# Обзор требований к средствам обеспечения безопасности персональных данных

*Сергей Золотухин*
*Руководитель направления*
*Дистрибуции услуг*
*ООО «Антивирусный Центр»*

# Основные документы

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСТЭК России от 5 февраля 2010 г. N 58 г. "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных"

# Базовые положения

- Все используемые средства защиты информации должны пройти в установленном порядке процедуру оценки соответствия в ФСТЭК.
- Для информационных систем 1 класса применяется программное обеспечение средств защиты информации, соответствующее 4 уровню контроля отсутствия недекларированных возможностей.
- При разделении информационной системы при помощи межсетевых экранов на отдельные части системы для указанных частей системы может устанавливаться более низкий класс, чем для информационной системы в целом.
- В зависимости от особенностей обработки персональных данных и структуры информационных систем могут разрабатываться и применяться другие методы защиты информации, обеспечивающие нейтрализацию угроз безопасности персональных данных.

# Защита от НСД. Общие требования

- реализация разрешительной системы допуска пользователей к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, а также, хранятся носители информации;
- разграничение доступа к программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и технических средств, позволяющих осуществлять обработку персональных данных;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

# Защита от НСД. Подключение к Интернет

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защита информации при ее передаче по каналам связи;
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
- использование средств антивирусной защиты;
- централизованное управление системой защиты персональных данных информационной системы.

# Защита от НСД. Другие особенности

- Информационные системы, обрабатывающих государственные информационные ресурсы
- Подключение к сетям связи общего пользования с целью предоставления общедоступной информации
- Удаленный доступе к информационной системе через сеть связи общего пользования
- Взаимодействие отдельных информационных систем через сеть связи общего пользования
- Взаимодействие отдельных информационных систем разных операторов

# Требования к системе защиты

**Класс системы (1-2-3-4)**

**Режим обработки и права доступа**

- **Системы однопользовательской обработки ПДн**
- **Системы многопользовательской обработки ПДн при равных правах доступа**
- **Системы многопользовательской обработки ПДн при различных правах доступа**

**Межсетевое взаимодействие**

# Защита от НСД

3.1. Для информационных систем 2 класса при однопользовательском режиме обработки применяются все методы и способы защиты … соответствующие системам 3 класса при однопользовательском режиме обработки.

3.2. Для информационных систем 2 класса при многопользовательском режиме обработки и равных правах доступа применяются все методы и способы защиты соответствующие системам 3 класса …

3.3. Для информационных систем 2 класса при многопользовательском режиме обработки и разных правах доступа реализуются все методы и способы защиты, соответствующие информационным системам 3 класса …

# Требования к МСЭ

| Класс ИСПДн | 3 | 2 | 1 |
|---|---|---|---|
| Независимая фильтрация сетевых пакетов | ✓ | ✓ | ✓ |
| Фильтрация пакетов служебных протоколов | ✓ | ✓ | ✓ |
| Проверка подлинности сетевых адресов (внешний и внутренний интерфейс) | | ✓ | ✓ |
| Фильтрация запросов на транспортном и прикладном уровне | | ✓ | ✓ |
| Учет даты и времени для запросов | | ✓ | ✓ |
| Аутентификация, регистрация и учет запросов | | | ✓ |
| Сигнализация о нарушениях и блокировка нарушителей | | | ✓ |
| Возможность сокрытия субъектов доступа или функций ИСПДн | | | ✓ |
| Регистрация и учет запрашиваемых сервисов прикладного уровня | | | ✓ |

# Подсистема управления доступом

| Класс ИСПДн | Однопользовательская обработка ПДн | | | Многопользовательская обработка ПДн при равных правах доступа | | | Многопользовательская обработка ПДн при различных правах доступа | | |
|---|---|---|---|---|---|---|---|---|---|
| | 3 | 2 | 1 | 3 | 2 | 1 | 3 | 2 | 1 |
| Идентификация и проверка подлинности пользователей при входе в ОС | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Идентификация и проверка подлинности администраторов систем защиты | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Идентификация терминалов, технических средств обработки ПДн, узлов ИСПДн, каналов связи, внешних устройств по логическим адресам (номерам) | | | | | | ✓ | | | ✓ |
| Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам | | | | | | ✓ | | | ✓ |
| Контроль доступа субъектов к объектам в соответствие с матрицей доступа | | | | | | | | | ✓ |

# Подсистема антивирусной защиты

| Класс ИСПДн | Однопользовательская обработка ПДн | | | Многопользовательская обработка ПДн при равных правах доступа | | | Многопользовательская обработка ПДн при различных правах доступа | | |
|---|---|---|---|---|---|---|---|---|---|
| | 3 | 2 | 1 | 3 | 2 | 1 | 3 | 2 | 1 |
| Автоматическая проверка на наличие вредоносного кода с возможностью блокирования, лечения или удаления | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Регулярная проверка по расписанию | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Инициализация проверки при факте обнаружения вредоносных программ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Наличие механизма отката при поиске вредоносных программ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Непрерывный контроль обмена с внешними сетями | | | ✓ | | | ✓ | | | ✓ |
| Непрерывный мониторинг каналов обмена информации ИСПДн | | | ✓ | | | ✓ | | | ✓ |
| Обязательная сертификация ПО | | | ✓ | | | ✓ | | | ✓ |

# Подсистемы технической защиты ПДн

**Управление доступом, регистрация и учет**

**SecretNet, Панцирь, Соболь, Аккорд и аналоги**

**или**

**Windows + Aladdin и аналоги**

**Обеспечение целостности -** Acronis

**Антивирусная защита –** Kapersky и аналоги

**Межсетевое экранирование**

Программные или программно аппаратные средства

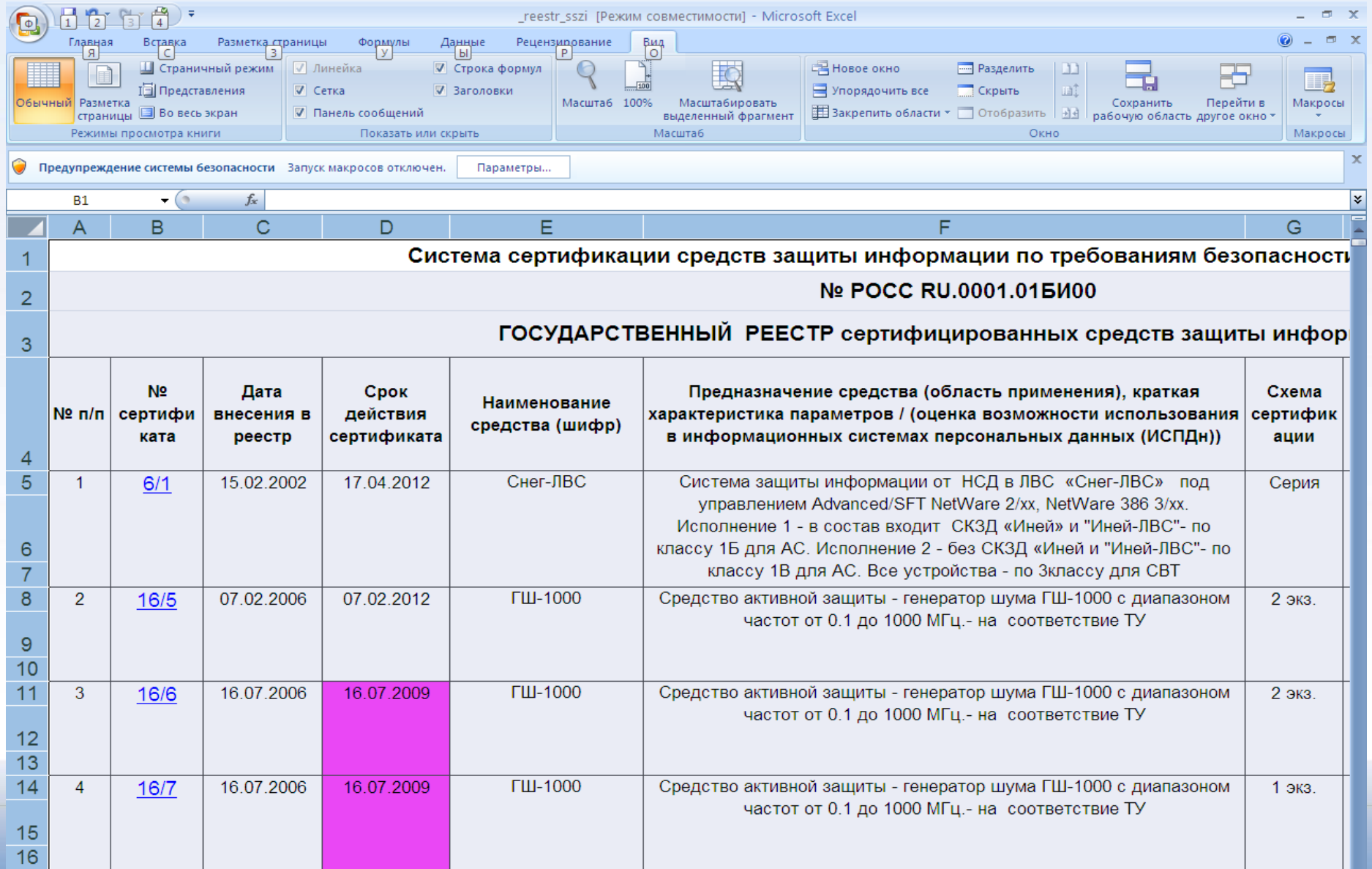
**Обнаружение вторжений**

Программно-аппаратные комплексы

**Анализ защищенности**

Xpider и аналоги

# Реестр сертифицированных средств




| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Система сертификации средств защиты информации по требованиям безопасности | | | | | | |
| 2 | № РОСС RU.0001.01БИ00 | | | | | | |
| 3 | ГОСУДАРСТВЕННЫЙ РЕЕСТР сертифицированных средств защиты инфор | | | | | | |
| 4 | № п/п | № сертификата | Дата внесения в реестр | Срок действия сертификата | Наименование средства (шифр) | Предназначение средства (область применения), краткая характеристика параметров / (оценка возможности использования в информационных системах персональных данных (ИСПДн)) | Схема сертификации |
| 5 | 1 | 6/1 | 15.02.2002 | 17.04.2012 | Снег-ЛВС | Система защиты информации от НСД в ЛВС «Снег-ЛВС» под управлением Advanced/SFT NetWare 2/xx, NetWare 386 3/xx. Исполнение 1 - в состав входит СКЗД «Иней» и "Иней-ЛВС"- по классу 1Б для АС. Исполнение 2 - без СКЗД «Иней и "Иней-ЛВС"- по классу 1В для АС. Все устройства - по 3классу для СВТ | Серия |
| 8 | 2 | 16/5 | 07.02.2006 | 07.02.2012 | ГШ-1000 | Средство активной защиты - генератор шума ГШ-1000 с диапазоном частот от 0.1 до 1000 МГц.- на соответствие ТУ | 2 экз. |
| 11 | 3 | 16/6 | 16.07.2006 | 16.07.2009 | ГШ-1000 | Средство активной защиты - генератор шума ГШ-1000 с диапазоном частот от 0.1 до 1000 МГц.- на соответствие ТУ | 2 экз. |
| 14 | 4 | 16/7 | 16.07.2006 | 16.07.2009 | ГШ-1000 | Средство активной защиты - генератор шума ГШ-1000 с диапазоном частот от 0.1 до 1000 МГц.- на соответствие ТУ | 1 экз. |

# Заключительные вопросы

- С кем проконсультироваться?
- Кто поможет сформировать решение?
- У кого купить?
- Кто поможет внедрить?
- Кто сможет поддерживать?

# Антивирусный Центр в Коми:

8 (8212) 245 000

АНТИВИРУСНЫЙ ЦЕНТР™

# Спасибо за внимание!!!