

Киберпреступность в России. Защита персональных данных.

Заместитель генерального директора по
информационной безопасности

Артём Агеев

Киберпреступность

Объём рынка киберпреступности в мире (Group IB) – 7 млрд. дол.
Из них «российский сегмент» - 1,3 млрд.; «русский» – 2,5 млрд.

Из 10 крупнейших спаммеров (www.spamhaus.org):
- 3 россиянина; 3 украинца; эстонец.

Рост киберпреступности – 115% за 2010 год
(Гос. Деп. США)

Основные направления

Дистанционное банковское обслуживание (ДБО, банк-клиент).

СМС - мошенничество

Социальные сети

DDOS атаки. Шантаж и вымогательство.

Спам. Ботнеты. Нелегальные медикаменты и ПО.

Кибервойна (Stuxnet)

«Бизнес» процесс



1. Специализация.

2. Упрощение процедур.

3. Эффективность.

ГОС. РЕГУЛИРОВАНИЕ

1. Не знает о виртуальных серверах, облачных вычислениях, терминалах ...

2. Активно ловит западных шпионов (ПЭМИН)

3. Плодит регуляторов (ФСТЭК, ФСБ, РОСКОМНАДЗОР, МИНСВЯЗИ и т.д.)

4. Любит ГОСТ, сертификацию, аттестацию и лицензирование

ВЫВОД: Отстаёт на 5-10 лет

Защищаемая информация

ГОСТАЙНА

ФЗ N 5485-1 "О государственной тайне"

Конфиденциальная информация (КИ)

Коммерческая тайна
ФЗ N 98-ФЗ «О коммерческой тайне»

Банковская тайна
ФЗ N 395-1 «О банках и банковской деятельности»

Персональные данные
ФЗ N 152-ФЗ «О персональных данных»

Служебная тайна
Указ Президента РФ N 188
«Об утверждении перечня сведений конфиденциального характера»

Сведения, которые не могут быть отнесены к ГОСТАЙНЕ и КИ

Информация о деятельности государственных органов и органом местного самоуправления
ФЗ N 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Нормативно-правовые документы

Федеральные
Законы

152-ФЗ
«О ПДн»

Постановления
Правительства

ПП687
ПДн без средств
автоматизации

ПП781
ИСПДн

ПП512
БиоПДн

Приказы
Федеральных
Служб

ФСТЭК ФСБ Минсвязи
55/86/20
Классификация ИСПДн

Письмо
«шести»

ФСТЭК
58
ИБ ПДн

ФСБ
Криптография

РКН
Регламент
проверок

Комплекс
БР ИББС

ФСТЭК
МУ

ФСБ
Регламент
проверок

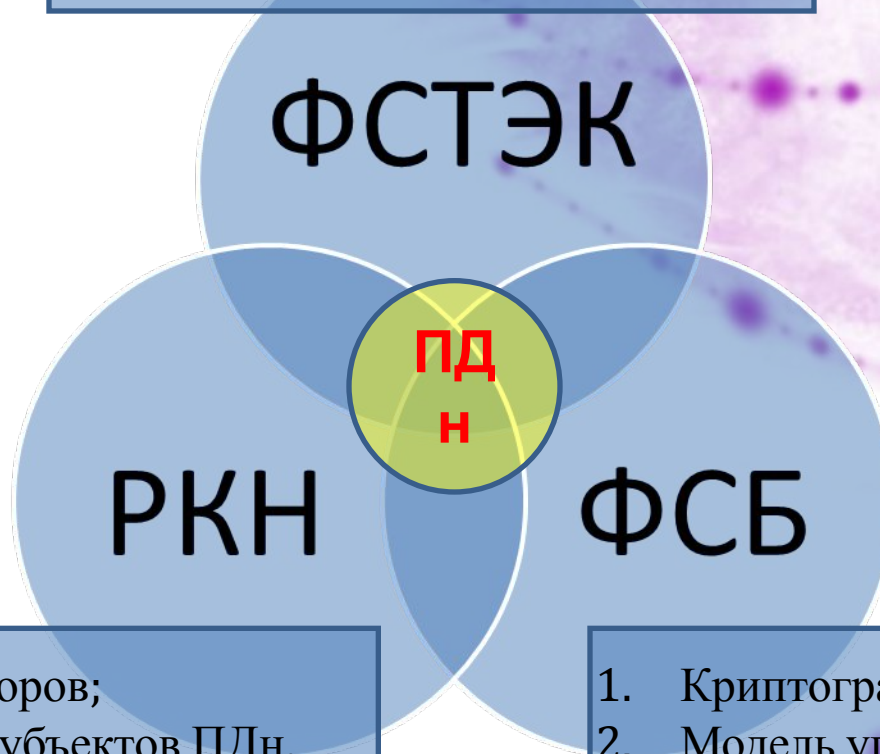
СТО БР
ИББС-1.x

ФСТЭК
ЮФО

Методические
рекомендации

РС БР
ИББС-2.x

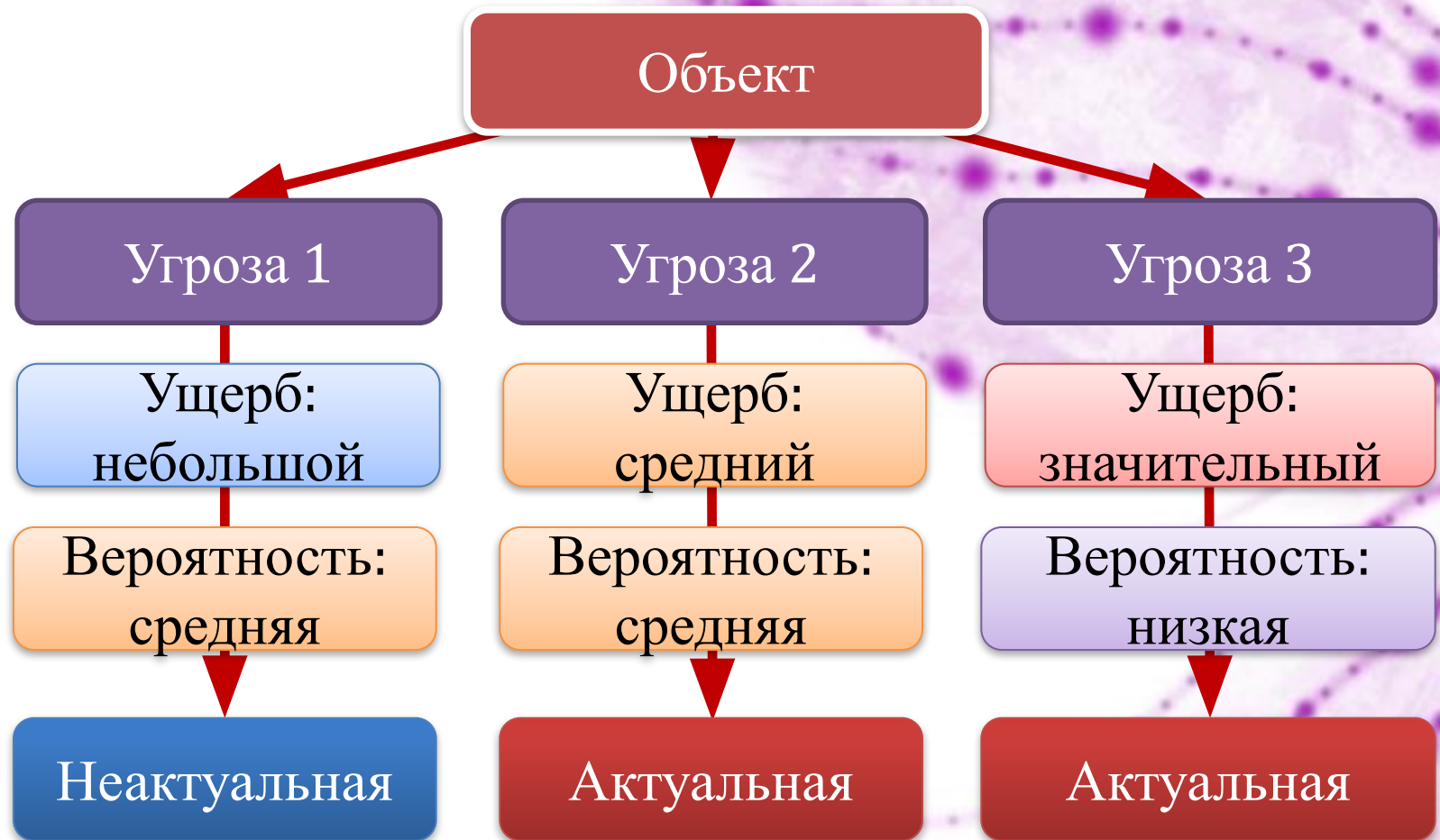
1. Технические вопросы;
2. Аттестация, Сертификация;
3. Модель угроз ФСТЭК.



1. Реестр операторов;
2. Защита прав субъектов ПДн.

1. Криптография;
2. Модель угроз ФСБ.

Модель угроз










Что такое ИСПДн?

152-ФЗ «О персональных данных»

информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в **базе данных**, а также информационных технологий и технических средств, позволяющих осуществлять **обработку** таких персональных данных с использованием средств автоматизации или без использования таких средств;

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.

Классификация ИСПДн

	 < 1 000	 1 000 < X < 100 000	 > 100 000
 4 кат.	К4	К4	К4
 1337 5047 3 кат.	К3	К3	К2
 2 кат.	К3	К2	К1
 1 кат.	К1	К1	К1

Согласия на обработку

Часть
согласи

СОГЛАСИЕ СУБЪЕКТА ПДн

с

Часть
расовой
убежде

СОГЛАСИЕ на обработку
СПЕЦИАЛЬНЫХ категорий ПДн

ся
их

Часть 1
основе
обраба
данных,

СОГЛАСИЕ на обработку
БИОМЕТРИЧЕСКИХ ПДн

на
т
их

Часть 1
субъект
рожден
предост

СОГЛАСИЕ на публикацию
ПДн в общедоступных источниках

ия
по
е,

Часть 3
государ
осущес
1) налич

СОГЛАСИЕ на трансграничную передачу ПДн

их
т

Часть 3
данных
субъект

СОГЛАСИЕ на передачу ПДн третьим лицам

их
ль

Часть
исключ
согласи

СОГЛАСИЕ на автоматизированную обработку с
принятием юридически значимого решения

и
и

152-ФЗ и Интернет



Часть 4 статьи 9: Согласие субъекта должно включать собственноручную подпись, либо ЭЦП.

Часть 1 статьи 7: Обеспечение конфиденциальности передаваемых данных.



Часть 1 статьи 5: Принцип достоверности при обработке ПДн

Часть 1 статьи 8: **согласие** на публикацию в общедоступных источниках.

Часть 2 статьи 7: не требуется обеспечивать **конфиденциальность** общедоступных данных.

Часть 2 статьи 22: **уведомление** не требуется, если обрабатываются общедоступные ПДн.

Мифы о защите ПДн

ОТКАЗ ОТ ЗАЩИТЫ

Статья 23 Конституции РФ:

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну...

Статья 86 ТК РФ:

9) работники не должны отказываться от своих прав на сохранение и защиту тайны.

ОБЕЗЛИЧИВАНИЕ

Адрес, телефон, e-mail практически однозначно определяют человека.

СНИЖЕНИЕ КЛАССА

K2=K3

ОБЪЕДИНЕНИЕ ИСПДн

Ст. 5 152-ФЗ. Принципы обработки ПДн:

5) недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

НЕСЕРТИФИЦИРОВАННЫЕ СЗИ

Статья 13.12 КоАП:

Использование несертифицированных средств защиты информации ...

Штраф до 20 тыс. руб. и конфискация СЗИ.

Сертификация средств защиты

Кем?

ФСТЭК



ФСБ



Что?

Экземпляр

Партия

Серия
(производство)

Срок действия
сертификата?

Как?

МЭ

СВТ

ОУД

ТУ

КС1(2,3)

НДВ

МЭ

АВ

СОК
А

КЛАСС АС

КЛАСС ИСПДН

ВЕРСИ
Я

ОБНОВЛЕНИЯ

КОМПЛЕКТ ПОСТАВКИ

ПЕРЕСЕРТИФИКАЦИ
Я

Нарушения и наказания

Федеральный Закон 152-ФЗ «О персональных данных»

Часть 3 статьи 22:

Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации. Уведомление должно содержать следующие сведения:

Пример: изменились реквизиты организации, а уведомление не обновили.

КоАП, ст. 19.7:

Непредставление или несвоевременное представление в государственный орган сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом его законной деятельности, а равно представление в государственный орган таких сведений в неполном объёме или в искажённом виде ..

Прокуратура. Предупреждение или штраф.



Часть 1 статьи 6:

Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

Пример: сбор сведений о близких родственниках, супругах, хранение сведений об уволенных сотрудниках (кроме бухгалтерской отчетности) без согласий.

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.



Часть 4 статьи 6:

В случае, если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Пример: охрана периметра другой организацией, корпоративный спортзал, негосударственный пенсионный фонд, «зарплатный» банк. В договорах с ними отсутствует обязательное условие обеспечения конфиденциальности.

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.



Часть 3 статьи 9:

В случае обработки общедоступных персональных данных, обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.

Пример: публикация ПДн на сайте, в телефонном справочнике.

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.



Часть 1 статьи 10:

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи (имеется письменное согласие).

Пример: графа «национальность» в анкете, сбор сведений о здоровье.

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.



Часть 3 статьи 10:

Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Пример: графа «судимость» в анкете

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.

Часть 1 статьи 11:

Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

Пример: Фотография сотрудника (на пропуске, в личном деле, в справочнике Outlook; рост, вес).

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.



Часть 3 статьи 18:

Если персональные данные были получены не от субъекта персональных данных, оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных информацию о наименовании, адресе, целях обработки, пользователях, правах субъекта персональных данных

Пример: УК провела конкурс на «лучшего клиента», получив от филиала информацию о клиентах.

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.



Часть 4 статьи 21:

В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных, уничтожить соответствующие персональные данные и уведомить об этом субъекта персональных данных.

Пример: -

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.



Часть 1 статьи 5:

*Обработка персональных данных должна осуществляться на основе принципов:
... недопустимости обработки персональных данных, избыточных по отношению
к целям, заявленным при сборе персональных данных;*

Пример: -



Постановления Правительства РФ № 687 (неавтоматизированная обработка ПДн)

Пункт 6:

Лица, осуществляющие обработку персональных данных, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

Пункт 8:

Устанавливает особенности ведения журналов учёта посетителей.

Пункт 13:

Обработка персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Пункт 15:

При хранении материальных носителей должны соблюдаться условия обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ.

2



Наши лицензии

ФСТЭК



ФСБ



Спасибо за внимание!
Вопросы?



(861) 279-32-00
info@rosint.net