



Защита персональных данных: что и как

В.В.Разувайкин

Директор по развитию направления
НИП «ИНФОРМЗАЩИТА»

ОСНОВНЫЕ ПРИВОДНЫЕ СИЛЫ РЫНКА

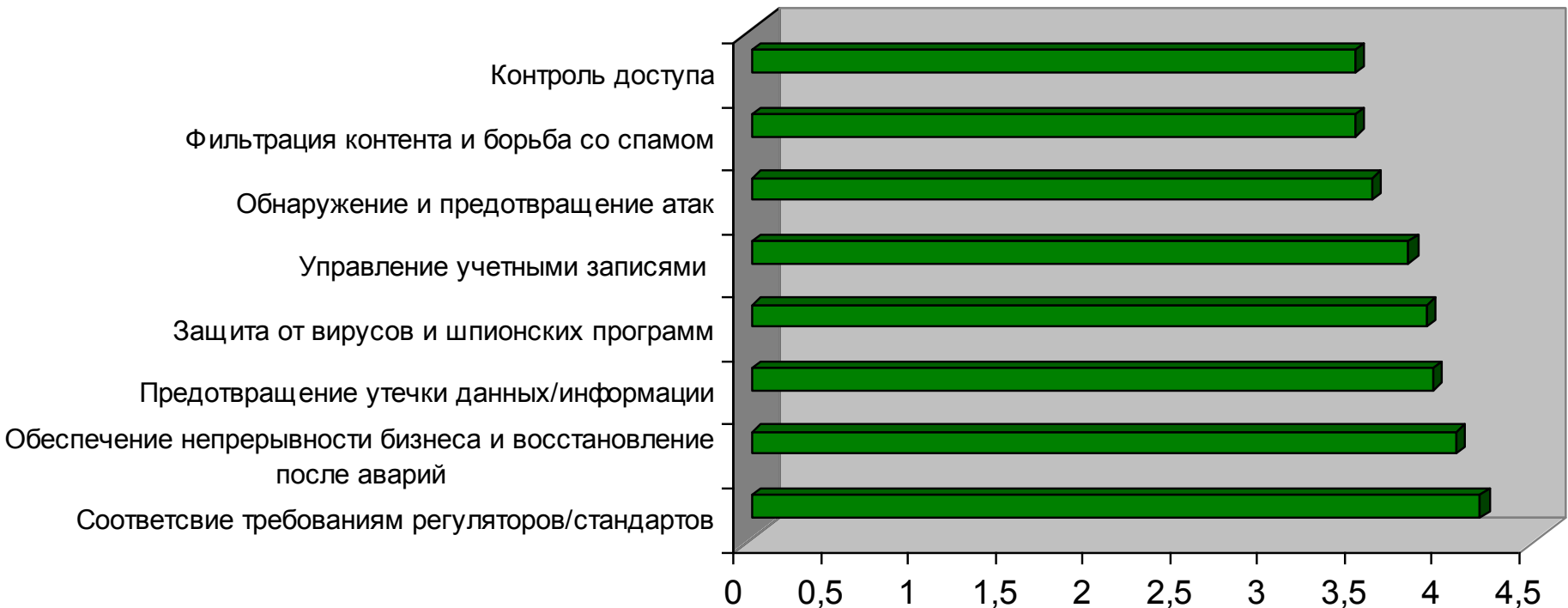
**Какие три фактора оказывают наибольшее влияние
на практику информационной безопасности вашего
предприятия**



*Источник: 10-е ежегодное международное исследование в области
информационной безопасности компании «Эрнст энд Янг»*

ОСНОВНЫЕ ПРОБЛЕМЫ УЧАСТНИКОВ РЫНКА

Пожалуйста проранжируйте, какие проблемы ИБ для вас наиболее критичны (1 - не важны, 5 - очень важны)



*Источник: Результаты анкетирования участников Forester's Security Forum
EMEA 2007*



Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персданных *обязан* принимать необходимые *организационные* и *технические меры*, в том числе использовать шифровальные (криптографические) средства, для защиты персданных от *неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персданных, а также от иных неправомерных действий.*



Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты

7) *защита персданных* работника от неправомерного их использования или утраты *должна быть обеспечена работодателем за счет его средств* в порядке, установленном настоящим Кодексом и иными федеральными законами;

РЕШЕНИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Персона: Пушкин Александр Сергеевич

Информация События Семья Документы Источники

Фамилия: Пушкин
Имя: Александр
Отчество: Сергеевич

Дата рождения: 26.05.1799 ст
Дата смерти: 29.01.1837 ст

Комментарий: Родоначальник новой русской литературы, основоположник русского литературного языка.

Фаворит: ☒
Пол: Мужской

Дополнительные поля
Основное занятие: Великий поэт

Место жительства: Нет данных. Щёлкните, чтобы выбрать...

Создано: 09.01.2006, изменено: 23.08.2006

OK Отмена

✓ технически сложные

✓ требуют:

- высокой квалификации исполнителей
- специальных знаний
- глубокого понимания функциональности:

- приложений, обрабатывающих персональные данные
- средств защиты информации, необходимых для нейтрализации актуальных угроз персональным данным

Персона №1, мужчина

Фамилия: Пушкин
Имя: Александр
Отчество: Сергеевич

Дата рождения: 26.05.1799
Дата смерти: 29.01.1837

Комментарий: Родоначальник новой русской литературы, основоположник русского литературного языка.

Фаворит: ☒
Пол: Мужской

Дополнительные поля
Основное занятие: Великий поэт

Дата	Событие	Место	Комментарий
26.05.1799	Родился	Москва	
18.02.1831	Женился	Церковь Большого Вознесения	
19.05.1832	Родилась Мария	Петербург	
06.07.1833	Родился Александр	Петербург	
14.05.1835	Родился Григорий	Петербург	

Роль	Участник
Мать	Пушкина (Ганнибал) Надежда Осиповна
Отец	Пушкин Сергей Львович

OK Отмена

ШАГ 1: ИНВЕНТАРИЗАЦИЯ РЕСУРСОВ



Проанализировать все эксплуатируемые информационные системы и традиционные хранилища данных, выявить все, где присутствуют и обрабатываются персданные.

ШАГ 2: СОГЛАСИЕ СУБЪЕКТОВ НА ОБРАБОТКУ



Оценить наличие предусмотренных законом оснований для обработки персональных данных, в случаях, когда они отсутствуют – получить согласие субъекта.

Отдельный вопрос – передача персональных данных

ШАГ 3: ПЕРЕСМОТР ДОГОВОРОВ С СУБЪЕКТАМИ



Пересмотреть договора с работниками и клиентами в части обработки персональных данных и, особенно, их распространения (передачи)

ШАГ 4: СФОРМИРОВАТЬ ПЕРЕЧЕНЬ ПЕРСДАННЫХ



ФЗ «О персональных данных»

Статья 9. Письменное согласие субъекта персданных на обработку своих персональных данных должно включать в себя ...*перечень персональных данных*, на обработку которых дается согласие субъекта

Статья 14. Субъект персданных имеет право на получение ... информации, касающейся обработки его персданных, в том числе содержащей ... *перечень обрабатываемых персданных* и источник их получения



ШАГ 5: УСТАНОВИТЬ СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Определить и зафиксировать документально предельные сроки хранения персональных данных после расторжения (прекращения) договора с работником, клиентом, абонентом (физическими лицами), исходя из сроков:

✓ требований законодательства:

- гражданского
- трудового
- пенсионного
- о безопасности и правоохранительной деятельности

...

✓ исковой давности взаимных претензий банка и клиента

Перечень
персональных данных, обрабатываемых
в ООО «Коммерческое»

№№ пп	Основания для обработки	Содержание сведений	Срок хранения, условия прекращения обработки
1	Глава 14 Трудового кодекса	Фамилия, имя, отчество Дата и место рождения Гражданство ИНН Номер свидетельства государственного пенсионного страхования ... Др. сведения унифицированной формы № Т-2	75 лет

Перечень
персональных данных, обрабатываемых
в ООО «Коммерческое»

№№ пп	Основания для обработки	Содержание сведений	Срок хранения, условия прекращения обработки
2	Письменное согласие клиента	Фамилия, имя, отчество Адрес места жительства Дата рождения Номер телефона Адрес электронной почты	До окончания действия программы лояльности или отзыва согласия клиента

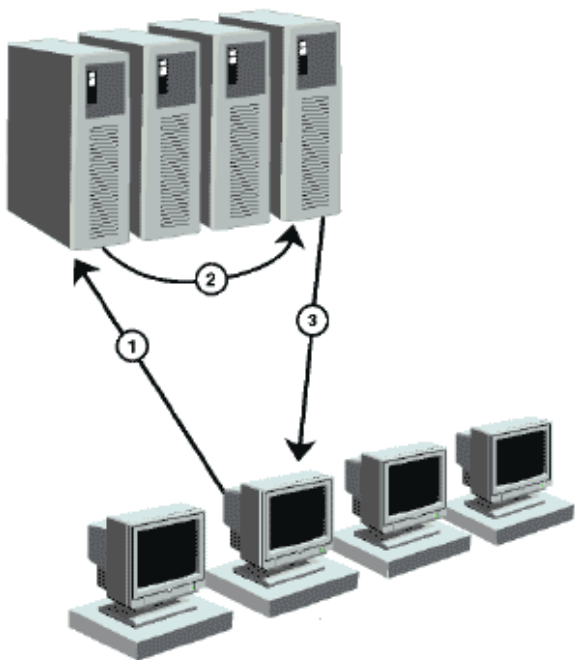
ШАГ 6: ОГРАНИЧИТЬ ДОСТУП РАБОТНИКОВ К ПЕРСДАНЫМ



Положение об обеспечении безопасности персональных данных при их обработке в ИСПДн

12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя ... *учет лиц, допущенных к работе с персональными данными* в информационной системе

14. Лица, доступ которых к персданным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, *допускаются к соответствующим персданным на основании списка, утвержденного оператором* или уполномоченным лицом.



ШАГ 7: ДОКУМЕНТАЛЬНО РЕГЛАМЕНТИРОВАТЬ РАБОТУ С ПЕРСДААННЫМИ



Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты

8) *работники* и их представители *должны быть ознакомлены под роспись с документами* работодателя, *устанавливающими порядок обработки персональных данных* работников, а также об их правах и обязанностях в этой области

ШАГ 8: СФОРМИРОВАТЬ МОДЕЛЬ УГРОЗ ПЕРСОНАЛЬНЫМ ДАННЫМ



Положение об обеспечении безопасности персональных данных при их обработке в ИСПДн

12. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИС включают в себя:

а) *определение угроз безопасности персональных данных* при их обработке, формирование на их основе модели угроз

15.02.2008 г. Заместителем директора ФСТЭК России утверждены:

Базовая модель угроз безопасности ПД при их обработке в ИСПД

Методика определения актуальных угроз безопасности ПД при их обработке в ИСПД

ШАГ 9: КЛАССИФИЦИРОВАТЬ ИСПДн

Приказ ФСТЭК/ФСБ/Мининформсвязи от 13.02 2008 № 55/86/20 «Об утверждении порядка проведения классификации ИСПДн»

- Классификация ИСПДн проводится госорганами, ..., юридическими и физическими *лицами, организующими и осуществляющими обработку ПДн*, а также определяющими цели и содержание такой обработки
- Определяются следующие категории обрабатываемых в информационной системе персональных данных ($X_{пд}$):
 - категория 2 – ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию;
- Коэффициент $X_{пдн}$ может принимать следующие значения:
 - 1 – в ИСПДн одновременно обрабатываются ПДн более чем 100 000 субъектов ПДн....;
 - 2 – в ИСПДн одновременно обрабатываются ПДн от 1 000 до 100 000 субъектов ПДн;

ШАГ 9: КЛАССИФИЦИРОВАТЬ ИСПДн

Приказ ФСТЭК/ФСБ/Мининформсвязи от 13.02 2008 № 55/86/20
«Об утверждении порядка проведения классификации ИСПДн»

15. Класс типовой информационной системы определяется в соответствии с таблицей.

$X_{пд}$ $X_{пдн}$	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Приказ ФСТЭК/ФСБ/Мининформсвязи
от 13.02 2008 № 55/86/20

«Об утверждении порядка проведения
классификации ИС персональных
данных»

1. Классификация - задача
неформальная
2. На этапе сбора и анализ исходных
данных по ИСПДн:
 - ✓ Определение целей обработки
ПДн
 - ✓ Формирование перечня ПДн
(состав сведений, отнесенных к
такой категории)
3. Оценка необходимости и
целесообразности отнесения ИСПДн к
специальным



Проблемы классификации

- ✓ Следование духу, а не формальной букве закона
- ✓ Разумный выбор параметров определяющих класс ИСПДн:
 - количество субъектов Vs локальность обработки
 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию
- ✓ Отсутствие формальных (законодательно определенных) определений таких понятий, как:
 - «состояние здоровья»,
 - «принятие решений, порождающих юридические последствия в отношении субъекта персональных данных»



ШАГ 10: СОСТАВИТЬ И НАПРАВИТЬ В УПОЛНОМОЧЕННЫЙ ОРГАН УВЕДОМЛЕНИЕ

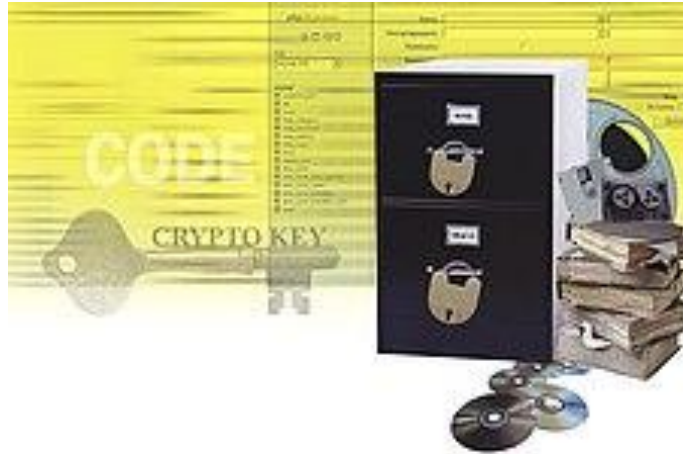
Персданные, обрабатываемые без уведомления

- 1) относящиеся к субъектам персданных, которых связывают с оператором *трудовые отношения*
- 2) полученные оператором *в связи с заключением договора*, стороной которого является субъект персданных, если персональные данные *не распространяются*, а также *не предоставляются третьим лицам без согласия субъекта* персональных данных и используются оператором *исключительно для исполнения* указанного *договора и заключения договоров* с субъектом

Представление персданных в случаях, предусмотренных законами РФ

Обработка персданных работников клиентов и контрагентов юридических лиц (банковская карточка)

ПРИВЕСТИ СИСТЕМУ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ РЕГУЛЯТОРОВ



ФЗ «О персональных данных»

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных *обязан* принимать необходимые *организационные и технические меры*, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от *неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.*

ПРИВЕСТИ СИСТЕМУ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ РЕГУЛЯТОРОВ

**15.02.2008 г. Заместителем директора ФСТЭК России
утверждены:**

Рекомендации по обеспечению безопасности ПД при их обработке
в ИСПД

Основные мероприятия по организации и техническому
обеспечению безопасности ПД, обрабатываемых в ИСПД

Базовая модель угроз безопасности ПД при их обработке в ИСПД

Методика определения актуальных угроз безопасности ПД при их
обработке в ИСПД

ШАГ 11: РАЗРАБОТАТЬ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДн

Модель угроз ПДн

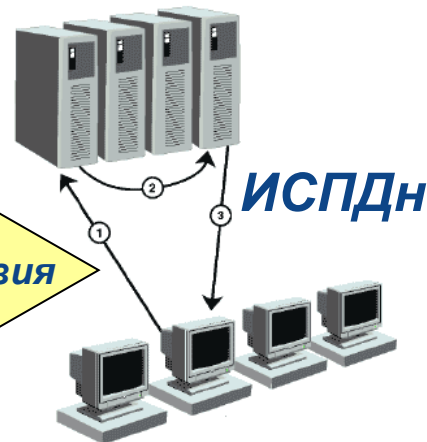
«Основные мероприятия по организации и техническому обеспечению безопасности ПД, обрабатываемых в ИСПДн», утвержденные ФСТЭК России

Угрозы

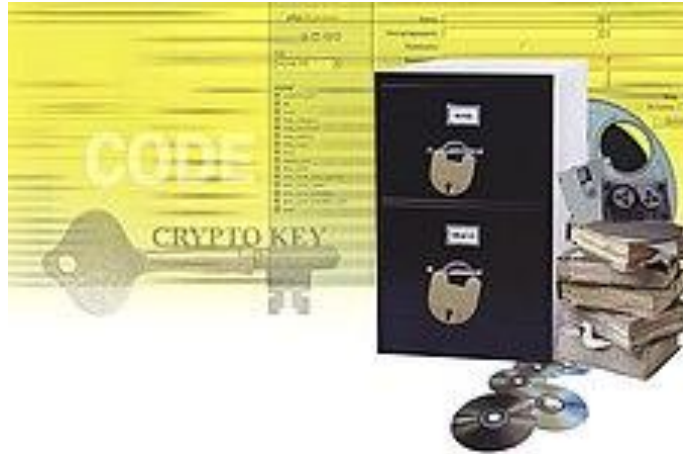
Требования по защите персональных данных в ИСПДн

Требования

Оценка соответствия



ШАГ 12: РАЗРАБОТАТЬ И ВНЕДРИТЬ ТЕХНИЧЕСКИЕ РЕШЕНИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

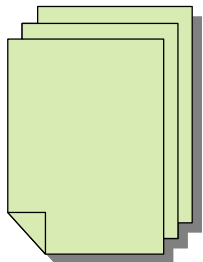


«Рекомендации по обеспечению безопасности ПД при их обработке в ИСПД» ФСТЭК России, от 15.02.2008 г.

Мероприятия по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий, включают:

- Управление доступом
- Регистрацию и учет
- Обеспечение целостности
- Контроль отсутствия недекларированных возможностей
- Антивирусную защиту
- Обеспечение безопасного межсетевого взаимодействия ИСПДн
- Анализ защищенности
- Обнаружение вторжений

ШАГ 13: РАЗРАБОТАТЬ ДОКУМЕНТАЦИЮ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДн



«Рекомендации по обеспечению безопасности ПД при их обработке в ИСПД», утверждены 15.02.2008 г. Заместителем директора ФСТЭК России.

При подготовке документации по вопросам обеспечения безопасности ПДн при их обработке в ИСПДн и эксплуатации СЗПДн в обязательном порядке разрабатываются:

- ✓ положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн;
- ✓ требования по обеспечению безопасности ПДн при обработке в ИСПДн;
- ✓ должностные инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;
- ✓ рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

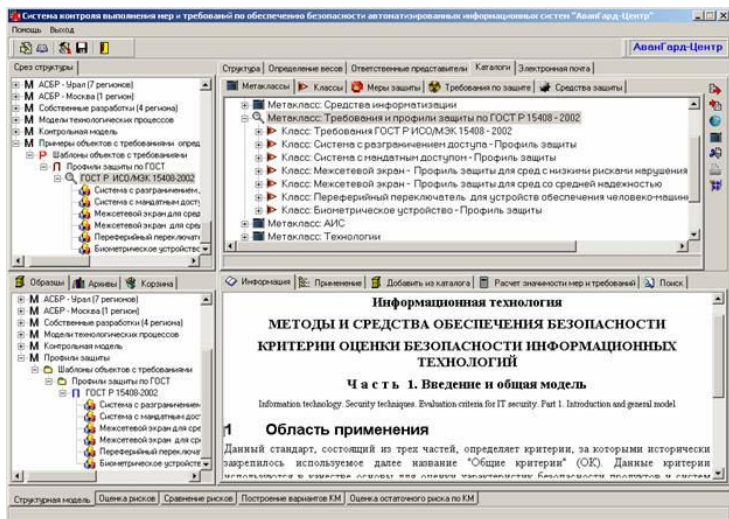
ШАГ 14: ПОЛУЧИТЬ ЛИЦЕНЗИЮ НА ТЕХНИЧЕСКУЮ ЗАЩИТУ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ



Основные мероприятия по организации и техническому обеспечению безопасности ПД, обрабатываемых в ИСПД

Операторы ИСПДн при проведении мероприятий по обеспечению безопасности ПДн (конфиденциальная информация) при их обработке в ИСПДн *1 и 2 классов и распределенных ИС 3 класса должны получить лицензию* на осуществление деятельности по технической защите конфиденциальной информации

ШАГ 15: СОЗДАТЬ ПОДСИСТЕМУ ИБ ИСПДн И АТТЕСТОВАТЬ (СЕРТИФИЦИРОВАТЬ) ЕЕ



Основные мероприятия по организации и техническому обеспечению безопасности ПД, обрабатываемых в ИСПД

Оценка соответствия ИСПДн по требованиям безопасности ПДн производится:

Для ИСПДн 1 и 2 классов – **обязательная сертификация (аттестация)** по требованиям безопасности информации

ШАГ 16: ОРГАНИЗОВАТЬ ЭКСПЛУАТАЦИЮ ИСПДн И КОНТРОЛЬ ЗА БЕЗОПАСНОСТЬЮ



Положение об обеспечении безопасности персональных данных при их обработке в ИСПДн

12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

з) контроль за соблюдением условий использования СЗИ, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн...



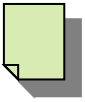
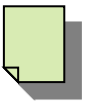
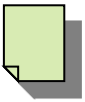
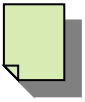
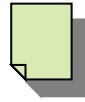
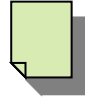
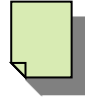
ВОПРОСЫ?

Василий Разувайкин

☎ (495) 980-2345

✉ vasraz@infosec.ru,
vasraz@gmail.com

УСЛУГИ ЗАО НИП «ИНФОРМЗАЩИТА» ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

- | | | | |
|----|---|---|----------------------------------|
| 1. | Выявление и обследование ИСПДн; |  | Отчет об
обследовании |
| 2. | Предварительная
классификация; |  | Акты
классификации |
| 3. | Разработка моделей угроз; |  | Модели угроз |
| 4. | Разработка требований по
защите, и оценка соответствия
требованиям регуляторов; |  | Требования по
защите |
| 5. | Разработка и внедрение
технических решений по защите; |  | Технические
проекты |
| 6. | Разработка необходимых
нормативных документов; |  | Нормативные
документы |
| 7. | Аттестация ИСПДн 1 и 2 класса
по требованиям безопасности
информации |  | Аттестат
соответствия |

Состав работ

Для достижения целей создания СЗИ ИСПД, работы проводятся в несколько этапов:

- ✓ Предпроектное обследование информационных систем Заказчика с целью:
 - ✓ выявления и уточнения фактов обработки персональных данных в этих системах, целей обработки, мест и путей ввода персональных данных, их прохождения, хранения и уничтожения, а также передачи третьим лицам в рамках существующих бизнес процессов.
 - ✓ выявления сегментов информационных систем персональных данных (далее – информационные системы), обеспечивающих функционирование бизнес процессов Заказчика.
 - ✓ определения границ сегментов информационных систем, выявления мест и форматов хранения персональных данных, а также изучения существующего порядка обработки и защиты персональных данных в этих сегментах информационных систем.
 - ✓ классификации информационных систем персональных данных.
- ✓ Разработка рекомендаций по выполнению требований законодательства РФ по защите персональных данных.
- ✓ Разработка и внедрение порядка обработки персональных данных в соответствии с требованиями законодательства РФ.
- ✓ Разработка рекомендаций по обеспечению технической защиты персональных данных, включая разработку актуализированных моделей угроз для специальных ИСПДн и определение перечня требований по технической защите ИСПДн.
- ✓ Разработка технического задания на подсистему защиты персональных данных в ИСПДн.
- ✓ Проектирование и внедрение технических средств защиты персональных данных.
- ✓ Аттестационные испытания ИСПДн Заказчика и подготовка Заказчика к выполнению лицензионных требований и условий, определенных постановлением Правительства Российской Федерации от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».