Кафедра: ПОВТАС

Дисциплина: Основы информационной безопасности

Лекция 3. Основные нормативные и методические документы ФСТЭК и ФСБ. Понятие лицензирования, стандартизации и сертификации в области ИБ

Вопросы занятия

1. Основные нормативные и методические документы ФСТЭК и ФСБ.

2. Лицензирование деятельности в области технической защиты информации.

3. Сертификация средств защиты информации.

1. Основные нормативные и методические документы ФСТЭК и ФСБ

ФЗ «О персональных данных» от 27.07.2006 г. № 152-ФЗ.

- определены основные термины и определения, связанные с обработкой ПДн (ст. 3).
- указаны принципы обработки ПДн (ст. 5).
- ***раскрываются случаи обработки ПДн, регулируется поручение обработки ПДн третьему лицу и связанные с этим обязательства*** (ст. 6).
- прописан порядок получения согласия, условия обработки ПДн без согласия, принципы получения согласия (ст. 9).
- ***определены специальные категории ПДн и условия их обработки (ст. 10).***
- ***определены биометрические данные и условия их обработки*** (ст. 11).
- уточнен порядок трансграничной передачи ПДн (ст. 12).
- прописаны права субъектов (ст. 14-17), обязанности оператора (ст.18-22).
- определены меры по обеспечению выполнения обязанностей, предусмотренных ФЗ «О персональных данных» (ст. 18.1)
- ***определены меры по обеспечению безопасности ПДн*** (ст. 19).
- уведомление об обработке ПДн: случаи необходимости подачи уведомления, содержание уведомления (ст. 22).
- ***появилось указание на лицо, ответственное за обработку ПДн, его обязанности (ст. 22.1).***
- ***определение уполномоченного органа по защите прав субъектов, его обязанности, полномочия*** (ст. 23).
- определена ответственность за нарушение требований ФЗ «О персональных данных» (ст. 24).

1. Основные нормативные и методические документы ФСТЭК и ФСБ

ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ:

✓ определены понятия по обработке и защите информации (ст. 2).

✓ прописано определение обладателя информации, его права, связанные с информацией (ст. 6).

✓ прописаны ограничения на доступ к информации, в т.ч. ПДн (ч. 8 ст. 9).

✓ указаны меры по защите информации (ст. 16).

✓ прописана ответственность за нарушения в сфере информации, информационных технологий и защиты информации (ст. 17).

ФЗ «О техническом регулировании» от 27.12.2002 г. № 184-ФЗ:

✓ определены понятия технического регламента, технического регулирования (ст. 2).

✓ прописаны принципы технического регулирования, его особенности (ст.ст. 3,5).

✓ указаны цели принятия технических регламентов(ст. 6).

✓ определены порядок разработки, принятия, изменения и отмены технического регламента (ст.9).

ФЗ «О лицензировании отдельных видов деятельности» от 04.05.2011 г. № 99-ФЗ:

✓ определены цели, задачи лицензирования (ст. 2).

✓ прописано, что лицензированию подлежит разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, ***если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя); деятельность по технической защите конфиденциальной информации*** (ст. 12).

1. Основные нормативные и методические документы ФСТЭК и ФСБ

Акты Правительства

Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

- ❖Отменяет Постановление Правительства № 781 от 17.11.2007 г.
- ❖Система защиты персональных данных может включать в себя только организационные меры.
- ❖Деление информационных систем персональных данных на виды.
- ❖Деление вышеуказанных ИСПДн на ИСПДн, в которых обрабатываются ПДн сотрудников оператора, и ИСПДн, в которых обрабатываются ПДн не сотрудников.
- ❖Выделяется 3 типа угроз безопасности ПДн;
- ❖Выделяются 4 уровня защищённости (УЗ) и меры для их обеспечения;
- ❖Контроль за выполнением указанных требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

1. Основные нормативные и методические документы ФСТЭК и ФСБ

Постановление Правительства РФ от 06.07.2008 N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»:

❖ ***определены требования к материальным носителям биометрических ПДн***:

- защиты от несанкционированной повторной и дополнительной записи после ее извлечения из ИСПДн.
- возможность доступа к записанным на материальный носитель биометрическим ПДн, осуществляемого оператором и лицами, уполномоченными в соответствии с законодательством РФ на работу с биометрическими ПДн.
- невозможность несанкционированного доступа к биометрическим ПДн, содержащимся на материальном носителе.

❖ ***определены обязанности оператора***:

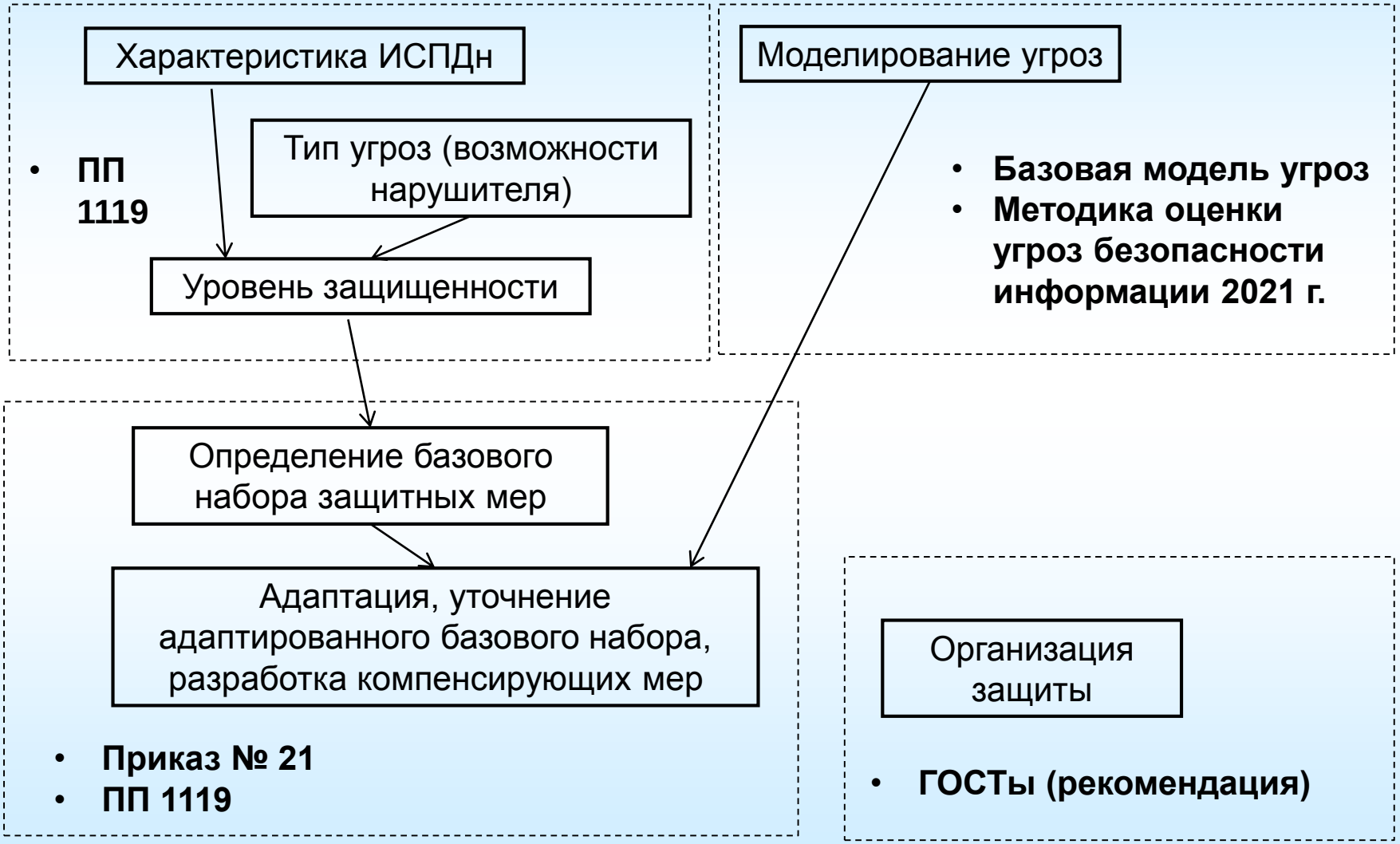
- утвердить порядок передачи материальных носителей уполномоченным лицам.
- осуществлять учет количества экземпляров материальных носителей.
- осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических ПДн на материальный носитель.

❖ ***определены условия хранения биометрических носителей ПДн***:

- должен обеспечиваться доступ к информации, содержащейся на материальном носителе, для уполномоченных лиц.
- применение средств электронной цифровой подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических ПДн, записанных на материальный носитель.

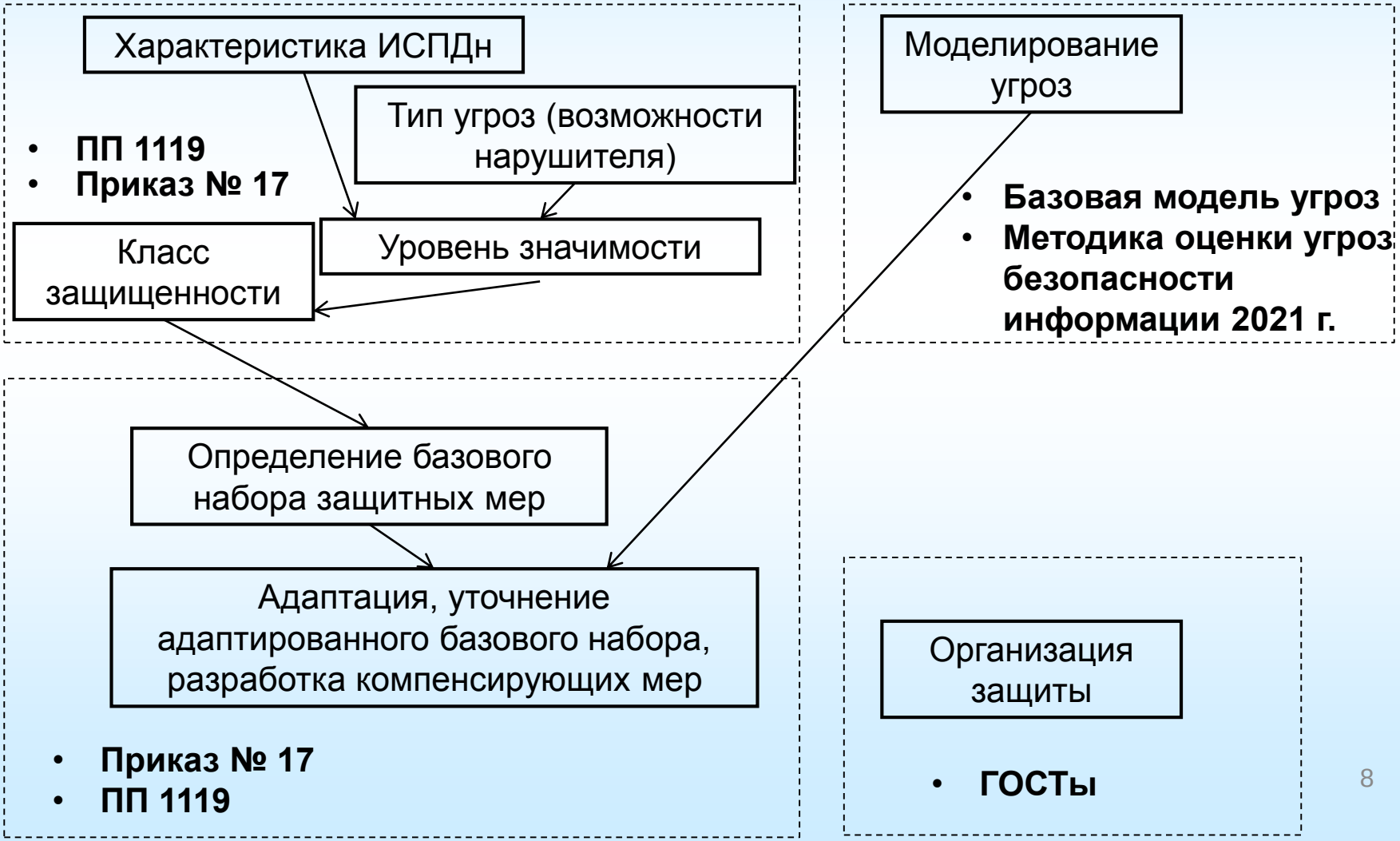
1. Основные нормативные и методические документы ФСТЭК и ФСБ

Порядок защиты персональных данных, действующий с июня 2013 г.



1. Основные нормативные и методические документы ФСТЭК и ФСБ

Порядок защиты информации, не составляющей государственную тайну (в т.ч. персональных данных), в государственных ИС, действующий с 1 сентября 2013 г.



1. Основные нормативные и методические документы ФСТЭК и ФСБ

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

- полная версия включает ПЭМИН и имеет гриф ДСП;
- подробная классификация и описание большинства угроз;
- классификация нарушителей
- приведены типовые модели угроз в ИСПДн различных конфигураций.

Методика оценки угроз безопасности информации

- позволяет из перечня угроз определить подмножество актуальных;
- в соответствии с новой редакцией закона «О персональных данных» моделирование угроз является обязанностью органов власти.

1. Основные нормативные и методические документы ФСТЭК и ФСБ

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждённая приказом № 282 от 30.08.2002

- распространяются на всю конфиденциальную информацию, в том числе на ПДн;
- для государственных информационных ресурсов носят обязательный характер, для остальных – рекомендательный;
- регламентирует взаимоотношения при оказании услуг по ТЗКИ;
- содержит образцы некоторых документов.

1. Основные нормативные и методические документы ФСТЭК и ФСБ

Приказ ФСТЭК России от 18.02.2013 N 21
"Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

- Определяет состав и содержание мер для каждого из уровней защищенности;
- Определяет порядок выбора мер из предложенного перечня;
- В случае применения сертифицированных по требованиям безопасности средств защиты информации четко указывает классы на соответствие которым осуществлена сертификация.

1. Основные нормативные и методические документы ФСТЭК и ФСБ

Приказ ФСТЭК России от 11 февраля 2013 г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

- Распространяется не только на ПДн, но и на другую конфиденциальную информацию;
- В основе почти такой же перечень мер, как и в приказе № 21;
- Определяет порядок классификации информационных систем в зависимости от значимости обрабатываемой информации и масштабов информационной системы;
- Предписывает использовать сертифицированные средства защиты и аттестовывать информационные системы.

1. Основные нормативные и методические документы ФСТЭК и ФСБ

МЕТОДИЧЕСКИЙ ДОКУМЕНТ
МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ
В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

- Утвержден ФСТЭК России 11 февраля 2014.
- Подробное описание реализации мер.
- Документ содержит 176 страниц.

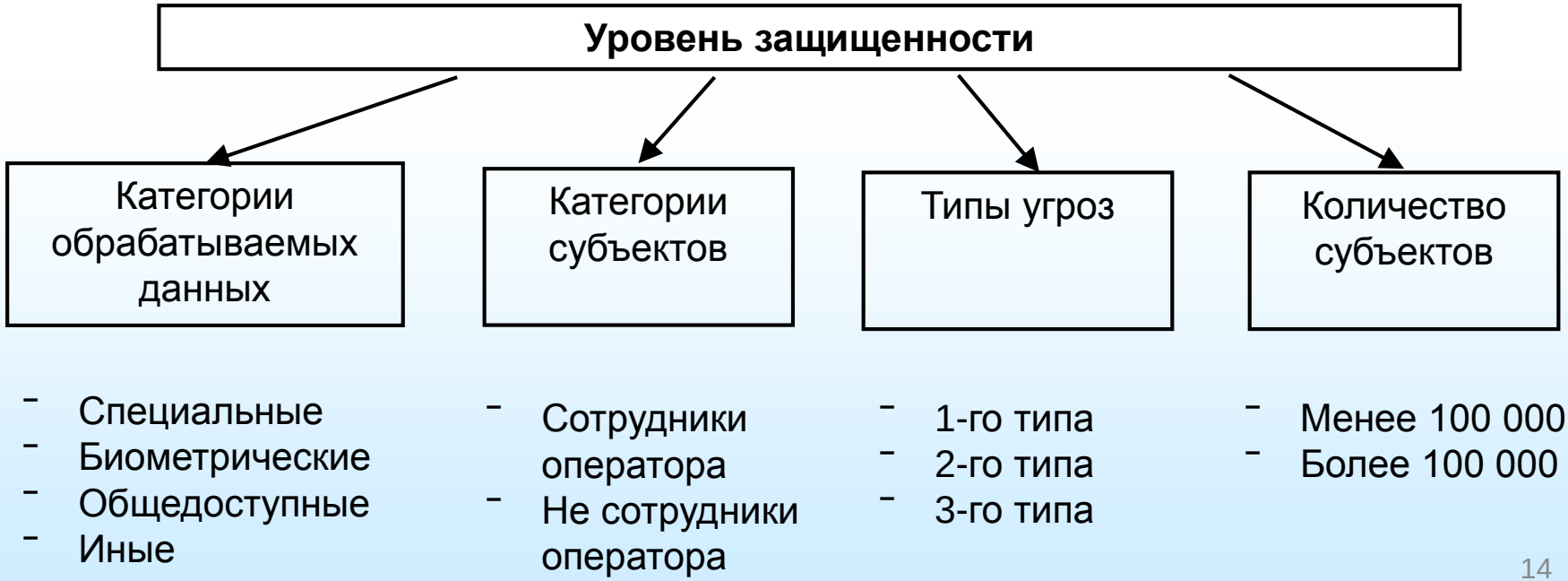
Информационное сообщение ФСТЭК России от 15.07.2013 N 240/22/2637

- Ранее аттестованные информационные системы повторной аттестации (оценке эффективности) в связи с изданием указанных нормативных правовых актов не подлежат.
- Требования, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. N 17, распространяются на муниципальные информационные системы.
- Приказа ФСТЭК N 17 не отменяет действие СТР-К и "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования о защите информации"

1. Основные нормативные и методические документы ФСТЭК и ФСБ

Определение необходимых уровней защищённости персональных данных при их обработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объёма обрабатываемых в них персональных данных
(*ПП РФ № 1119 от 01. 11. 2012г.*)

Исходные данные для определения уровня защищенности



Типы угроз

- **1 типа** - актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе
- **2 типа** – если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе
- **3 типа** - если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе

В соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждёнными Постановлением Правительства РФ от 01.11.2012 № 1119, для ИСПДн актуальны угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Угрозы 1-го и 2-го типа не актуальны в связи с тем, что работа ИСПДн планируется на ***лицензионном*** *системном программного обеспечении, в защищённой информационной среде, созданной на основе* ***сертифицированных*** *средств защиты информации.*

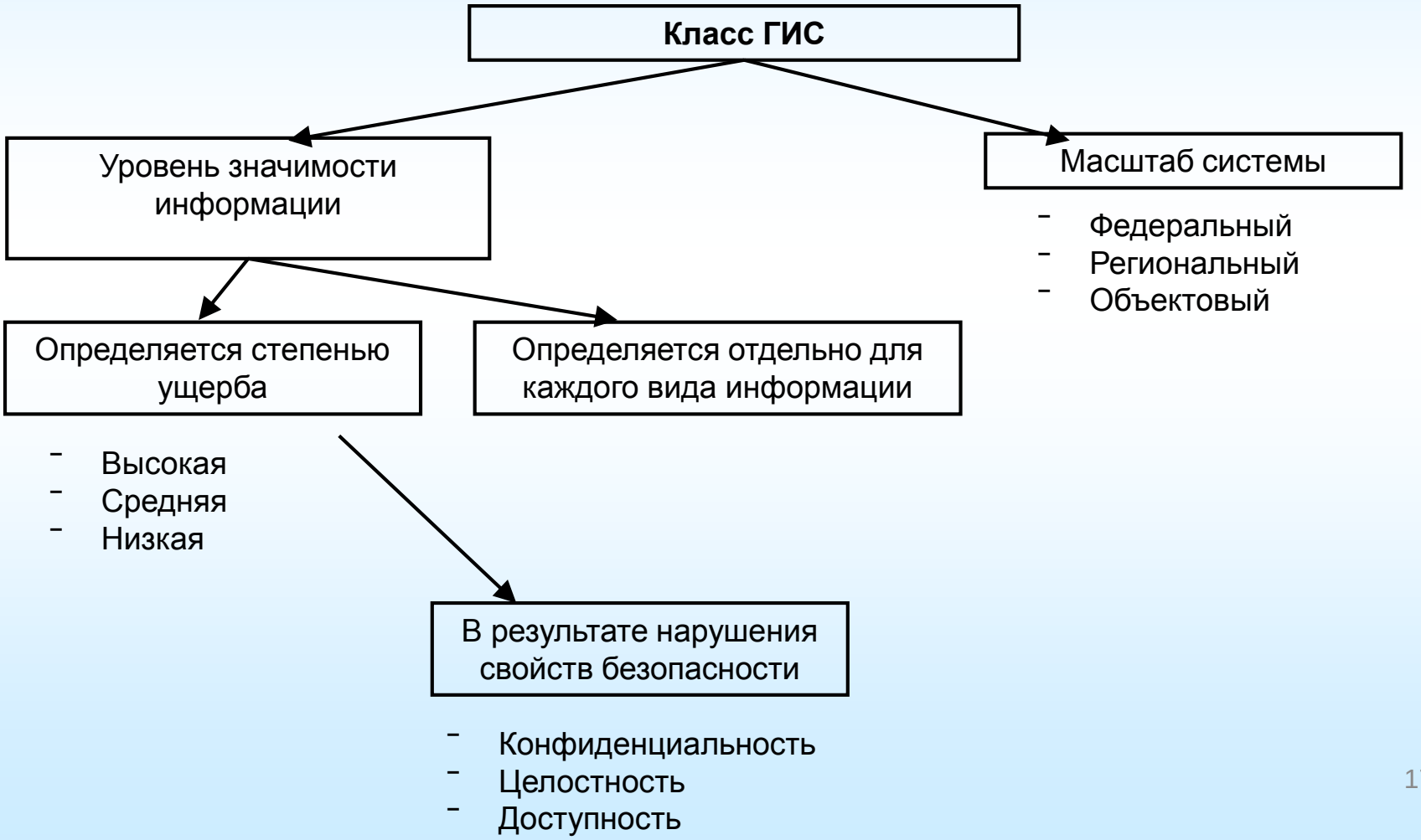
1. Основные нормативные и методические документы ФСТЭК и ФСБ

Определение уровня защищенности

Тип ИСПДн	Категория субъекта	Количество субъектов	Типы актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн-СК (Специальная)	Сотрудники	больше 100 тыс.	1 УЗ	2 УЗ	3 УЗ
		меньше 100 тыс.	1 УЗ	2 УЗ	3 УЗ
	Не сотрудники	больше 100 тыс.	1 УЗ	1 УЗ	2 УЗ
		меньше 100 тыс.	1 УЗ	2 УЗ	3 УЗ
ИСПДн-Б (Биометрия)	Сотрудники	больше 100 тыс.	1 УЗ	2 УЗ	3 УЗ
		меньше 100 тыс.	1 УЗ	2 УЗ	3 УЗ
	Не сотрудники	больше 100 тыс.	1 УЗ	2 УЗ	3 УЗ
		меньше 100 тыс.	1 УЗ	2 УЗ	3 УЗ
ИСПДн-О (Общедоступные)	Сотрудники	больше 100 тыс.	2 УЗ	3 УЗ	4 УЗ
		меньше 100 тыс.	2 УЗ	3 УЗ	4 УЗ
	Не сотрудники	больше 100 тыс.	2 УЗ	2 УЗ	4 УЗ
		меньше 100 тыс.	2 УЗ	3 УЗ	4 УЗ
ИСПДн-И (Иные)	Сотрудники	больше 100 тыс.	1 УЗ	3 УЗ	4 УЗ
		меньше 100 тыс.	1 УЗ	3 УЗ	4 УЗ
	Не сотрудники	больше 100 тыс.	1 УЗ	2 УЗ	3 УЗ
		меньше 100 тыс.	1 УЗ	3 УЗ	4 УЗ

1. Основные нормативные и методические документы ФСТЭК и ФСБ

Определение класса ГИС
(*Приложение 1 к Пр. №17 ФСТЭК России от 11.02.2013г.*)
Исходные данные для классификации ГИС



1. Основные нормативные и методические документы ФСТЭК и ФСБ

Определение уровня значимости информации

Свойства безопасности информации	Степень ущерба			
	Высокая	**Средняя**	**Низкая**	**Не определена**
Конфиденциальность	УЗ 1	УЗ 2, если нет Высокого и есть Средняя	УЗ 3, если везде Низкие	УЗ 4
Целостность				
Доступность				

1. Основные нормативные и методические документы ФСТЭК и ФСБ

Степени ущерба

1. **Высокая** степень ущерба – если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) **возможны существенные негативные последствия** в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор не могут выполнять возложенные на них функции.
2. **Средняя** степень ущерба – если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) **возможны умеренные негативные последствия** в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор не могут выполнять хотя бы одну из возложенных на них функций.
3. **Низкая** степень ущерба – если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности**) возможны незначительные негативные последствия** в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.
4. **Не определена** степень ущерба – если степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) **не может быть** определена, но при этом **информация подлежит защите** в соответствии с законодательством Российской Федерации.

Определение уровня значимости (для разных видов информации)

При обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации (УЗ) **определятся отдельно для каждого вида информации.**

Итоговый уровень значимости информации, обрабатываемой в информационной системе, устанавливается **по наивысшим значениям степени возможного ущерба**, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

Выбор масштаба информационной системы

- Информационная система имеет **федеральный масштаб,** если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

- Информационная система имеет **региональный масштаб,** если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

- Информационная система имеет **объектовый масштаб,** если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Выбор класса защищённости информационной системы

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ1	К1	К1	К1
УЗ2	К1	К2	К2
УЗ3	К2	К3	К3
УЗ 4	К3	К3	К4

Уточнение класса защищенности информационной системы

5. При обработке в **государственной** информационной системе информации, **содержащей персональные данные**, настоящие Требования применяются наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. **№1119** (Собрание законодательства Российской Федерации , 2012, N 45, ст. 6257).

1. Основные нормативные и методические документы ФСТЭК и ФСБ

Уточнение класса защищённости информационной системы

Класс защищенности ГИС	Уровень защищенности ИСПДн			
	1 УЗ	2 УЗ	3 УЗ	4 УЗ
К1	+	+	+	+
К2		+	+	+
К3			+	+
К4				+

Частная модель угроз

Разрабатывается на основе следующих документов:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России

- Методика оценки угроз безопасности информации. ФСТЭК России

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. ФСБ России

2. Лицензирование деятельности в области технической защиты информации

Федеральный закон от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

Статья. 3

… лицензия - специальное разрешение на право осуществления… конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим …

Статья. 2

Лицензирование отдельных видов деятельности осуществляется в целях предотвращения ущерба правам, законным интересам, жизни или здоровью граждан, окружающей среде, объектам культурного наследия …, обороне и безопасности государства, возможность нанесения которого связана с осуществлением …отдельных видов деятельности…. и регулирование которых не может осуществляться иными методами, кроме как лицензированием.

2. Лицензирование деятельности в области технической защиты информации

Лицензиат - юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.

Лицензируемый вид деятельности - вид деятельности, на осуществление которого на территории РФ требуется получение лицензии в соответствии с законодательством РФ.

Лицензионные требования и условия - совокупность установленных положениями о лицензировании конкретных видов деятельности требований и условий, выполнение которых лицензиатом обязательно при осуществлении лицензируемого вида деятельности;

Лицензирующие органы - федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом;

Реестр лицензий - совокупность данных о предоставлении лицензий, переоформлении документов, подтверждающих наличие лицензий, приостановлении и возобновлении действия лицензий и об аннулировании лицензии.

2. Лицензирование деятельности в области технической защиты информации

Федеральный закон от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

Статья 12 Перечень видов деятельности, на которые требуются лицензии

1) разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

….

5) деятельность по технической защите конфиденциальной информации;

2. Лицензирование деятельности в области технической защиты информации

Какие лицензируемые виды деятельности связаны с защитой конфи и ПДн?

2. Лицензирование деятельности в области технической защиты информации

ТЗКИ как лицензируемый вид деятельности

П. 2 Под **технической защитой конфиденциальной информации** понимается выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

«Положение о лицензировании деятельности по технической защите конфиденциальной информации» *Утверждено постановлением Правительства РФ от 3 февраля 2012 г. N 79*

- **Такая формулировка предполагает необходимость лицензии даже при деятельности по защите конфиденциальной информации для своих нужд**

Получение юрлицом лицензии ФСТЭК России является обязательным в следующих случаях. Деятельность организации направлена на получение прибыли от выполнения работ или оказания услуг по технической защите конфиденциальной информации. Она необходима для достижения целей деятельности, предусмотренных в учредительных документах юрлица. Организация обеспечивает техническую защиту конфиденциальной информации при ее обработке по поручению обладателя информации конфиденциального характера и (или) заказчика информационной системы.

Информационное сообщение ФСТЭК от 30 мая 2012 г. № 240/22/2222 **“По вопросу необходимости получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации”**

2. Лицензирование деятельности в области технической защиты информации

При осуществлении деятельности по технической защите конфиденциальной информации лицензированию подлежат следующие виды работ и услуг:

а) контроль защищенности конфиденциальной информации от утечки по техническим каналам в:

- средствах и системах информатизации;
- технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;
- помещениях со средствами (системами), подлежащими защите;
- помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);

б) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

в) сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации);

2. Лицензирование деятельности в области технической защиты информации

При осуществлении деятельности по технической защите конфиденциальной информации лицензированию подлежат следующие виды работ и услуг (продолжение):

г) аттестационные испытания и аттестация на соответствие требованиям по защите информации:
средств и систем информатизации;
помещений со средствами (системами) информатизации, подлежащими защите;
защищаемых помещений;

д) проектирование в защищенном исполнении:
средств и систем информатизации;
помещений со средствами (системами) информатизации, подлежащими защите;
защищаемых помещений;

е) **установка**, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, **программных (программно-технических) средств защиты информации**, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

2. Лицензирование деятельности в области технической защиты информации

Лицензионные требования

а) наличие в штате соискателя лицензии (лицензиата) **специалистов**, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;

б) наличие у соискателя лицензии (лицензиата) **помещений** для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему на праве собственности или на ином законном основании;

в) наличие на любом законном основании производственного, испытательного и контрольно-измерительного **оборудования**, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;

г) использование **автоматизированных систем**, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;

д) использование предназначенных для осуществления лицензируемой деятельности **программ** для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;

е) наличие нормативных правовых актов, нормативно-методических и методических **документов** по вопросам технической защиты информации в соответствии с перечнем, установленным Федеральной службой по техническому и экспортному контролю.

Лицензирование деятельности, связанной с шифровальными (криптографическими) средствами

Постановление Правительства РФ от 16.04.2012 N 313

"Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств **(за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя),** осуществляемой юридическими лицами и индивидуальными предпринимателями”

Лицензирование деятельности, связанной с шифровальными (криптографическими) средствами

Постановление Правительства РФ от 16.04.2012 N 313 содержит следующие сведения:

1) Что относится к шифровальным (криптографическим) средствам (средствам криптографической защиты информации).

2) На какую деятельность не распространяется данное Положение.

3) Перечень выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств.

4) Лицензионными требованиями при осуществлении лицензируемой деятельности.

5) Порядок лицензирования и контроля лицензионной деятельности.

2. Лицензирование деятельности в области технической защиты информации

Перечень выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств

1. Разработка шифровальных (криптографических) средств (ШКС).
2. Разработка защищённых с использованием ШКС информационных систем.
3. Разработка защищённых с использованием ШКС телекоммуникационных систем.
4. Разработка средств изготовления ключевых документов.
5. Модернизация ШКС.
6. Модернизация средств изготовления ключевых документов.
7. Производство (тиражирование) ШКС.
8. Производство защищённых с использованием ШКС информационных систем.
9. Производство защищённых с использованием ШКС телекоммуникационных систем.
10. Производство средств изготовления ключевых документов.
11. Изготовление с использованием ШКС изделий, предназначенных для подтверждения прав (полномочий) доступа к информации и (или) оборудованию в информационных и телекоммуникационных системах.
12. Монтаж, установка (инсталляция), наладка ШКС.
13. Монтаж, установка (инсталляция), наладка защищённых с использованием ШКС информационных систем.
14. Монтаж, установка (инсталляция), наладка защищённых с использованием ШКС телекоммуникационных систем.
15. Монтаж, установка (инсталляция), наладка средств изготовления ключевых документов.
16. Ремонт ШКС.
17. Ремонт, сервисное обслуживание защищённых с использованием ШКС информационных систем.

2. Лицензирование деятельности в области технической защиты информации

Перечень выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств (продолжение)

18. Ремонт, сервисное обслуживание защищённых с использованием ШКС телекоммуникационных систем.
19. Ремонт, сервисное обслуживание средств изготовления ключевых документов.
20. Работы по обслуживанию ШКС, предусмотренные технической и эксплуатационной документацией на эти средства **(за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)**.
21. Передача ШКС.
22. Передача защищённых с использованием ШКС информационных систем.
23. Передача защищённых с использованием ШКС телекоммуникационных систем.
24. Передача средств изготовления ключевых документов.
25. Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием ШКС в интересах юридических и физических лиц, а также индивидуальных предпринимателей.
26. Предоставление услуг по имитозащите информации, не содержащей сведений, составляющих государственную тайну, с использованием ШКС в интересах юридических и физических лиц, а также индивидуальных предпринимателей.
27. Предоставление юридическим и физическим лицам защищённых с использованием ШКС каналов связи для передачи информации.
28. Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для ШКС.

Лицензионные требования на деятельность по техническому обслуживанию СКЗИ

а) наличие у соискателя лицензии (лицензиата) права собственности или иного законного основания на владение и использование помещений, сооружений, **технологического, испытательного, контрольно-измерительного оборудования и иных объектов**, необходимых для осуществления лицензируемой деятельности;

б) выполнение соискателем лицензии (лицензиатом) при осуществлении лицензируемой деятельности требований по обеспечению информационной безопасности, устанавливаемых в соответствии со статьями 11.2 и 13 Федерального закона "О федеральной службе безопасности";

в) наличие у соискателя лицензии (лицензиата) условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг, составляющих лицензируемую деятельность, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом "Об информации, информационных технологиях и о защите информации";

г) наличие у соискателя лицензии (лицензиата) допуска к выполнению работ и оказанию услуг, связанных с использованием сведений, составляющих государственную тайну (при выполнении работ и оказании услуг, указанных в пунктах 1, 4 - 6, 16 и 19 перечня);

д) наличие в штате у соискателя лицензии (лицензиата) следующего квалифицированного **персонала**:

Лицензионные требования на деятельность по техническому обслуживанию СКЗИ (продолжение)

Руководитель и (или) лицо, уполномоченное руководить работами в рамках лицензируемой деятельности, имеющие высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по одной из специальностей этого направления **(нормативный срок - свыше 1000 аудиторных часов),** а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности **не менее 5 лет** (только для работ и услуг, указанных в пунктах 1, 4 - 6, 16 и 19 перечня);

руководитель и (или) лицо, уполномоченное руководить работами в рамках лицензируемой деятельности, имеющие высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по одной из специальностей этого направления **(нормативный срок - свыше 500 аудиторных часов)**, а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности **не менее 3 лет** (только для работ и услуг, указанных в пунктах 2, 3, 7 - 15, 17, 18, 20, 25 - 28 перечня);

руководитель и (или) лицо, уполномоченное руководить работами в рамках лицензируемой деятельности, имеющие высшее или среднее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по одной из специальностей этого направления **(нормативный срок - свыше 100 аудиторных часов)** (только для работ и услуг, указанных в пунктах 21 - 24 перечня);

Лицензионные требования на деятельность по техническому обслуживанию СКЗИ (продолжение)

инженерно-технические работники (минимум 2 человека), имеющие высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по одной из специальностей этого направления **(нормативный срок - свыше 1000 аудиторных часов),** а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности **не менее 5 лет** (только для работ и услуг, указанных в пунктах 1, 4 - 6, 16 и 19 перечня);

инженерно-технический работник (минимум 1 человек), имеющий высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедший переподготовку по одной из специальностей этого направления **(нормативный срок - свыше 500 аудиторных часов**), а также имеющий стаж в области выполняемых работ в рамках лицензируемой деятельности **не менее 3 лет** (только для работ и услуг, указанных в пунктах 2, 3, 7 - 15, 17, 18, 20, 25 - 28 перечня);

инженерно-технический работник, имеющий высшее или среднее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей (только для работ и услуг, указанных в пунктах 21 - 24 перечня);

Лицензионные требования на деятельность по техническому обслуживанию СКЗИ (продолжение)

е) наличие у соискателя лицензии **приборов и оборудования, прошедших поверку и калибровку в соответствии с Федеральным** законом "Об обеспечении единства измерений", **принадлежащих ему на праве собственности или ином законном основании** и необходимых для выполнения работ и оказания услуг, указанных в пунктах 1 - 11, 16 - 19 перечня;

ж) представление соискателем лицензии (лицензиатом) в лицензирующий орган перечня шифровальных (криптографических) средств, в том числе иностранного производства, не имеющих сертификата Федеральной службы безопасности Российской Федерации, технической документации, определяющей состав, характеристики и условия эксплуатации этих средств, и (или) образцов шифровальных (криптографических) средств;

з) использование соискателем лицензии (лицензиатом) предназначенных для осуществления лицензируемой деятельности **программ для электронных вычислительных машин и баз данных, принадлежащих соискателю лицензии (лицензиату) на праве собственности или ином законном основании**.

2. Лицензирование деятельности в области технической защиты информации

Примеры лицензий ФСБ И ФСТЭК

СЕРИЯ КИ 0061 НОМЕР 003024

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 1117 от 27 мая 2010 г.

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

Лицензия предоставлена Обществу с ограниченной ответственностью «Поволжский экспертно-аттестационный центр «ЮРАТЭКС»

(ООО «ЮРАТЭКС»)

ОГРН 1087325006174, ИНН 7325081862

Адрес места нахождения:

432063, г. Ульяновск, ул. Дмитрия Ульянова, д. 9

Адрес места осуществления лицензируемой деятельности:

432063, г. Ульяновск, ул. Дмитрия Ульянова, д. 9, стр. 1

Лицензия предоставлена на срок до 27 мая 2015 г.

на основании приказа ФСТЭК России от 27 мая 2010 г. № 293

Первый заместитель директора

М.П. В.Селин

Центр по лицензированию, сертификации и защите государственной тайны ФСБ России

(наименование лицензирующего органа)

ЛИЦЕНЗИЯ

ЛЗ № 0024130 Рег. № 10846 П от „ 27 “ июня 2011 г.

На осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

(указывается конкретный вид лицензируемой деятельности)

Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности (в отношении видов деятельности, указанных в пункте 2, статьи 17 Федерального закона „О лицензировании отдельных видов деятельности“): Условия действия лицензии см. на обороте бланка лицензии.

(указываются в соответствии с перечнем работ (услуг) установленным положением о лицензировании конкретного вида деятельности)

Настоящая лицензия предоставлена федеральному научно-производственному центру открытому акционерному обществу «Научно-производственное объединение «Марс» (ФНПЦ ОАО «НПО «Марс»)

(указывается полное и сокращенное наименование (в случае, если имеется), в том числе фирменное наименование и организационно-правовая форма юридического лица (ф., и., о. индивидуального предпринимателя, данные документа, удостоверяющего его личность)

Основной государственный регистрационный номер записи о государственной регистрации юридического лица или индивидуального предпринимателя 1067328003027

Идентификационный номер налогоплательщика 7303026811

Место нахождения и места осуществления лицензируемого вида деятельности

432022, г. Ульяновск, ул. Солнечная, д. 20

(указывается адрес места нахождения (место жительства – для индивидуального предпринимателя)

432022, г. Ульяновск, ул. Солнечная, д. 20

и адреса мест осуществления лицензируемого вида деятельности)

Настоящая лицензия предоставлена на срок до „ 27 “ июня 2016 г.

на основании решения лицензирующего органа от „ 27 “ июня 2011 г.

№ 8/ЛЗ/2/2-2172

Начальник Центра (подпись уполномоченного лица) Н.И.Умерников (ф., и., о. уполномоченного лица)

М.П.

Действие настоящей лицензии продлено на срок до „ “ г.

на основании решения лицензирующего органа от „ “ г.

№

(должность уполномоченного лица) (подпись уполномоченного лица) (ф., и., о. уполномоченного лица)

М.П.

МПФГ, Москва, 2006, „5“

3. Сертификация средств защиты информации

использование средств защиты информации, прошедших процедуру **оценки соответствия** требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз

ПП 1119 от 01.11.2012 г.

№ 184-ФЗ от 27.12.2002 О техническом регулировании

Технические регламенты (ТР)

- ТР имеет силу закона
- устанавливает обязательное применение и исполнение требований к объектам технического регулирования
- должен содержать перечень и описание объектов тех. регулирования, требования к ним, правила и формы **оценки соответствия**

До вступления в силу соответствующего ТР действуют существующие нормы

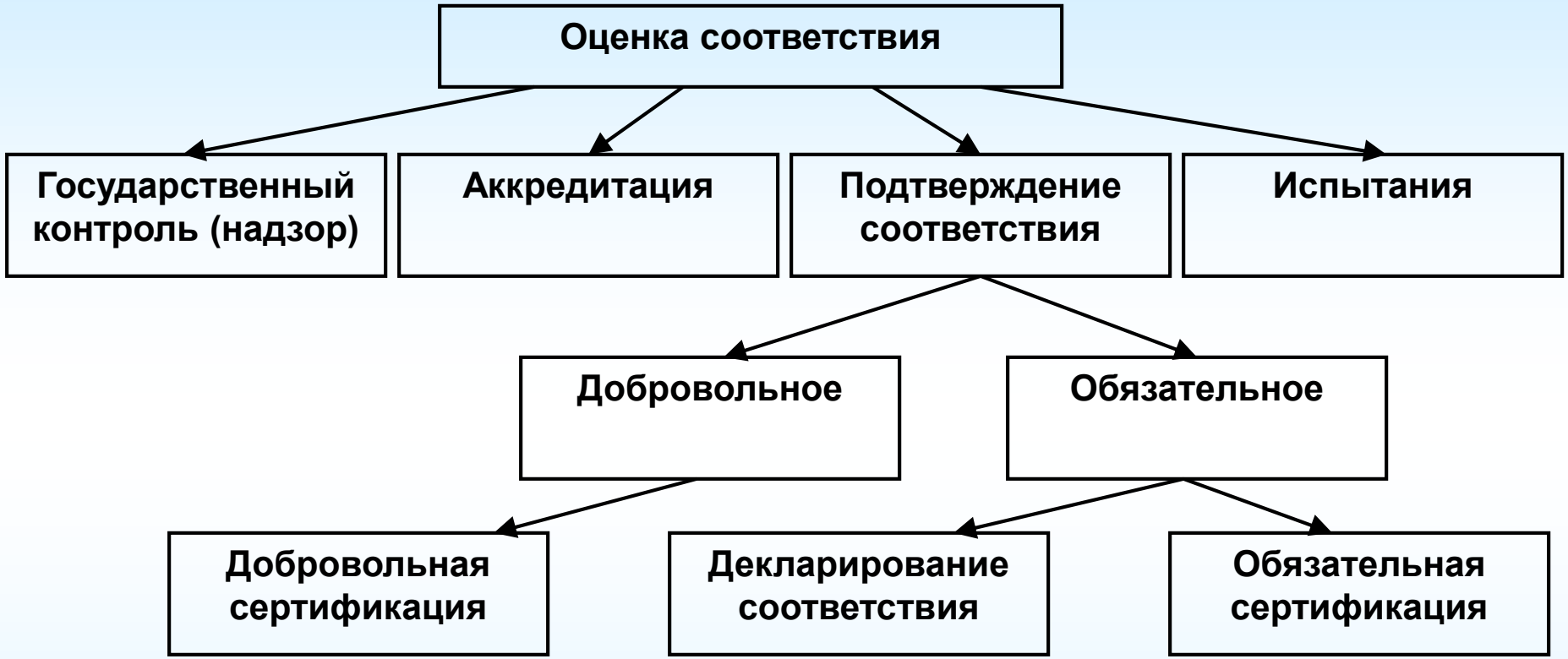
Положение о сертификации средств защиты информации. Утв. ПП-608 от 26.06.1995 г.

Положение о сертификации СЗИ по требованиям безопасности информации. Утв. председателем Гостехкомиссии от 27.10.1995 г.

Положение об особенностях оценки соответствия продукции (работ, услуг) используемой в целях защиты конфиденциальной информации. ПП-330 от 15.05.2010

3. Сертификация средств защиты информации

Сертификация – форма подтверждения соответствия



Сертификация – форма подтверждения соответствия объектов требованиям технических регламентов (184-ФЗ)

Сертификация СЗИ - деятельность по подтверждению соответствия требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Гостехкомиссией России.

(Положение о сертификации СЗИ по требованиям безопасности информации. Утв. председателем Гостехкомиссии от 27.10.1995 г.)

3. Сертификация средств защиты информации

Обязательность использования сертифицированных СЗИ

Выдержки из «Требований о защите информации, …» утв. Приказом ФСТЭК РФ №17

п.11 «Для обеспечения **защиты информации,** содержащейся в информационной системе**, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на** соответствие требованиям по безопасности информации …»

п.15.1 осуществляется выбор средств защиты информации, **сертифицированных на соответствие требованиям по безопасности информации**, с учётом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищённости информационной системы;

При отсутствии необходимых **средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации**, организуется разработка (доработка) средств защиты информации **и их сертификация** … или производится корректировка проектных решений по информационной системе и (или) ее системе защиты информации с учётом функциональных возможностей имеющихся сертифицированных средств защиты информации.

3. Сертификация средств защиты информации

Структура системы сертификации в РФ

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам (далее именуется - система сертификации).

Участниками сертификации средств защиты информации являются:

- федеральный орган по сертификации (ФСТЭК);
- центральный орган системы сертификации (создаваемый при необходимости) - орган, возглавляющий систему сертификации однородной продукции;
- органы по сертификации средств защиты информации - органы, проводящие сертификацию определённой продукции;
- испытательные лаборатории - лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определённой продукции;
- изготовители - продавцы, исполнители продукции.

3. Сертификация средств защиты информации

Центральный орган системы сертификации

- организует работы по формированию системы сертификации и руководство ею, координирует деятельность органов по сертификации средств защиты информации и испытательных лабораторий, входящих в систему сертификации;
- ведет учет входящих в систему сертификации органов по сертификации средств защиты информации и испытательных лабораторий, выданных и аннулированных сертификатов и лицензий на применение знака соответствия;
- обеспечивает участников сертификации информацией о деятельности системы сертификации.

3. Сертификация средств защиты информации

Органы по сертификации средств защиты информации:

сертифицируют средства защиты информации, выдают сертификаты и лицензии на применение знака соответствия с представлением копий в федеральные органы по сертификации и ведут их учет;

приостанавливают либо отменяют действие выданных ими сертификатов и лицензий на применение знака соответствия;

принимают решение о проведении повторной сертификации при изменениях в технологии изготовления и конструкции (составе) сертифицированных средств защиты информации;

формируют фонд нормативных документов, необходимых для сертификации;

представляют изготовителям по их требованию необходимую информацию в пределах своей компетенции.

3. Сертификация средств защиты информации

Испытательные лаборатории

Испытательные лаборатории проводят сертификационные испытания средств защиты информации и по их результатам оформляют заключения и протоколы, которые направляют в соответствующий орган по сертификации средств защиты информации и изготовителям.

Испытательные лаборатории несут ответственность за полноту испытаний средств защиты информации и достоверность их результатов.

3. Сертификация средств защиты информации

Изготовители

производят (реализуют) средства защиты информации только при наличии сертификата;

извещают орган по сертификации, проводивший сертификацию, об изменениях в технологии изготовления и конструкции (составе)сертифицированных средств защиты информации;

маркируют сертифицированные средства защиты информации знаком соответствия в порядке, установленном для данной системы сертификации;

указывают в сопроводительной технической документации сведения о сертификации и нормативных документах, которым средства защиты информации должны соответствовать, а также обеспечивают доведение этой информации до потребителя;

применяют сертификат и знак соответствия, руководствуясь законодательством Российской Федерации и правилами, установленными для данной системы сертификации;

обеспечивают соответствие средств защиты информации требованиям нормативных документов по защите информации;

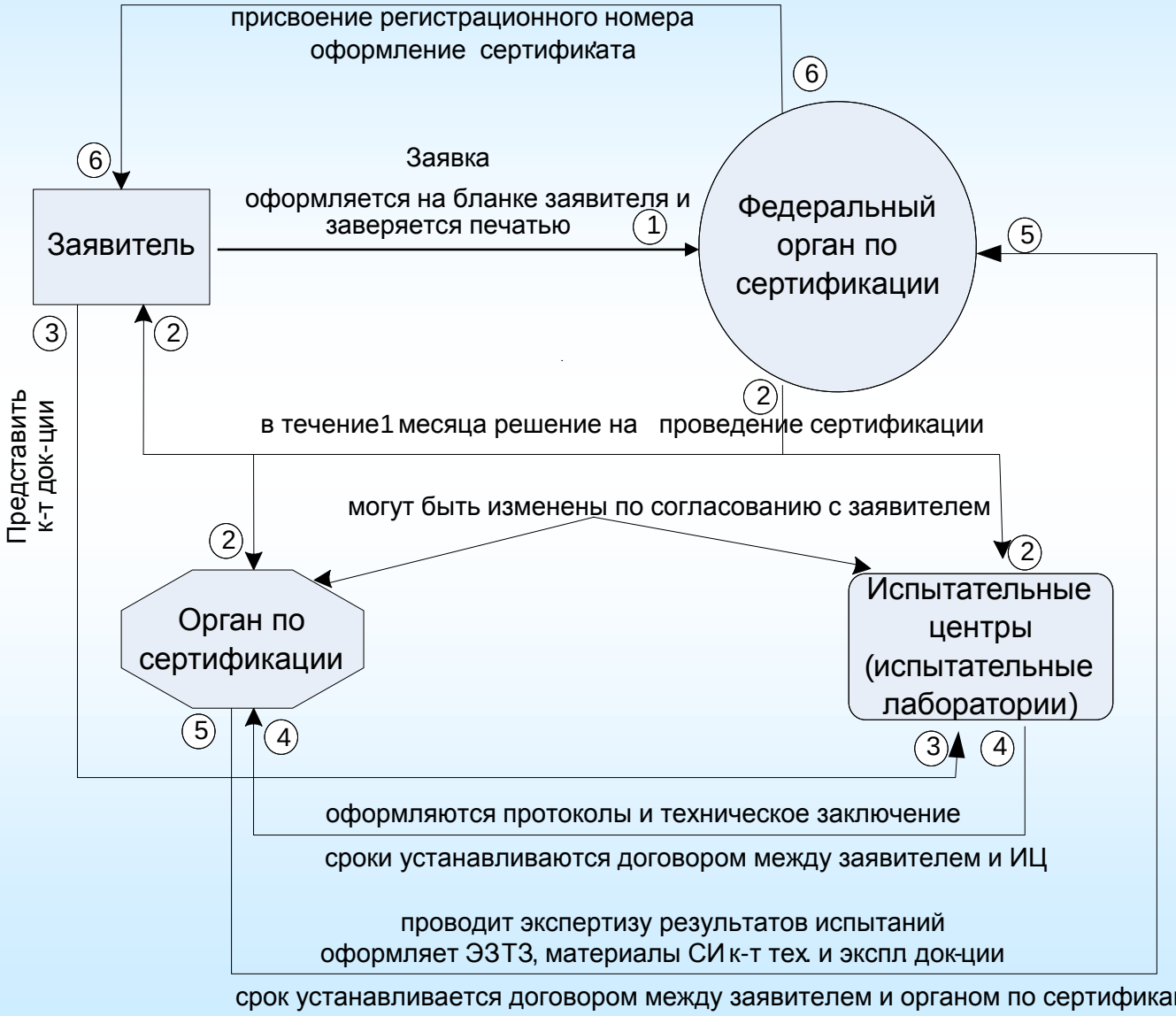
обеспечивают беспрепятственное выполнение своих полномочий должностными лицами органов, осуществляющих сертификацию, и контроль за сертифицированными средствами защиты информации;

прекращают реализацию средств защиты информации при несоответствии их требованиям нормативных документов или по истечении срока действия сертификата, а также в случае приостановки действия сертификата или его отмены.

Изготовители должны иметь лицензию на соответствующий вид деятельности.

3. Сертификация средств защиты информации

Порядок проведения сертификации



3. Сертификация средств защиты информации

Основными схемами сертификации средств защиты информации

- для единичных образцов средств защиты информации – проведение Испытаний образца на соответствие требованиям по безопасности информации;
- для партии средств защиты информации - проведение испытаний репрезентативной выборки образцов средств на соответствие требованиям по безопасности информации;
- для серийного производства средств защиты информации - проведение типовых испытаний образцов продукции на соответствие требованиям по безопасности информации и последующий инспекционный контроль за стабильностью характеристик сертифицированной продукции, обеспечивающих (определяющих) выполнение этих требований.

Кроме того, по решению федерального органа по сертификации допускается предварительная проверка **(аттестация)** производства по утверждённой программе

Особенности сертификации

• Реестр сертификатов на официальном сайте ФСТЭК.

• Сертификация может проводится в отношении одного изделия, партии или производства в целом.

• Сертификация проводится органами по сертификации и испытательными лабораториями (их количество 8 и 44 соответственно), следовательно, лучше ориентироваться на СЗИ с сертифицированным производством.

• Сертификация может быть различной – на НДВ, РД, ОУД, ТУ. Проще, когда в сертификате сразу говорится, что СЗИ может использоваться в ИСПДн такого-то класса.

• Внимательно читайте сертификат. В нем могут быть оговорены условия, при которых он действителен.

• Сертификат имеет ограниченный срок действия (3 года) и должен своевременно продляться.

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 640

Выдан 27 июня 2002 г.
Действителен до 28 марта 2008 г.
Продлен до 28 марта 2011 г.

Настоящий сертификат удостоверяет, что **система защиты информации «Secret Net 2000» версии 4.0 (автономный вариант)**, функционирующая под управлением ОС MS Windows 2000 и изготавливаемая ЗАО «Научно-инженерное предприятие «ИНФОРМЗАЩИТА» в соответствии с техническими условиями УВАЛ 00300-46 ТУ, является программным средством защиты от несанкционированного доступа к информации и соответствует требованиям руководящих документов «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999 г.) - по **3** уровню контроля, и «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по **3** классу защищенности при условии соблюдения ограничений, приведенных в приложении к настоящему сертификату.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Центр безопасности информации» (аттестат аккредитации от 23.05.1997 № СЗИ RU.117.Б08.025) – техническое заключение от 20.06.2002, экспертного заключения Гостехкомиссии России от 26.06.2002 и результатов инспекционного контроля, проведенного испытательной лабораторией ООО «Центр безопасности информации» – техническое заключение от 18.02.2008.

Заявитель: ЗАО «Научно-инженерное предприятие «ИНФОРМЗАЩИТА»
Адрес: 129010, г. Москва, Протопоповский пер., д. 19, стр. 10, корп. 14
Телефон: (495) 937-3385

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанных в настоящем сертификате руководящих документов и технических условий осуществляется испытательной лабораторией ООО «Центр безопасности информации».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

А.Гапонов

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
27 июня 2002 г.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2110

Выдан 9 июня 2010 г.
Действителен до 9 июня 2013 г.

Настоящий сертификат удостоверяет, что **программный комплекс iPension 8.01** (партия из 150 (ста пятидесяти) экземпляров продукции с серийными номерами с № 001 по № 150, маркированных знаками соответствия с № Г 151390 по № Г 151539) производства ООО «ЭСОНА» является программным средством обработки информации, не содержащей сведений, составляющих государственную тайну, функционирующим под управлением операционных систем Microsoft Windows 2000/XP/2003/2008, и 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 **4** уровню контроля.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «Научно-Производственное Объединение «Эшелон» (аттестат аккредитации от 03.06.2009 № СЗИ RU.2321.Б011.033) – техническое заключение от 02.04.2010, и экспертного заключения от 22.04.2010 органа по сертификации ОАО «Безопасность информационных технологий и компонентов» (аттестат аккредитации от 21.11.2008 № СЗИ RU.1190.А98.011).

Заявитель: МОУ «Институт инженерной физики»
Адрес: 142210, Московская обл., г. Серпухов, Большой Ударный пер., д. 1А
Телефон: (4967) 35-3193

Маркирование знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям указанного в настоящем сертификате руководящего документа осуществляется испытательной лабораторией ЗАО «Научно-Производственное Объединение «Эшелон».

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Селин

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 9 июня 2010 г.