



## Защита персональных данных: алгоритм для законопослушных банков

**М.Ю.Емельяников**

*Заместитель коммерческого директора  
НИП «ИНФОРМЗАЩИТА»*

# 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 ПЕРСДААННЫХ



## ФЗ «О персональных данных»

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

Статья 14. Субъект персональных данных имеет право на получение ... информации, касающейся обработки его персональных данных, в том числе содержащей ... *перечень обрабатываемых персональных данных* 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

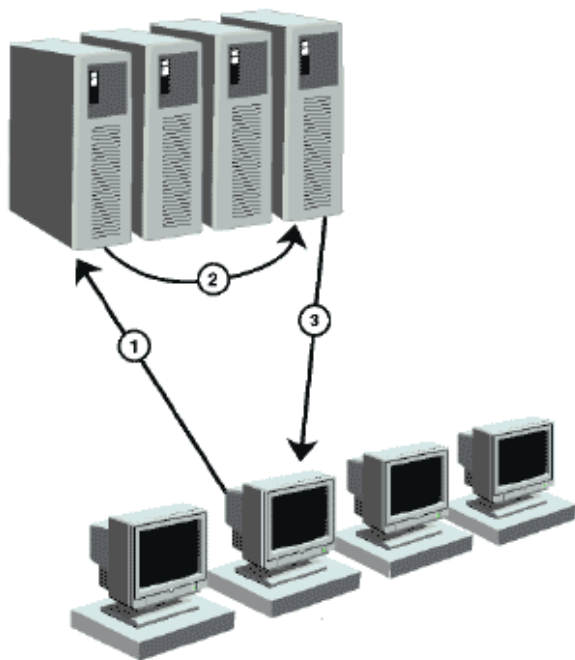
# ШАГ 6: ОГРАНИЧИТЬ ДОСТУП РАБОТНИКОВ БАНКА К ПЕРСДАНЫМ



## 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 ПЕРСОНАЛЬНЫМИ



**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 ХПДН 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 10: СОСТАВИТЬ И НАПРАВИТЬ В УПОЛНОМОЧЕННЫЙ ОРГАН УВЕДОМЛЕНИЕ

*Директору на рассмотрение  
1 000/005 09  
Трудовой инспекции  
Э.С. Виткина*



**ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ МАССОВЫХ  
КОММУНИКАЦИЙ, СВЯЗИ И ОХРАНЫ КУЛЬТУРНОГО НАСЛЕДИЯ  
(РОССВЯЗЬОХРАНКУЛЬТУРА)**

## ПРИКАЗ

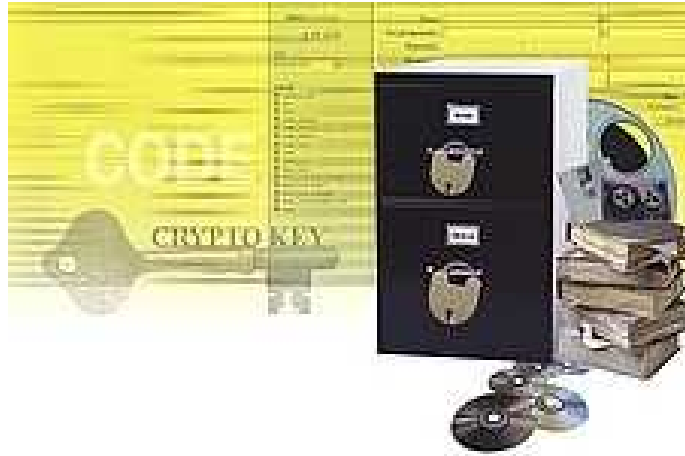
«28» марта 2008 г.

Москва

№ 153

**Об утверждении формы уведомления об обработке  
персональных данных**

# ШАГ 11: ПРИВЕСТИ СИСТЕМУ ЗАЩИТЫ ПЕРСДАННЫХ 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**.

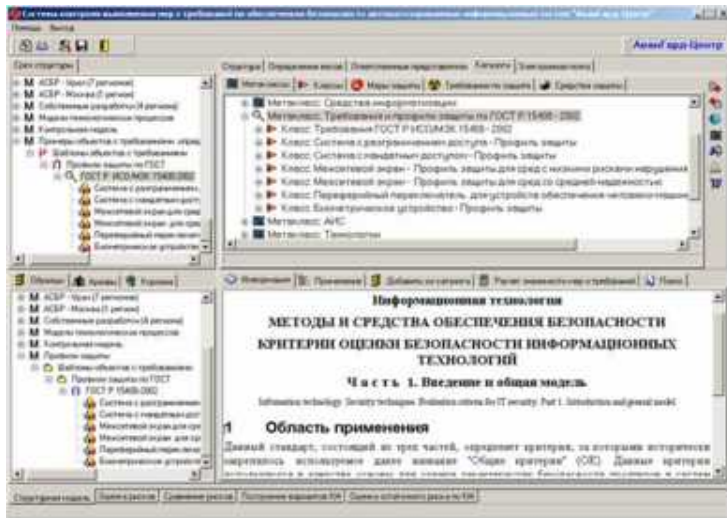
# ШАГ 12: ПОЛУЧИТЬ ЛИЦЕНЗИЮ НА ТЕХНИЧЕСКУЮ ЗАЩИТУ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ



**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 13: 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 14: 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?

**М.Ю.Емельяников**

 (495) 980-2345

 [m.eme@infosec.ru](mailto:m.eme@infosec.ru)