств защиты информации и работ по защите ИСПДн составит:

- от 10500 рублей для средств защиты информации каждого АРМ;
- от 80 000 рублей для межсетевого экрана в каждой точке соединения с Интернет;
- от 9000 рублей (до 4 сетевых узлов в ЛВС) для средства анализа защищенности;
- 20% стоимости средств защиты на работы по их установке и настройке.

ТИПОВЫЕ РЕШЕНИЯ ПО ЗАЩИТЕ ИСПДн

3. Решение по защите персональных данных, обрабатываемых в распределенной вычислительной сети :



- Сертифицированные средства защиты информации от несанкционированного доступа
- Сертифицированные средства антивирусной защиты
- Сертифицированные средства аппаратной идентификации
- Сертифицированные межсетевые экраны на границе с сетью Интернет
- Средство обнаружение вторжений со стороны сетей общего пользования
- Средство анализа защищенности ИСПДн
- Сертифицированные средства построения VPN

Стоимость защиты распределенной ЛВС составит:

- от 10500 рублей для средств защиты информации каждого АРМ;
- от 80 000 рублей для межсетевого экрана в каждой точке соединения с Интернет;
- от 9000 рублей (до 4 сетевых узлов в ЛВС) для средства анализа защищенности;
- от 120 000 рублей для каждого филиала (СКЗИ);
- 20% стоимости средств защиты на работы по их установке и настройке.

ОРИЕНТИРОВОЧНАЯ СТОИМОСТЬ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ БИБЛИОТЕЧНЫХ СИСТЕМАХ

Общая стоимость работ включает:

1. **Стоимость средств защиты информации от 10 500 руб.**
2. **Стоимость работ по установке и настройке средств защиты информации – 20 % от стоимости средств защиты**
3. **Разработка рабочей и проектной документации - от 150 000 рублей**
4. **Аттестация информационной системы по требованиям информационной безопасности (при необходимости) от 30 000 рублей (для 1 АРМ)**

Примерный срок исполнения данных работ – 1 месяц.

ЗАБЛУЖДЕНИЯ И РЕАЛИИ В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИМОННЫХ СИСТЕМАХ

Заблуждение 1. *Разработчики программного обеспечения сделают всё за нас*

Реальность.

Сертификация программного обеспечения автоматизированных библиотечных информационных систем является дорогостоящим и долговременным процессом, в полной мере не выполняющая всех требований действующего законодательства в области защиты персональных данных.

Система защиты информации должна обеспечивает безопасность персональных данных при их обработке на всех программно-технических средствах, входящих в состав информационной системы.

Решение. Разработка подсистемы защиты информации для уже эксплуатируемых библиотечных информационных систем или создание библиотечной информационной системы в защищенном исполнении с последующей аттестацией по требованиям безопасности информации.

ЗАБЛУЖДЕНИЯ И РЕАЛИИ В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИМОННЫХ СИСТЕМАХ

(продолжение)

Заблуждение 2. *Защита персональных данных–это дело системного администратора, IT-специалиста (IT службы), и эта задача может быть ими успешно выполнена самостоятельно.*

Реальность.

Защита персональных данных – это лицензируемый ФСТЭК и ФСБ России вид деятельности, требующий от персонала профессиональных знаний, навыков и умений по разработке и внедрению полноценных и адекватных технических решений. Исходя из практики, сотрудниками Оператора ИСПДн применяются отдельные, известные им мероприятия технического или организационного характера, не решающих проблему защиты персональных данных в комплексе. При создании системы защиты самостоятельно Оператору приходится решать массу вопросов организационно-административного и правового характера, привлекая к данным мероприятиям юридическую, финансовую, кадровую службу, и тд. В итоге все равно к работам привлекаются специализированные организации.

Решение. Привлечение специализированной организации, имеющей соответствующие лицензии и профессиональный штат сотрудников.

ТЕХЦЕНТР
ЗАЩИТА ИНФОРМАЦИИ И ОБЪЕКТОВ

ЗАБЛУЖДЕНИЯ И РЕАЛИИ В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИМОННЫХ СИСТЕМАХ

(продолжение)

Заблуждение 3. *Система защиты персональных данных – это некие программно-технические средства. Нужно их купить и установить. Обследование, классификация, проектирование, тестирование и аттестация – это избыточно, это придумано, чтобы побольше заработать на проблемах оператора.*

Реальность.

Этап обследования предшествует организационно-правовым, физическим и техническим мероприятиям по защите персональных данных. Обследование помогает не только достоверно выявить слабые места информационных систем и разработать замысел защиты, но и, как ни странно, сэкономить деньги. Квалифицированное обследование определяет, как именно можно сократить издержки при построении системы защиты. Способов много: оправданное снижение класса ИСПДн, пересмотр перечня ПДн, подлежащих обработке, сегментирование информационных систем, оптимизация топологии сети и т.п. Все эти способы известны специализированным организациям.

Решение. Привлечение специализированной организации, имеющей соответствующие лицензии и профессиональный штат сотрудников.