Защита информации и персональных данных. Требования к антивирусному комплекту

Инна Педченко
ЗАО «Лаборатория Касперского»
Региональный представитель в СФО
тел/факс: +7 983 121 79 74
E-mail: inna.pedchenko@ru.kaspersky.com

История

- 1981 г. Совет Европы. Конвенция «О защите личности в связи автоматической обработкой персональных данных»
- 2001 г. Россия подписала конвенцию
- 2005 г. 19 декабря. Россия. ФЗ от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных»
- 2006 г. 27 июля президент России подписал Федеральный закон № 152-ФЗ «О персональных данных».

ФЗ №152 «О персональных данных»

Основные понятия

- **Персональные данные (ПДн)** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (**субъекту ПД**), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- **Оператор персональных данных** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки;

ФЗ №152 «О персональных данных»

Обеспечение безопасности ПДн

- **Операторами … должна обеспечиваться конфиденциальность** персональных данных, за исключением случаев, обезличенных и общедоступных персональных данных.
- **Оператор обязан принимать** организационные и технические меры, для защиты ПД от НСД, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий (ст. 19, ч. 1)
- **Правительство РФ устанавливает требования** к обеспечению безопасности ПД при их обработке Требования должны быть выполнены **до 01.01.2011 г.**
- **Лица,** виновные в нарушении требований **несут** гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ **ответственность**

Защита персональных данных

- **Регуляторы:** Роскомнадзор, ФСТЭК, ФСБ России

Постановление Правительства РФ от 17.11.2007 г. № 781

- возлагает на **оператора ПДн** задачу обеспечения безопасности ПДн и обязанность классификации ИС
- возлагает на **ФСТЭК России** и **ФСБ России** разработку методов и способов защиты ПДн в информационных системах

Методические материалы ФСТЭК

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года (Базовая модель).
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года (Методика).

Положение о методах и способах защиты информации в информационных системах персональных данных

Приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

Вступил в действие 16 марта 2010 г.

Классификация ИСПДн

Классы ПДн

- **категория 1** – расовая принадлежность, политические взгляды, религиозные убеждения, состояния здоровья, интимной жизни;
- **категория 2** - персональные данные, позволяющие идентифицировать субъекта и получить о нем дополнительную информацию;
- **категория 3** - персональные данные, позволяющие идентифицировать субъекта персональных данных;
- **категория 4** - обезличенные и (или) общедоступные персональные данные.

Классы ИС

- **категория 1** - в ИС обрабатываются ПДн более чем 100 000 субъектов;
- **категория 2** - в ИС обрабатываются ПДн от 1 000 до 100 000 субъектов;
- **категория 3** - в ИС одновременно обрабатываются данные менее чем 1 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Классификация ИСПДн

ИС, обрабатывающие ПД, делятся на типовые и специальные:

- **Типовые ИС** - информационные системы, в которых требуется обеспечение только конфиденциальности ПД;
- **Специальные ИС** - системы, в которых вне зависимости от необходимости обеспечения конфиденциальности ПД требуется обеспечить хотя бы одну из характеристик безопасности ПД, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий)

Классификация ИСПДн

В зависимости от последствий нарушений заданной характеристики безопасности ПД, типовой ИС присваивается один из классов:

класс 1 (К1) - ИС, для которых нарушения могу привести к значительным негативным последствиям для субъектов ПД;

- **класс 2 (К2)** - ИС, для которых нарушения могут привести к негативным последствиям для субъектов ПД;
- **класс 3 (К3)** - ИС, для которых нарушения могут привести к незначительным негативным последствиям для субъектов ПД;
- **класс 4 (К4)** - ИС, для которых нарушения не приводят к негативным последствиям для субъектов ПД.

Количество субъектов / Категории ПД	> 1000	1000 – 100 000	< 100 000
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Положение о методах и способах защиты информации

II. Методы и способы защиты информации от несанкционированного доступа

2.3. В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются **средства антивирусной защиты**.

2.5. Подключение информационных систем, обрабатывающих **государственные информационные ресурсы**, к информационно-телекоммуникационным сетям международного информационного обмена осуществляется в соответствии с **Указом** Президента Российской Федерации от **17 марта 2008 г. N 351** "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" (Собрание законодательства Российской Федерации, 2008, N 12, ст. 1110; N 43, ст. 4919).

Положение о методах и способах защиты информации

2.12. Программное обеспечение средств защиты информации, применяемых в информационных системах **1 класса**, проходит **контроль отсутствия недекларированных возможностей**.

Необходимость проведения **контроля отсутствия недекларированных возможностей** программного обеспечения средств защиты информации, применяемых в информационных системах **2 и 3 классов**, **определяется оператором** (уполномоченным лицом).

Приложение к Положению о методах и способах защиты информации в информационных системах персональных данных

Методы и способы защиты информации от несанкционированного доступа в зависимости от класса информационной системы

7. Для информационных систем **1 класса** применяется программное обеспечение средств защиты информации, соответствующее **4 уровню контроля отсутствия недекларированных возможностей.**

Классификация по уровню контроля отсутствия НДВ

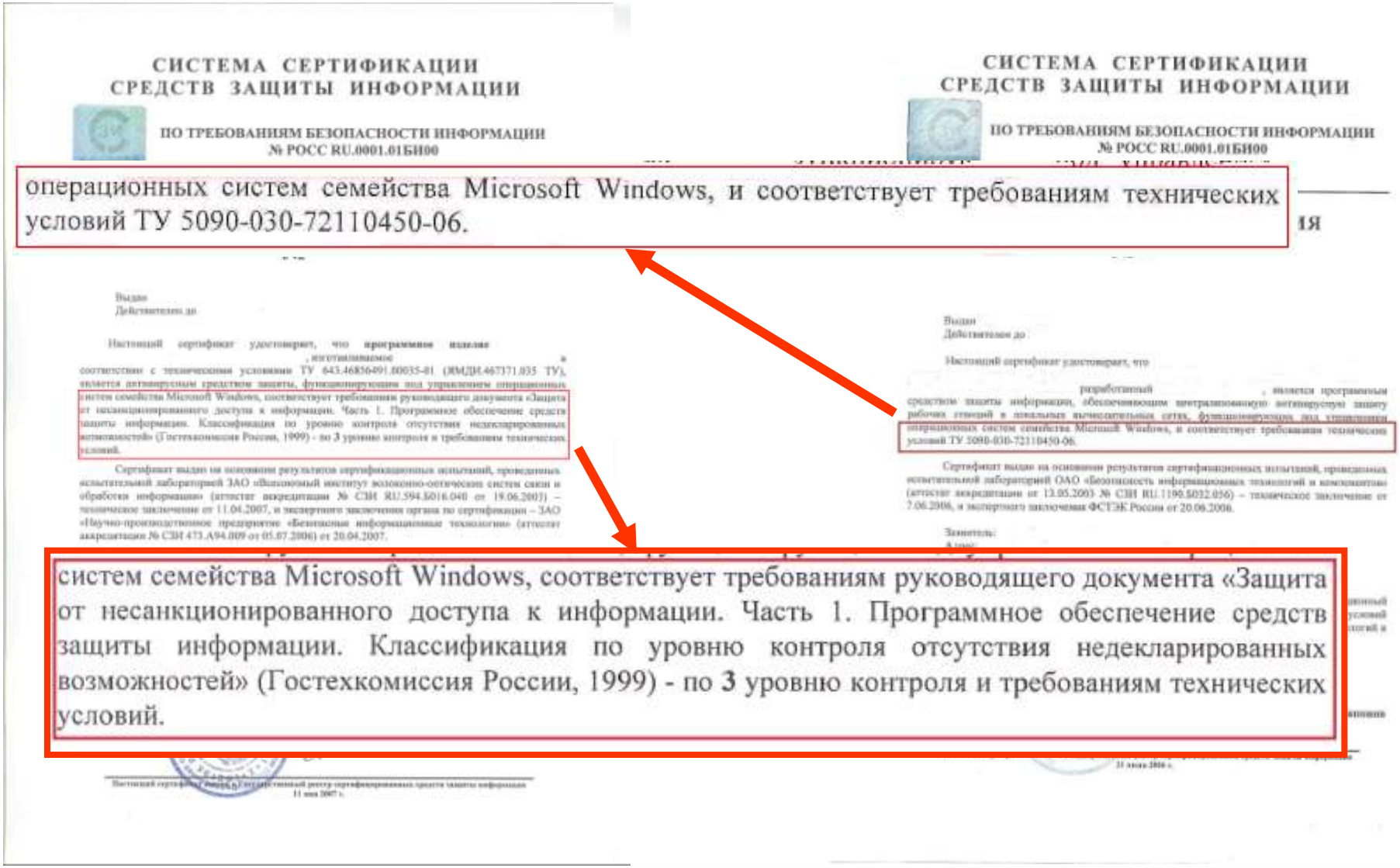
«Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации Классификация по уровню контроля

Недекларированные возможности – функциональные возможности средств вычислительной техники и (или) программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

1.5. Самый низкий уровень контроля - **четвертый**, достаточен для НО, используемого при защите **конфиденциальной** информации.

Руководящий документ
Гостехкомиссии №114 от 04.06.99 г

Сертификаты ФСТЭК России



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

операционных систем семейства Microsoft Windows, и соответствует требованиям технических условий ТУ 5090-030-72110450-06.

Выдан
Действителен до

Настоящий сертификат удостоверяет, что программное изделие
, изготавливаемое
соответствии с техническими условиями ТУ 643.46856491.00035-01 (ЯМДИ.467371.035 ТУ), является антивирусным средством защиты, функционирующим под управлением операционных систем семейства Microsoft Windows, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 3 уровню контроля и требованиям технических условий.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «Волоконный институт волоконно-оптических систем связи и обработки информации» (аттестат аккредитации № СЗИ RU.594.Б016.040 от 19.06.2003) – техническое заключение от 11.04.2007, и экспертного заключения органа по сертификации – ЗАО «Научно-производственное предприятие «Безопасные информационные технологии» (аттестат аккредитации № СЗИ 473.А94.009 от 05.07.2006) от 20.04.2007.

Выдан
Действителен до

Настоящий сертификат удостоверяет, что

разработанный , является программным средством защиты информации, обеспечивающим централизованную антивирусную защиту рабочих станций в локальных вычислительных сетях, функционирующих под управлением операционных систем семейства Microsoft Windows, и соответствует требованиям технических условий ТУ 5090-030-72110450-06.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ОАО «Безопасность информационных технологий и компьютеры» (аттестат аккредитации от 13.05.2003 № СЗИ RU.7190.Б032.056) – техническое заключение от 7.06.2006, и экспертного заключения ФСТЭК России от 20.06.2006.

Заявитель:

систем семейства Microsoft Windows, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по **3** уровню контроля и требованиям технических условий.

Указ №351 от 17.03.2008

Основные положения

- **……подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники к информационно-телекоммуникационным сетям международного информационного обмена производится только с использованием средств защиты информации прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для операторов информационных систем, владельцев информационно-телекоммуникационных сетей и (или) средств вычислительной техники;**

- **…..государственные органы в целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, используют только средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю;**

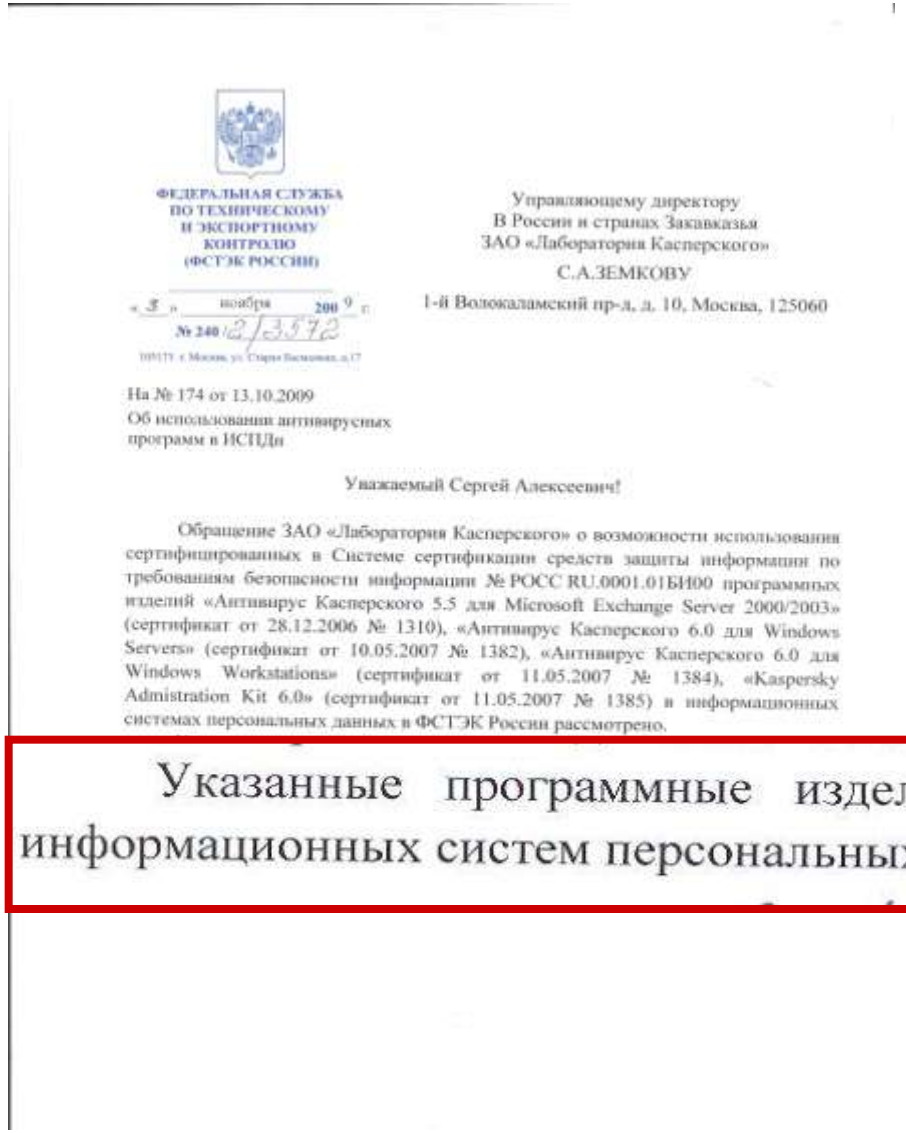
«ЛК»: соответствие закону и стандартам

- Сертификаты ФСБ России для защиты информации, составляющей государственную тайну

- Сертификаты ФСТЭК России по 3 уровню контроля отсутствия недекларированных возможностей

Государственный реестр сертифицированных средств защиты информации http://www.fstec.ru

«ЛК»: соответствие закону и стандартам



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК РОССИИ)

« 3 » ноября 200 9 г.
№ 240/2/3572

Управляющему директору
В России и странах Закавказья
ЗАО «Лаборатория Касперского»
С.А.ЗЕМКОВУ
1-й Волоколамский пр-д, д. 10, Москва, 125060

На № 174 от 13.10.2009
Об использовании антивирусных программ в ИСПДн

Уважаемый Сергей Алексеевич!

Обращение ЗАО «Лаборатория Касперского» о возможности использования сертифицированных в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 программных изделий «Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003» (сертификат от 28.12.2006 № 1310), «Антивирус Касперского 6.0 для Windows Servers» (сертификат от 10.05.2007 № 1382), «Антивирус Касперского 6.0 для Windows Workstations» (сертификат от 11.05.2007 № 1384), «Kaspersky Administration Kit 6.0» (сертификат от 11.05.2007 № 1385) в информационных системах персональных данных в ФСТЭК России рассмотрено.

Указанные программные изделия могут использоваться при создании информационных систем персональных данных до первого класса включительно.

- Антивирус Касперского 6.0 для Windows Workstations
(Сертификат № 1384)
- Антивирус Касперского 6.0 для Windows Server
(Сертификат № 1382)
- Kaspersky Administration Kit 6.0
(Сертификат № 1385)
- Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003 (Сертификат № 1310)

«ЛК»: соответствие закону и стандартам

Сертифицируется программный код

Сертифицированные дистрибутивы ФСТЭК:

- Kaspersky WorkSpace Security Certified Media Pack
- Kaspersky BusinessSpace Security Certified Media Pack
- Kaspersky EnterpriseSpace Security Certified Media Pack

Комплект поставки сертифицированного дистрибутива включает:

- CD в конверте с записанными сертифицированными приложениями,
- формуляр – документ, подтверждающий, что данный(е) CD действительно содержат сертифицированные приложения
- заверенные копии сертификатов ФСТЭК.

Сертифицированные дистрибутивы ФСБ:

- Kaspersky Open Space Security Certified Media Pack Customized

Спасибо за внимание!

Инна Педченко
ЗАО «Лаборатория Касперского»
Региональный представитель в СФО
тел/факс: +7 983 121 79 74
E-mail: inna.pedchenko@ru.kaspersky.com

KASPERSKY lab