Эшелон
комплексная безопасность

Сертификация и персональные данные

Михаил Никулин
Директор департамента тестирования и сертификации
ЗАО «НПО «Эшелон»

План доклада

- Виды сертификационных испытаний ПО
- Нормативная база
- Классификация ИСПДн
- Требования по защите ПДн
- Необходимость сертификации в ИСПДн
- Выбор требуемого класса защищенности и уровня контроля отсутствия НДВ в ИСПДн
- Ответственность за нарушение требований по сертификации

Виды сертификационных испытаний средств защиты информации

- Проверка функциональных возможностей продукта по защите информации на соответствие требованиям:
  - РД Гостехкомиссии России. СВТ. Защита от НСД. Показатели защищённости от несанкционированного доступа к информации
  - РД Гостехкомиссии России. СВТ. МЭ. Защита от несанкционированного доступа. Показатели защищённости от НСД к информации
  - Технических условий
  - Задания по безопасности
- Проверка исходного кода продукта на соответствие требованиям:
  - Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия НДВ

Нормативная база защиты персональных данных

- Федеральный закон «**О персональных данных**» №152-ФЗ
- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (Постановление Правительства РФ №781 от 17.11.2007)
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (Постановление Правительства РФ №687 от 15.09.2008)
- Порядок проведения классификации информационных систем персональных данных (приказ от 13.02.2008 №55/86/20 ФСТЭК/ФСБ/МИТСРФ)
- Положение об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа … (Постановление Правительства РФ от 15 мая 2010 г. № 330)

Нормативная база защиты персональных данных (документы ФСТЭК России)

- **Базовая модель угроз** безопасности ПДн при их обработке в ИСПДн (утверждена 15.02.2008 ФСТЭК России)
- **Методика определения актуальных угроз** безопасности ПДн при их обработке в ИСПДн (утверждена 14.02.2008 ФСТЭК России)
- **Положение** о методах и способах защиты информации в информационных системах персональных данных (приказ ФСТЭК России от 05.02.2010 N 58)

Нормативная база защиты персональных данных (документы ФСБ России)

- **Типовые требования** по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности ПДн при их обработке в ИСПДн (утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622)
- **Методические рекомендации** по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации (утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144)

Регуляторы по защите персональных данных

- **ФСТЭК России**

- **ФСБ России**

- **Роскомнадзор** (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) - осуществляет функции по контролю и надзору за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн, является уполномоченным федеральным органом исполнительной власти по защите прав субъектов ПДн

Основные понятия в защите персональных данных

- **Персональные данные** (ПДн) – любая информация, относящаяся к ***определенному*** или ***определяемому*** на основании такой информации физическому лицу, в том числе:
  - фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация
- **Конфиденциальность персональных данных** – ***обязательное*** для соблюдения оператором или иным получившим доступ к ПДн лицом требование ***не допускать их распространения без согласия субъекта*** персональных данных или наличия иного законного основания

Основные понятия в защите персональных данных

- **Обезличенные персональные данные** – ПДн, для которых невозможно установить принадлежность ***конкретному*** лицу
- **Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, ***организующие*** и (или) ***осуществляющие*** обработку ПДн, а также ***определяющие*** цели и содержание обработки персональных данных

Исходные данные для классификации ИСПДн

- **Категория** обрабатываемых данных – $\mathbf{X_{пд}}$
- **Объем** одновременно обрабатываемых данных – $\mathbf{X_{нпд}}$
- А также:
  - характеристики безопасности
  - структура информационной системы
  - наличие подключений к ССОП
  - режим обработки ПДн
  - режим разграничения прав доступа
  - местонахождение технических средств

Категории и объемы ПДн

- Определено 4 категории
  - **Категория 4** – ***обезличенные*** данные
  - **Категория 3** – данные, позволяющие ***идентифицировать*** Субъекта
  - **Категория 2** – данные, позволяющие ***идентифицировать*** Субъекта и получить о нем ***дополнительную информацию***
  - **Категория 1** – данные о состоянии ***здоровья***, расовой и национальной принадлежности, политических, религиозных и философских взглядах, интимной жизни
- Определены 3 значения объема:
  - **3** – данные ***менее чем 1 000*** Субъектов или данные Субъектов в пределах конкретной организации
  - **2** – данные ***от 1 000 до 100 000*** Субъектов или данные Субъектов в пределах отрасли экономики, органа гос.власти, проживающих в пределах муниципального образования
  - **1** – данные ***более чем 100 000*** Субъектов или данные Субъектов в пределах субъекта РФ или РФ в целом

Исходные данные для классификации ИСПДн

$X_{пд}$ \ $X_{нпд}$	3	2	1
Категория 4	4 класс	4 класс	4 класс
Категория 3	3 класс	3 класс	2 класс
Категория 2	3 класс	2 класс	***1 класс***
Категория 1	***1 класс***	***1 класс***	***1 класс***

- От выбора класса зависит состав и объем защитных мер
- Понижение класса системы
  - снижение категории (***обезличивание*** данных)
  - снижение объема (***дробление*** системы)

Общий порядок действий оператора по приведению ИСПДн в соответствие ФЗ-152

- Классификация ИСПДн
- Обоснование необходимости обработки ПДн
- Документирование информационных потоков и технологии обработки ПДн
- Разработка модели угроз
- Разработка технического задания на ИСПДн
- Разработка частного задания на систему защиты ПДн
- Разработка и внедрение системы защиты ПДн
- Получение лицензий ФСТЭК России и ФСБ России
- Аттестация ИСПДн

Необходимость сертификации в ИСПДн

- Положение об обеспечении безопасности ПДн при их обработке в ИСПДн:
  - П.5: Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят **процедуру оценки соответствия**.
- Положение о методах и способах защиты информации в ИСПДн:
  - П.2.1: Методами и способами защиты информации от несанкционированного доступа являются:

    …

    - использование средств защиты информации, прошедших в установленном порядке **процедуру оценки соответствия**.

Необходимость сертификации в ИСПДн

- Положение о методах и способах защиты информации в ИСПДн:
  - П.3.2: Для исключения утечки персональных данных за счет ПЭМИН в информационных системах 1 класса могут применяться следующие методы и способы защиты информации:

    - использование средств защиты информации, прошедших в установленном порядке **процедуру оценки соответствия**.
  - П.2.12: Программное обеспечение средств защиты информации, применяемых в информационных системах 1 класса, проходит **контроль отсутствия НДВ**. Необходимость проведения контроля отсутствия НДВ программного обеспечения средств защиты информации, применяемых в информационных системах 2 и 3 классов, определяется оператором (уполномоченным лицом).

Необходимость сертификации в ИСПДн

- Методы и способы защиты информации от несанкционированного доступа в зависимости от класса информационной системы (Приложение к Положению о методах и способах защиты информации в ИСПДн):
  - П.7: Для информационных систем 1 класса применяется программное обеспечение средств защиты информации, соответствующее 4 уровню контроля отсутствия НДВ.

Необходимость сертификации в ИСПДн

- Положение об особенностях оценки соответствия продукции … (Постановление Правительства РФ от 15 мая 2010 г. № 330):
  - Оценка соответствия осуществляется в формах **обязательной сертификации** и государственного контроля (надзора).
  - Организация и проведение обязательной сертификации продукции осуществляются в порядке, определяемом уполномоченным федеральным органом исполнительной власти в пределах его компетенции.

Необходимость сертификации СКЗИ в ИСПДн

- Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации:
  - П. 3.1: Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации) криптосредства.

Лицензирование деятельности

- Положение о методах и способах защиты информации в ИСПДн:
  - Для выбора и реализации методов и способов защиты информации в информационной системе может привлекаться организация, имеющая оформленную в установленном порядке **лицензию на осуществление деятельности по технической защите конфиденциальной информации**.

СЕРИЯ КИ 0033 НОМЕР 001631

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 0586 от 13 июля 2007 г.

Федеральная служба по техническому и экспортному контролю разрешает осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации

Лицензия предоставлена Закрытому акционерному обществу
«Научно-Производственное Объединение «Эшелон»
(ЗАО «НПО «Эшелон»)
ОГРН 1057748235577, ИНН 7713565119

Адрес места нахождения:
127591, г. Москва, Керамический пр., д. 53, корп. 1

Адрес места осуществления лицензируемой деятельности:
109052, г. Москва, ул. Подъемная, д. 14, стр. 7

Лицензия предоставлена на срок до 13 июля 2012 г.

на основании приказа ФСТЭК России от 13 июля 2007 г. № 155

Заместитель директора
А.Гапонов

Перечень применяемых в ИСПДн СЗИ

- Положение о методах и способах защиты информации в ИСПДн:
  - средства предотвращения несанкционированного доступа
  - средства защиты информации при межсетевом взаимодействии
  - антивирусные средства
  - средства анализа защищенности
  - средства обнаружения вторжений
  - криптографические средства

Требования по сертификации средств защиты в ИСПДн

- Для ИСПДн 4 класса оценка соответствия проводится по **решению оператора**
- Для ИСПДн 3 класса:

Класс АС	Класс МЭ (при подключении ИСПДн к сетям ОП)	Класс МЭ (при разделении ИСПДн на отдельные части)	Уровень контроля отсутствия НДВ
3Б	5 класс	5 класс	-
2Б			
1Д			

Требования по сертификации средств защиты в ИСПДн

- Для ИСПДн 2 класса:

Класс АС	Класс МЭ (при подключении ИСПДн к сетям ОП)	Класс МЭ (при разделении ИСПДн на отдельные части)	Уровень контроля отсутствия НДВ
3Б	4 класс	5 класс	-
2Б			
1Д			

Требования по сертификации средств защиты в ИСПДн

- Для ИСПДн 1 класса:

Класс АС	Класс МЭ (при подключении ИСПДн к сетям ОП)	Класс МЭ (при разделении ИСПДн на отдельные части)	Уровень контроля отсутствия НДВ
3А*	3 класс	5 класс	4 уровень
2А**			
1Г***			

Требования по сертификации средств защиты в ИСПДн

* **3А** без требования по применению сертифицированных СЗИ.

** **2А** без:

- полномочного управления доступом,
- автоматического учета создаваемых файлов и их маркировки,
- описания способа очистки памяти,
- физической охраны без указания на использование технических средств охраны и специального персонала, использования строгого пропускного режима, специального оборудования помещений,
- требований к наличию администратора безопасности,
- требования по применению сертифицированных СЗИ.

*** **1Г** без:

- журнала учета выдачи защищаемых носителей,
- описания способа очистки памяти,
- упора на нерабочее время для физической охраны.

Ответственность за нарушение требований ФЗ «О персональных данных»

- Ст. 24 ФЗ-152:
  - Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут гражданскую, **уголовную**, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность

- Ст. 19 ФЗ-152:
  - **Оператор** обязан принимать необходимые организационные и технические меры для защиты ПДн от неправомерных действий

Ответственность за нарушение требований «О персональных данных»

- П.10 «Положения об обеспечении безопасности персональных данных…»
  - Безопасность ПДн при их обработке в ИС обеспечивает **оператор** или лицо, которому на основании договора оператор поручает обработку персональных данных (далее - уполномоченное лицо). Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность ПДн и безопасность ПДн при их обработке в ИС

Кодекс РФ об административных правонарушениях

- Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (**персональных данных**) - влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - **от пяти тысяч до десяти тысяч рублей**

- Ст.13.12. п.1. Нарушение условий, предусмотренных **лицензией на осуществление деятельности в области защиты информации** (за исключением информации, составляющей государственную тайну), -влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - **от пяти тысяч до десяти тысяч рублей**

Кодекс РФ об административных правонарушениях

- Ст.13.12. п.2. Использование **несертифицированных информационных систем, баз и банков данных**, а также несертифицированных **средств защиты информации**, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от одной тысячи до двух тысяч рублей; на юридических лиц - **от десяти тысяч до двадцати тысяч рублей с конфискацией несертифицированных средств защиты информации** или без таковой

Кодекс РФ об административных правонарушениях

- Ст.13.12. п.3. **Нарушение условий**, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей **государственную тайну**, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от двух тысяч до трех тысяч рублей; на юридических лиц - **от пятнадцати тысяч до двадцати тысяч** рублей

Кодекс РФ об административных правонарушениях

- Ст.13.12. п.4. Использование **несертифицированных средств**, предназначенных для защиты информации, составляющей **государственную тайну**, - влечет наложение административного штрафа на должностных лиц в размере от трех тысяч до четырех тысяч рублей; на юридических лиц - от двадцати тысяч до тридцати тысяч рублей **с конфискацией несертифицированных средств,** предназначенных для защиты информации, составляющей государственную тайну, или без таковой

Кодекс РФ об административных правонарушениях

- Ст.13.12. п.5. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей гос.тайну), влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от 1 тысячи до 1,5 тысячи рублей или административное приостановление деятельности на срок до 90 суток; на должностных лиц - от 1 тысячи до 1,5 тысячи рублей; на юридических лиц - **от 10 тысяч до 15 тысяч рублей** или административное **приостановление деятельности на срок до 90 суток**

Кодекс РФ об административных правонарушениях

- Ст. 13.13. п.1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) **без получения** в установленном порядке специального разрешения (**лицензии**), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц - от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - **от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации** или без таковой.

Кодекс РФ об административных правонарушениях

- Ст. 13.13. п.2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей **государственную тайну**, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, **без лицензии** - влечет наложение административного штрафа на должностных лиц в размере от четырех тысяч до пяти тысяч рублей; на юридических лиц - **от тридцати тысяч до сорока тысяч рублей с конфискацией созданных без лицензии средств защиты информации**, составляющей государственную тайну, или без таковой

Кодекс РФ об административных правонарушениях

- Ст. 13.14. **Разглашение информации**, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, - влечет наложение административного штрафа на граждан в размере от 500 до 1 тысячи рублей; на должностных лиц - от 4 тысяч до 5 тысяч рублей

Уголовный кодекс РФ

- Ст. 171. Незаконное предпринимательство. Осуществление предпринимательской деятельности … без специального разрешения (лицензии) в случаях, когда такое разрешение (лицензия) обязательно, или **с нарушением лицензионных требований и условий**, если это деяние причинило крупный ущерб гражданам наказывается штрафом в размере до 300 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до 2 лет, либо обязательными работами на срок от 180 до 240 часов, либо арестом на **срок** от 4 до 6 месяцев.

Ответственность за нарушения, которые могут быть связаны с использованием СЗИ

- **Уголовный кодекс РФ:**
  - Гл. 32. Преступления против порядка управления: ст.320 (разглашение сведений..)
  - Гл. 31. Преступления против правосудия: ст.310, 311 (разглашение..)
  - Гл. 30. Преступления против государственной власти…: ст. 293 (халатность)
  - Гл. 28. Преступления в сфере компьютерной информации
  - Гл. 26. Экологические преступления
  - Гл. 22. Преступления в сфере экономической деятельности: ст.178, 183 (условия.., разглашения тайн)
  - Гл. 19. Преступления против Конституционных прав и свобод человека и гражданина
  - и др.

Спасибо за внимание

Михаил Никулин

Директор департамента тестирования и сертификации
ЗАО «НПО «Эшелон»

тел: (495) 645-38-09(10,11)

e-mail: m.nikulin@cnpo.ru

web: http://эшелон.рф