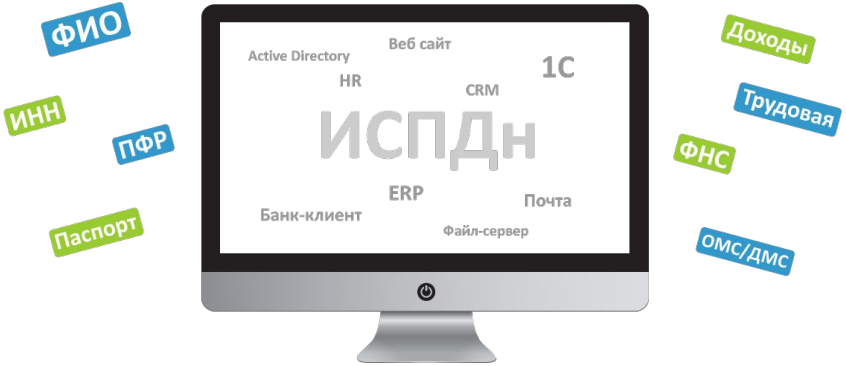
ГАЗИНФОРМСЕРВИС

Проектирование СЗПДн

на примере типовой коммерческой компании



Докладчик: Трофименко Виталий Сергеевич

Самара 2017

Актуальность

Сегодня в РФ (особенно у компаний, которые содержат ИСПДн) существуют 2 понятия информационной безопасности:

- состояние защищенности информационной системы компании **от различного вида угроз безопасности**;
- состояние «защищенности» компании **от возможных санкций**, при невыполнении требований законодательства.

ИСПДн – информационная система персональных данных

Регуляторы

В соответствии с №152-ФЗ, в орбиту процессов, связанных с защитой ПДн, вовлечены **три органа** государственной власти:

РКН

• проверяет организационные и нормативно-правовые аспекты защиты ПДн

ФСБ

• контролирует использование шифровальных средств

ФСТЭК

• контролирует использование технических средств

Законодательство

- ФЗ РФ от 27.07.2006 N 149 ;
- ФЗ РФ от 27.07.2006 N 152 ;
- ФЗ РФ от 27.12.2002 N 184;
- ФЗ РФ от 04.05.2011 N 99;
- ПП РФ от 01.11.2012 N 1119;
- ПП РФ от 15.09.2008 N 687;
- ПП РФ от 21.03.2012 N 211;
- ПП РФ от 3.02.2012 N 79;
- Приказ ФСТЭК РФ от 18.02.2013 N 21;
- Приказ ФСТЭК РФ от 11.02.2013 N 17;
- Приказ ФСБ РФ от 10.07.2014 N 378;
- …

Нужно ли выполнять требования?

Законопроекты № **683952-6, 1131107-6** вносят изменения в ст. 13.11 КоАП РФ. **Штрафы увеличатся, будут суммироваться, штрафы сможет «выписывать» сам РКН**, без участия прокуратуры и суда.

№ части статьи	Правонарушение	Нарушаемая статья	Наказание для юридических лиц
1	Нарушение требований к согласию	Ст.9 ФЗ-152	30 - 50 тысяч рублей
2	Обработка ПДн без согласия	Ст.6 ФЗ-152	15 - 75 тысяч рублей
3	Неопубликование политики в области ПДн	Ст. 18.1 ФЗ 152	15 - 30 тысяч рублей
4	Отказ в предоставлении информации субъекту	Ст.14, Ст.20 ФЗ 152	20 - 40 тысяч рублей
5	Отказ в уничтожении и блокировании ПДн	Ст.21 ФЗ-152	25-45 тысяч рублей
6	Нарушение правил хранения материальных носителей ПДн	ПП-687	25-50 тысяч рублей
7	Нарушение правил обезличивания (ГИС/МИС)	ПП-211 и приказ РКН №996	Не предусмотрено (только для должностных лиц)

Базовые этапы проектирования СЗПДн

- произвести аудит ИС и определить уровни защищенности ПДн, которые обрабатываются в ИСПДн;
- разработать модель угроз (МУ);
- определить базовый состав и содержание мер по обеспечению безопасности ПДн;
- адаптировать базовый состав и содержание мер по обеспечению безопасности ПДн;
- разработать технический проект на СЗПДн;
- внедрить СЗПДн;
- разработать пакет требуемых законодательством организационно-правовых документов (приказы, политики) по защите ПДн (30-50 документов);
- провести оценку соответствия ИСПДн;
- обеспечить защиту ПДн в ходе эксплуатации ИСПДн.

Для типовой коммерческой организации, весь перечень работ может быть выполнен внутренними силами компании!!!

ГАЗИНФОРМСЕРВИС

Уровни защищенности ПДн

	ИСПДн-С (Специальные)	ИСПДн-Б (Биометрические)	ИСПДн-И (Иные)	ИСПДн-О (Общедоступные/Обезличенные)
ПДн сотрудников оператора или ПДн менее чем 100 000 субъектов, не являющихся сотрудникам оператора				
угрозы 3 типа	3	3	4	4
угрозы 2 типа	2	2	3	3
угрозы 1 типа	1	1	1	2
ПДн более чем 100 000 субъектов, не являющихся сотрудникам оператора				
угрозы 3 типа	2	3	3	4
угрозы 2 типа	1	2	2	2
угрозы 1 типа	1	1	1	2

Модель угроз

Модель угроз – это документ, разрабатываемый внутри компании с целью определения актуальных угроз ИСПДн. Грамотно разработанная МУ поможет не только спроектировать СЗПДн высокого уровня защищенности, но и избавить компанию от необходимости выполнять дополнительные «ненужные» требования законодательства.

Технический проект

Технический проект – это совокупность технических документов, которые содержат окончательные проектные решения по системе (по СЗПДн). В данном документе описывают решения, которые планируют внедрить с целью выполнения всех задач, стоящих перед компанией в плане обеспечения защиты ПДн.

Ключевые вопросы

Вопросы

- **Обязательно ли использовать сертифицированные СЗИ** для построения СЗПДн?

Ответы

- Коммерческие компании не обязаны использовать сертифицированные СЗИ (ФЗ 184).
- ГИС/МИС, обязаны использовать СЗИ, прошедшие оценку соответствия в форме сертификации по линии ФСТЭК или ФСБ исходя из требований ФЗ 149 и Приказа ФСТЭК №17.

Ключевые вопросы

Вопросы	Ответы
▪ В каких ситуациях компания обязана использовать **криптографические СЗИ**, работающие с отечественными криптоалгоритмами **ГОСТ**?	▪ Коммерческие организации могут использовать СЗИ, работающие либо с отечественными алгоритмами шифрования ГОСТ, либо с американскими алгоритмами шифрования (AES, 3DES и т.п.). ▪ Использование сертифицированных в ФСБ СКЗИ обязательно для ГИС и МИС, при актуальности соответствующих угроз исходя из требований ФЗ 149 и Приказа ФСТЭК №17. Все сертифицированные в ФСБ СКЗИ используют отечественный криптоалгоритм ГОСТ.

Ключевые вопросы

Вопросы

- Должна ли коммерческая компания получать **лицензию на техническую защиту конфиденциальной информации (ТЗКИ)?**

Ответы

- Если компания обрабатывает ПДн исключительно для собственных нужд, то она не обязана получать лицензию на ТЗКИ.
- Если компания оказывает услуги по защите ПДн (или по ТЗКИ), либо деятельность по защите ПДн прописана в учредительных документах компании, то лицензия обязательна.

Ключевые вопросы

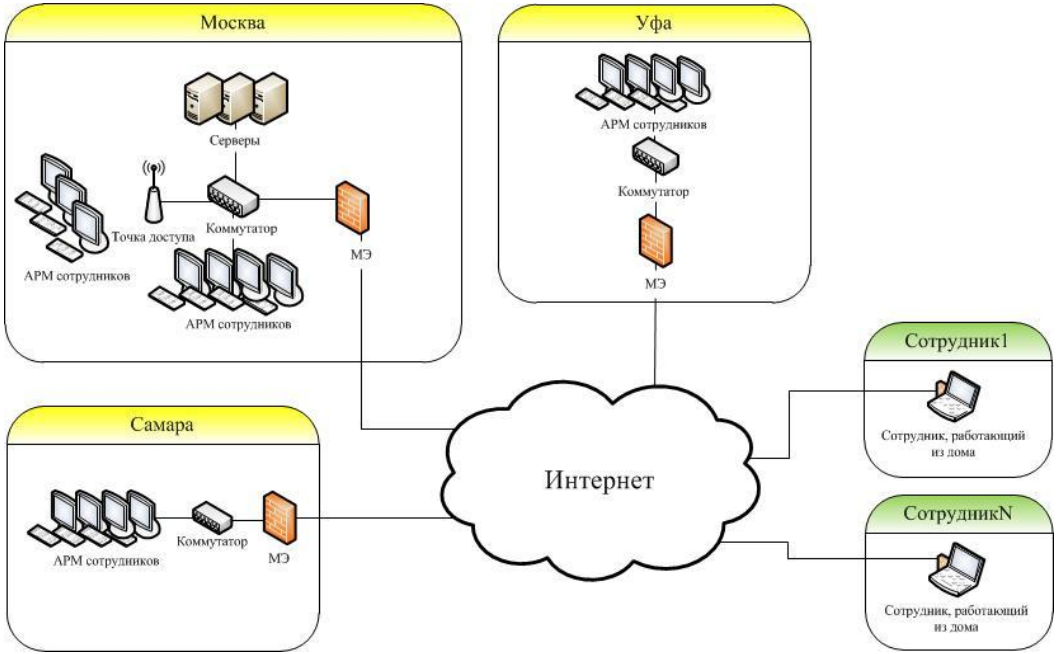
Вопросы

- Нужно ли проводить аттестацию ИСПДн с помощью лицензиата ФСТЭК или **можно оценить соответствие ИСПДн самостоятельно?**

Ответы

- **Аттестация ИСПДн не обязательна для коммерческих компаний.** В законодательстве нет требований по обязательной аттестации ИС коммерческих предприятий.
- Исходя из требований Приказа ФСТЭК №17 **аттестация ИС (включая ИСПДн) в ГИС/МИС обязательна**.

Разбор


Москва
Серверы
Точка доступа
Коммутатор
МЭ
АРМ сотрудников
АРМ сотрудников
Уфа
АРМ сотрудников
Коммутатор
МЭ
Сотрудник1
Сотрудник, работающий из дома
Самара
Коммутатор
МЭ
АРМ сотрудников
Интернет
СотрудникN
Сотрудник, работающий из дома

ГАЗИНФОРМСЕРВИС

Разбор

Вопросы	Ответы
Какой уровень защищенности?	УЗ-4
Обязательно ли использовать сертифицированные СЗИ?	Нет
Обязательно ли использовать криптографические СЗИ?	Да
Должны ли криптографические СЗИ использовать ГОСТ?	Нет
Нужна ли лицензия по ТЗКИ?	Нет
Обязательно ли аттестовать ИСПДн?	Нет

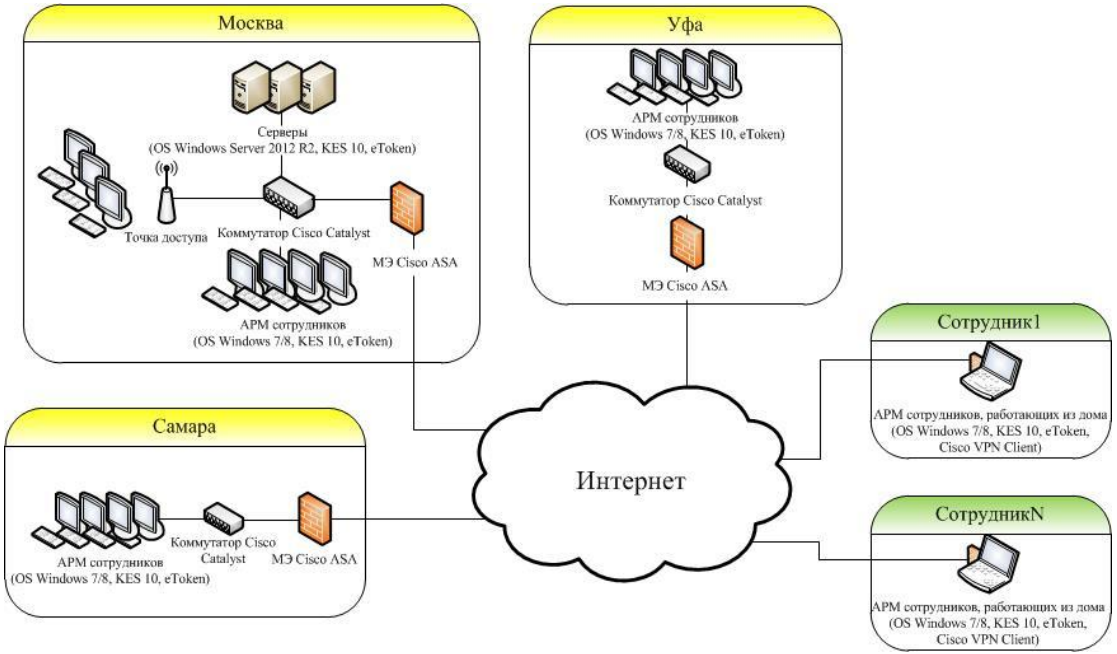
ГАЗИНФОРМСЕРВИС

Базовый набор мер защиты

Технические меры	Организационные меры	Не актуально
идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);	защита технических средств (ЗТС)	ограничение программной среды (ОПС);
управление доступом субъектов доступа к объектам доступа (УПД);		защита машинных носителей информации (ЗНИ);
регистрация событий безопасности (РСБ);		обнаружение вторжений (СОВ);
антивирусная защита (АВЗ);		обеспечение целостности информационной системы и информации (ОЦЛ);
контроль (анализ) защищенности информации (АНЗ);		обеспечение доступности информации (ОДТ);
защита среды виртуализации (ЗСВ);		выявление инцидентов и реагирование на них (ИНЦ);
защита информационной системы, ее средств, систем связи и передачи данных (ЗИС);		управление конфигурацией информационной системы и системы защиты персональных данных (УКФ).

ГАЗИНФОРМСЕРВИС

Схема функциональной структуры



ГАЗИНФОРМСЕРВИС

Выводы

- для выполнения требований законодательства в области защиты ПДн можно обойтись внутренними силами компании;
- для выполнения требований нужны квалифицированные кадры;
- использование сертифицированных СЗИ не обязательно для коммерческих компаний;
- лицензия на ТЗКИ не требуется для защиты «своей» ИСПДн;
- для обеспечения конфиденциальности ПДн в коммерческих компаниях можно использовать СЗИ, работающие на различных алгоритмах шифрования (не только ГОСТ);
- для подтверждения соответствия ИСПДн требованиям законодательства не обязательно проводить аттестацию (можно произвести оценку соответствия самостоятельно);
- выполнение требований законодательства можно делегировать лицензиату ФСТЭК;
- в случае проведения аттестации системы, у контролирующих органов возникнет меньше вопросов к оператору ПДн (меньшее количество проверок), так как система уже была проверена лицензиатом ФСТЭК;
- необходимо следить за изменениями законодательства и оперативно на них реагировать.