

Министерство образования и науки Российской Федерации  
Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
«Российский экономический университет имени Г. В. Плеханова»  
(ФГБОУ ВО «РЭУ им. Г. В. Плеханова»)

**Ю. Н. Сычев**

**Стандарты информационной безопасности.  
Защита и обработка конфиденциальных  
документов**

Утверждено издательским советом университета  
в качестве учебного пособия

Москва  
ФГБОУ ВО «РЭУ им. Г. В. Плеханова»  
2017

УДК 005.922.1(075.8)  
ББК 60.844я73  
С958

*Рецензенты:* д-р техн. наук М. М. Т а р а с к и н (МИНИТ ФСБ России); канд. техн. наук В. В. К р е о п а л о в (РЭУ им. Г. В. Плеханова)

**Сычев, Ю. Н.**

С958      Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю. Н. Сычев. – Москва: ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2017. – 207 с.  
ISBN 978-5-7307-1148-8

Специалистам в области информационной безопасности в настоящее время невозможно обойтись без знания международных и национальных стандартов. Необходимость применения требований криптографических стандартов, Руководящих документов Гостехкомиссии России закреплена законодательно. Помимо этого, во всех стандартах зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами в своей области. Стандарты являются основой обеспечения взаимной совместимости информационных, аппаратно-программных систем и их компонентов. Учебное пособие отличается качеством изложения теоретического материала. В нем чувствуется четкость и продуманность структуры и содержания. Материал представлен по этапам создания стандартов, т. е. с учетом развития информационного общества.

Для студентов, обучающихся по направлению 10.03.01 «Информационная безопасность», профиль «Безопасность автоматизированных систем».

В учебных целях стандарты и руководящие документы приведены автором в неполном объеме и в измененном виде.

УДК 005.922.1(075.8)  
ББК 60.844я73

ISBN 978-5-7307-1148-8

© ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2017

## ОГЛАВЛЕНИЕ

Глава 1. СТАНДАРТИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	6
Глава 2. БРИТАНСКИЕ И МЕЖДУНАРОДНЫЕ СТАНДАРТЫ	
2.1. БРИТАНСКИЙ СТАНДАРТ BS 7799 .....	14
2.1.1. Британский стандарт BS 7799-1 «Информационная технология. Практический кодекс по менеджменту информационной безопасности» .....	16
2.1.2. Британский стандарт BS 7799-2 «Управление информационной безопасностью. Практические правила» .....	17
2.1.3. Британский стандарт BS 7799-3 26«Руководство по управлению рисками информационной безопасности» .....	26
2.2. МЕЖДУНАРОДНЫЙ СТАНДАРТ ISO/IEC 17799 «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ТЕХНОЛОГИИ БЕЗОПАСНОСТИ. ПРАКТИЧЕСКИЕ ПРАВИЛА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».....	31
2.3. СЕМЕЙСТВО МЕЖДУНАРОДНЫХ СТАНДАРТОВ ISO/IEC 27000.....	34
2.3.1. Международный стандарт ISO/IEC 27001 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования».....	38
2.3.2. Международный стандарт ISO/IEC 27002 «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности» .....	40
Глава 3. НАЦИОНАЛЬНЫЕ СТАНДАРТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
3.1. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р 50922-2006 «ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ» .....	44

3.2. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ Р 50.1.053-2005 «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ» .....	52
3.1. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р 51188-1998 «ЗАЩИТА ИНФОРМАЦИИ. ИСПЫТАНИЕ ПРОГРАММНЫХ СРЕДСТВ НА НАЛИЧИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ» .....	59
3.2. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р 51275-2006 «ЗАЩИТА ИНФОРМАЦИИ. ОБЪЕКТ ИНФОРМАТИЗАЦИИ. ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ. ОБЩИЕ ПОЛОЖЕНИЯ» .....	69
3.5. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р ИСО/МЭК 15408-2008 «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ» .....	77
3.5.1. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» .....	81
3.5.2. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» .....	93
3.5.3. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности» .....	106
3.6. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р ИСО/МЭК 17799-2005 «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ» .....	111

3.7. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р ИСО/МЭК 27001-2006 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».....	119
Глава 4. РУКОВОДЯЩИЕ ДОКУМЕНТЫ ГОСТЕХКОМИССИИ РОССИИ	
4.1. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	127
4.2. КОНЦЕПЦИЯ ЗАЩИТЫ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (НСД) К ИНФОРМАЦИИ.....	131
4.3. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ .....	132
4.4. СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ.....	160
4.5. ВРЕМЕННОЕ ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ РАЗРАБОТКИ, ИЗГОТОВЛЕНИЯ И ЭКСПЛУАТАЦИИ ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ И СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ.....	177
Глава 5. ЗАЩИТА И ОБРАБОТКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ	
5.1. ВИДЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ .....	180
5.2. ПОРЯДОК ОБРАЩЕНИЯ С КОНФИДЕНЦИАЛЬНЫМИ ДОКУМЕНТАМИ.....	192
СОКРАЩЕНИЯ .....	198
КОНТРОЛЬНЫЕ ВОПРОСЫ.....	200
СПИСОК ЛИТЕРАТУРЫ .....	204

## Глава 1. СТАНДАРТИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Стандартизация* – деятельность по разработке, опубликованию и применению стандартов, по установлению норм, правил и характеристик в целях обеспечения безопасности продукции, работ и услуг для окружающей среды, жизни, здоровья и имущества, технической и информационной совместимости, взаимозаменяемости и качества продукции, работ и услуг в соответствии с уровнем развития науки, техники и технологии, единства измерений, экономии всех видов ресурсов, безопасности хозяйственных объектов с учетом риска возникновения природных и техногенных катастроф и других чрезвычайных ситуаций, обороноспособности и мобилизационной готовности страны.

Стандартизация направлена на достижение оптимальной степени упорядочения в определенной области посредством установления положений для всеобщего и многократного применения в отношении реально существующих или потенциальных задач.

За реализацию норм стандартизации отвечают органы и службы стандартизации, наделенные законным правом руководить разработкой и утверждать нормативные документы и другие правила, придавая им статус стандартов.

*Органы и службы стандартизации* – организации, учреждения, объединения и их подразделения, основной деятельностью которых является осуществление работ по стандартизации или выполнение определенных функций по стандартизации.

Руководство российской национальной стандартизацией осуществляет национальный орган по стандартизации – Федеральное агентство по техническому регулированию и метрологии – Ростехрегулирование. Оно имеет право представлять интересы страны в области стандартизации в международных или региональных организациях по стандартизации.

Ростехрегулирование осуществляет:

- принятие программы разработки национальных стандартов;
- утверждение национальных стандартов;
- учет национальных стандартов, правил стандартизации, норм и рекомендаций в этой области и обеспечение их доступности заинтересованным лицам;
- введение в действие общероссийских классификаторов технико-экономической и социальной информации.

Ростехрегулирование осуществляет свои функции непосредственно и через свои межрегиональные территориальные управления (МТУ), а также российские службы стандартизации.

В структуру Ростехрегулирования входят:

- Центральное межрегиональное территориальное управление (место расположения центрального аппарата территориального органа – Москва);
- Северо-Западное межрегиональное территориальное управление (место расположения центрального аппарата территориального органа – Санкт-Петербург);
- Южное межрегиональное территориальное управление (место расположения центрального аппарата территориального органа – Ростов-на-Дону);
- Приволжское межрегиональное территориальное управление (место расположения центрального аппарата территориального органа – Нижний Новгород);
- Уральское межрегиональное территориальное управление (место расположения центрального аппарата территориального органа – Екатеринбург);
- Сибирское межрегиональное территориальное управление (место расположения центрального аппарата территориального органа – Новосибирск);
- Дальневосточное межрегиональное территориальное управление (место расположения центрального аппарата территориального органа – Хабаровск).

*Службы стандартизации* – специально создаваемые организации и подразделения для проведения работ по стандартизации на определенных уровнях управления – государственном, отраслевом, предприятий (организации).

Российские службы стандартизации – научно-исследовательские институты Ростехрегулирования России и технические комитеты по стандартизации.

К научно-исследовательским институтам, например, относятся:

- НИИ стандартизации (ВНИИ стандарт) – головной институт в области национальной системы стандартизации;
- ВНИИ сертификации продукции (ВНИИС) – головной институт в области сертификации продукции (услуг) и систем управления качеством продукции (услуг);

– ВНИИ по нормализации в машиностроении (ВНИИНМАШ) – головной институт в области разработки научных основ унификации и агрегатирования в машиностроении и приборостроении;

– «Стандартинформ» – головной институт в области разработки и дальнейшего развития Единой системы классификации и кодирования технико-экономической информации, стандартизации научно-технической терминологии.

Технические комитеты по стандартизации (ТК) создаются на базе организаций, специализирующихся на определенных видах продукции (услуг) и имеющих в данной области наиболее высокий научно-технический потенциал. На сегодняшний день зарегистрировано свыше 350 ТК.

Стандарт – продукт согласованного мнения всех заинтересованных в этом документе сторон (пользователей).

Задача Технического комитета заключается в обеспечении «круглого стола» участников разработки проекта стандарта. Поэтому в состав этих ТК включают представителей разработчиков, изготовителей, поставщиков, потребителей (заказчиков) продукции, обществ (союзов) потребителей и других заинтересованных предприятий и организаций, а также ведущих ученых и специалистов в конкретной области. ТК несут ответственность за качество и сроки разрабатываемых ими проектов стандартов в соответствии с действующим законодательством и заключенными договорами на проведение этих работ.

Руководители предприятий непосредственно несут ответственность за организацию и состояние выполняемых работ по стандартизации на этих предприятиях. Предприятия создают при необходимости службы стандартизации (отдел, лабораторию, бюро), которые выполняют научно-исследовательские, опытно-конструкторские и другие работы по стандартизации.

Выделяют следующие ключевые задачи стандартизации:

– налаживание взаимопонимания между субъектами производственных процессов (разработчиками, промышленниками, продавцами, покупателями товаров и услуг);

– выработка оптимальных критериев стандартизации, отражающих особенности развития тех или иных отраслей или экономики в целом;

– содействие выработке предприятиями оптимальных схем доступа к необходимым ресурсам посредством внедрения стандартов,

отражающих применение тех или иных видов сырья, материалов, компонентов;

- унификация производственных процессов с целью повышения динамики масштабирования бизнесов (как результат – позитивный эффект в аспекте роста экономики);

- установление оптимальных норм в области метрологии (с целью оптимизации производственных цепочек как на национальном, так и на международном уровне);

- нормативное обеспечение процедур контроля, испытаний, измерений, исследования продукции на предмет качества;

- оптимизация технологических процессов с точки зрения трудоемкости, потребности в материалах, электроэнергии;

- содействие инвестиционной привлекательности национальных предприятий в аспекте повышения эффективности производства за счет оптимизации стандартов.

Стандарты нацелены на регулирование какой-либо конкретной части производственного процесса (предоставления услуг). В них также могут указываться критерии, имеющие, к примеру, отношение к терминологии каких-либо товаров или услуг. Данные документы разрабатываются на основе обобщенных научных исследований, инженерных работ, они аккумулируют в себе результаты практики производства (оказания услуг) в различных сферах экономики.

В соответствии с Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», все стандарты, применяемые в российской практике, имеют единообразный формат обозначения. Это означает, что в любой категории стандартов РФ структура соответствующих норм представлена в виде индекса, номера регистрации, а также года принятия. Например, ГОСТ Р 50597-93.

Целями стандартизации являются:

- повышение уровня безопасности жизни и здоровья граждан, имущества физических и юридических лиц, государственного и муниципального имущества;

- обеспечение конкурентоспособности и качества продукции (работ, услуг), единства измерений, рационального использования ресурсов – взаимозаменяемости технических средств (машин и оборудования, их составных частей, комплектующих изделий и материалов), технической и информационной совместимости, сопоставимости результатов исследований (испытаний) и измерений, технических и экономико-статистических данных, проведения анализа характеристик продукции (работ, услуг), исполнения государствен-

ных заказов, добровольного подтверждения соответствия продукции (работ, услуг);

- содействие соблюдению требований технических регламентов;
- создание систем классификации и кодирования технико-экономической и социальной информации, систем каталогизации продукции (работ, услуг), систем обеспечения качества продукции (работ, услуг), систем поиска и передачи данных, содействие проведению работ по унификации.

Выделяют следующие основные категории стандартов:

- международные;
- государственные стандарты РФ (ГОСТ Р);
- межгосударственные (ГОСТ);
- корпоративные (стандарты предприятий);
- отраслевые;
- издаваемые общественными объединениями.

Есть в мировой практике и другие категории. Например, региональные стандарты, применимые одновременно в нескольких странах, которые объединены по культурным или географическим признакам.

Государственные стандарты (или ГОСТы) всех типов – российские или межгосударственные – характеризуются обязательностью в аспекте применения предприятиями и организациями, деятельность которых попадает под положения соответствующих норм. ГОСТы в ряде случаев могут быть одним из критериев проведения сертификации предприятия.

Отраслевые стандарты (ОСТ) действуют в отношении конкретного сегмента экономики. Они также могут использоваться в качестве критериев при проведении сертификации.

С помощью стандартов предприятий (СТП) устанавливаются требования в отношении методов (или же процессов), которые характерны для тех или иных участков производства. В ряде случаев могут иметь схожесть в отдельных положениях с ГОСТами и ОСТами, однако, как правило, отражают частные особенности производственных процессов на конкретных предприятиях.

В ОСТах название нормы выглядит так же, как и в случае с ГОСТ, т. е. в виде последовательного обозначения индекса, регистрационного номера и года принятия.

### ***Классификация источников норм в стандартизации***

В России принята четырехуровневая схема организации национального фонда источников права в сфере стандартизации.

На первой ступени располагается техническое законодательство. Главный источник права здесь – Федеральный закон «О техническом регулировании». На данном уровне присутствуют законы и подзаконные правовые акты (постановления российского правительства, приказы различных ведомств и т. д.).

На втором уровне располагаются документы, в которых содержатся нормы, регулирующие производственные объекты и процессы. Это национальные и межгосударственные стандарты, различные классификаторы, рекомендации.

На третьем уровне – источники, содержащие в себе отраслевые стандарты, и те, которые создаются научно-техническими обществами.

На четвертом – источники, включающие стандарты предприятий, а также дополняющие и сопровождающие их нормы.

### ***Виды стандартов***

Основной фактор отнесения нормы к тому или иному виду (не только в российской, но и в мировой практике) – наличие специфики объекта нормирования. Выделяют несколько основных классов, в рамках которых можно ее определить. Так, в зависимости от специфики объекта нормирования, стандарты могут быть:

- основополагающими;
- ориентированными на продукцию (услуги);
- ориентированными на работу (процессы);
- адаптированными для методов контроля (в отношении испытаний, измерений или же, например, анализа).

Основополагающие стандарты регламентируют ключевые организационные аспекты, положения и нормы, которые являются общими в отношении разных сегментов производства, областей науки и техники. Стандарты, ориентированные на продукцию или услуги, устанавливают критерии для конкретных видов активностей на производстве (или в сервисах) – выпуск, эксплуатация, перевозка, ремонт и т. д.

### ***Требования к стандартам***

*Универсальность стандарта* – определяется множеством типов вычислительных систем и областью информационных технологий, к которым могут быть корректно применены его приложения.

*Гибкость стандарта* – возможность его применения к постоянно развивающимся информационным технологиям и время его «устаревания» (гибкость может быть достигнута исключительно через фундаментальность требований и критериев и их инвариантность по отношению к механизмам реализации и технологиям создания продукта информационных технологий).

*Гарантированность* – определяется мощностью предусмотренных стандартом методов и средств подтверждения надежности результатов квалификационного анализа.

*Реализуемость* – возможность адекватной реализации требований и критериев стандарта на практике с учетом затрат на этот процесс.

*Актуальность* – отражает соответствие требований и критериев стандарта постоянно развивающемуся множеству угроз безопасности, новейшим методам и средствам, используемым злоумышленниками.

### ***Стандарты информационной безопасности***

*Стандарты информационной безопасности* – это обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня информационной безопасности (ИБ) и установлены требования к безопасным информационным системам.

Стандарты в области ИБ выполняют следующие важнейшие функции:

- выработка понятийного аппарата и терминологии в области информационной безопасности;
- формирование шкалы измерений уровня информационной безопасности;
- согласованная оценка продуктов, обеспечивающих информационную безопасность;
- повышение технической и информационной совместимости продуктов, обеспечивающих информационную безопасность;
- накопление сведений о лучших практиках обеспечения информационной безопасности и их предоставление различным группам заинтересованной аудитории (производителям средств информационной безопасности, экспертам, ИТ-директорам, администраторам и пользователям информационных систем;

– функция нормотворчества – придание некоторым стандартам юридической силы и установление требования их обязательного выполнения.

Основными областями стандартизации ИБ являются:

- аудит информационной безопасности;
- модели информационной безопасности;
- методы и механизмы обеспечения информационной безопасности;
- криптография;
- безопасность межсетевых взаимодействий;
- управление информационной безопасностью.

Классификация стандартов информационной безопасности:

1. По странам разработчикам стандартов:

- международные;
- отечественные;
- зарубежные.

2. По выполнению:

- обязательные;
- рекомендуемые.

3. По доступности:

- общедоступные;
- распространяемые по лицензии.

Основные элементы системы ИБ:

- внешняя защита от несанкционированного доступа к системам;
- внутренняя защита от несанкционированного доступа к системам сотрудников организации;
- авторизация и аутентификация;
- защита каналов передачи данных, обеспечение целостности;
- обеспечение актуальности данных при обмене информацией с клиентами;
- управление электронным документооборотом;
- управление инцидентами ИБ;
- управление непрерывностью ведения бизнеса;
- внутренний и внешний аудит системы ИБ.

Необходимость следования стандартам информационной безопасности закреплена законодательно. Однако и добровольное выполнение стандартов очень эффективно, поскольку в них описаны наиболее качественные и опробованные методики и решения.

## **Глава 2. БРИТАНСКИЕ И МЕЖДУНАРОДНЫЕ СТАНДАРТЫ**

### **2.1. БРИТАНСКИЙ СТАНДАРТ BS 7799**

Родоначальником международных стандартов управления информационной безопасностью является британский стандарт BS 7799. Он постепенно стал главным стандартом информационной безопасности.

Первая его часть – BS 7799-1 «Практические правила управления информационной безопасностью» – была разработана BSI в 1995 г. по заказу Правительства Великобритании. Как следует из названия, этот документ является практическим руководством по управлению информационной безопасностью в организации.

Он описывает 10 областей и 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определенных на основе лучших примеров мирового опыта в данной области. Этот документ служит практическим руководством по созданию СУИБ. Стандарт в большинстве своем предназначался для определения норм безопасности при ведении коммерческой деятельности.

В 1998 г. появилась вторая часть этого британского стандарта – BS 7799-2 «Системы управления информационной безопасностью. Спецификация и руководство по применению», определившая общую модель построения СУИБ и набор обязательных требований, на соответствие которым должна производиться сертификация. С появлением второй части BS 7799, определившей, что должна из себя представлять СУИБ, началось активное развитие системы сертификации в области управления безопасностью.

Этот международный стандарт был подготовлен для того, чтобы предоставить модель для создания, внедрения, эксплуатации, мониторинга, пересмотра, сопровождения, совершенствования СУИБ.

Принятие СУИБ должно являться стратегическим решением для организации. На проектирование и внедрение СУИБ оказывают влияние:

- бизнес-цели и потребности организации, вытекающие из них требования безопасности;
- используемые процессы;
- размер и структура организации.

Эти факторы, а также поддерживающие их системы, предположительно, со временем будут изменяться. Ожидается, что реализация СУИБ будет масштабироваться в соответствии с потребностями организации, например, простая ситуация требует простого решения по построению СУИБ.

Этот международный стандарт может использоваться внутренними и внешними сторонами для оценки соответствия.

Вторая часть BS 7799 пересматривалась в 2002 г., а в конце 2005 г. была принята ISO в качестве международного стандарта ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования». В это же время была обновлена и первая часть стандарта.

В начале 2006 г. была принята третья часть британского национального стандарта в области управления рисками информационной безопасности BS 7799-3. «Руководство по управлению рисками информационной безопасности». Первые две части получили международное признание и представляют собой практические рекомендации по построению системы ИБ и оценочные требования (главным образом сертификационные) к СУИБ. Третья часть британского стандарта посвящена анализу, оценке и управлению рисками. К сожалению, несмотря на очевидную методологическую важность этой части стандарта BS 7799, в нашей стране она не получила должного внимания (таблица).

**Соответствие стандартов**

Британский стандарт	Международный стандарт	Российский стандарт
BS 7799-1:2005	ISO 27002:2007 (ISO 17799:2005)	ГОСТ 17799:2005
BS 7799-2:2005	ISO 27001:2005	ГОСТ 27001:2005
BS 7799-3:2006	ISO 27005	Отсутствует

### **2.1.1. Британский стандарт BS 7799-1 «Информационная технология. Практический кодекс по менеджменту информационной безопасности»**

Стандарт содержит систематический, весьма полный, универсальный перечень регуляторов безопасности, необходимый для организации практически любого размера, структуры и сферы деятельности. Он предназначен для использования в качестве справочного документа руководителями и сотрудниками, отвечающими за планирование, реализацию и поддержание внутренней системы информационной безопасности.

Согласно стандарту, цель информационной безопасности – обеспечить бесперебойную работу организации, по возможности предотвратить и / или минимизировать ущерб от нарушений безопасности.

Управление информационной безопасностью позволяет коллективно использовать данные, одновременно обеспечивая их защиту и защиту вычислительных ресурсов.

Подчеркивается, что защитные меры оказываются значительно более дешевыми и эффективными, если они заложены в информационные системы и сервисы на стадиях задания требований и проектирования.

Следующие факторы выделены в качестве определяющих для успешной реализации системы информационной безопасности в организации:

- цели безопасности и ее обеспечение должны основываться на производственных задачах и требованиях. Функции управления безопасностью должно взять на себя руководство организации;
- необходима явная поддержка и приверженность к соблюдению режима безопасности со стороны высшего руководства;
- требуется хорошее понимание рисков (как угроз, так и уязвимостей), которым подвергаются активы организации, и адекватное представление о ценности этих активов;
- необходимо ознакомление с системой безопасности всех руководителей и рядовых сотрудников организации.

В стандарте предлагаются регуляторы безопасности:

- политика безопасности;
- общеорганизационные аспекты защиты;
- классификация активов и управление ими;
- безопасность персонала;

- физическая безопасность и безопасность окружающей среды;
- администрирование систем и сетей;
- управление доступом к системам и сетям;
- разработка и сопровождение информационных систем;
- управление бесперебойной работой организации;
- контроль соответствия требованиям.

### **2.1.2. Британский стандарт BS 7799-2 «Управление информационной безопасностью. Практические правила»**

В стандарте предметом рассмотрения является система управления информационной безопасностью (СУИБ).

Под СУИБ понимается часть общей системы управления, базирующаяся на анализе рисков и предназначенная для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности. Эту систему составляют организационные структуры, политика, действия по планированию, обязанности, процедуры, процессы и ресурсы.

В основу процесса управления положена четырехфазная модель, включающая планирование; реализацию; оценку; корректировку.

Предлагаемые в первой части стандарта регуляторы безопасности разбиты на десять групп.

*Первая группа регуляторов безопасности* – политика безопасности. К ней относится:

- документально оформленная политика;
- процесс ревизии политики.

Цель регуляторов этой группы – определить стратегию управления безопасностью и обеспечить ее поддержку.

*Вторая группа регуляторов безопасности* касается общеорганизационных аспектов.

По сравнению с первой она более многочисленна и наделена внутренней структурой. Ее первая подгруппа – инфраструктура информационной безопасности, цель которой – управление безопасностью в организации. Она включает следующие регуляторы:

- создание сообщества по управлению информационной безопасностью;

- меры по координации действий в области информационной безопасности;
- распределение обязанностей в области информационной безопасности;
- утверждение руководством (административное и техническое) новых средств обработки информации;
- получение рекомендаций специалистов по информационной безопасности;
- сотрудничество с другими организациями (правоохранительными органами, поставщиками информационных услуг и т. д.);
- проведение независимого анализа информационной безопасности.

Регуляторы второй подгруппы – безопасность доступа сторонних организаций – предназначены для обеспечения безопасности вычислительных и информационных ресурсов, к которым имеют доступ сторонние организации. Этих регуляторов два:

1. Идентификация рисков, связанных с подключениями сторонних организаций, и реализация соответствующих защитных мер.
2. Выработка требований безопасности для включения в контракты со сторонними организациями.

*Третья группа регуляторов безопасности* имеет цель – обеспечение информационной безопасности при использовании услуг внешних организаций.

Предлагается выработать требования безопасности для включения в контракты с поставщиками информационных услуг.

Очень важна третья группа регуляторов безопасности как классификация активов и управление ими. Необходимым условием обеспечения надлежащей защиты активов является их идентификация и классификация. Должны быть выработаны критерии классификации, в соответствии с которыми активы тем или иным способом получают метки безопасности.

*Четвертая группа регуляторов безопасности* – безопасность персонала. Она охватывает все этапы работы персонала, и первый из них – документирование ролей и обязанностей в области информационной безопасности при определении требований ко всем должностям. В соответствии с этими требованиями должен производиться отбор новых сотрудников, заключаться с ними соглашения о соблюдении конфиденциальности, оговариваться в контрактах другие условия.

Для сознательного поддержания режима информационной безопасности необходимо обучение всех пользователей и регулярное повышение их квалификации.

Наряду с превентивными стандарт предусматривает и меры реагирования на инциденты в области безопасности, чтобы минимизировать ущерб и извлечь уроки на будущее. Предусмотрены уведомления (доклады) –

- об инцидентах;
- замеченных уязвимостях;
- нештатной работе программного обеспечения.

Следует разработать механизмы оценки ущерба от инцидентов и сбоев, дисциплинарного наказания виновных сотрудников.

*Пятая группа регуляторов безопасности* направлена на обеспечение физической безопасности и безопасности окружающей среды. Она включает три подгруппы:

1. Организация защищенных областей.
2. Защита оборудования.
3. Меры общего характера.

Для организации защищенных областей требуется определить периметры физической безопасности, контролировать вход в защищенные области и работу в них, защитить производственные помещения (особенно имеющие специальные требования по безопасности) и места погрузочно-разгрузочных работ, которые по возможности необходимо изолировать от производственных помещений.

Чтобы предупредить утерю, повреждение или несанкционированную модификацию оборудования, рекомендуется:

- размещать оборудование в защищенных областях;
- наладить бесперебойное электропитание;
- защитить кабельную разводку;
- организовать обслуживание оборудования;
- перемещать устройства (в том числе за пределы организации) только с разрешения руководства;
- удалять информацию перед выведением из эксплуатации или изменением характера использования оборудования.

К числу мер общего характера относится политика «чистого» рабочего стола и «чистого» экрана, а также уничтожение активов, оборудования, программ и данных только с разрешения руководства.

*Шестая группа регуляторов безопасности* – меры по безопасному администрированию систем и сетей. Она разделена на семь подгрупп:

1. Операционные процедуры и обязанности.
2. Планирование и приемка систем.
3. Защита от вредоносного программного обеспечения.
4. Повседневное обслуживание.
5. Администрирование сетей.
6. Безопасное управление носителями.
7. Обмен данными и программами с другими организациями.

*Операционные процедуры и обязанности.* Документирование операционных процедур и обязанностей преследует цель обеспечения корректного и надежного функционирования средств обработки информации. Требуется обязательно контролировать все изменения этих средств. Доклады о нарушениях безопасности должны быть своевременными и эффективными. Разделение обязанностей должно препятствовать злоупотреблению полномочиями. Средства разработки и тестирования необходимо отделить от производственных ресурсов. Для безопасного управления внешними ресурсами предлагается предварительно оценить риски и включить в контракты со сторонними организациями соответствующие положения.

*Планирование и приемка систем* призваны минимизировать риск их отказа. Для этого рекомендуется отслеживать и прогнозировать вычислительную нагрузку, требуемые ресурсы хранения и т. д. Следует разработать критерии приемки новых систем и версий, организовать их тестирование до введения в эксплуатацию.

*Защита от вредоносного программного обеспечения* должна включать как превентивные меры, так и меры обнаружения и ликвидации вредоносного ПО.

*Повседневным обслуживанием* включает резервное копирование, протоколирование действий операторов, регистрацию, доведение до сведения руководства и ликвидацию сбоев и отказов.

*Администрирование сетей* в стандарте не раскрывается, лишь констатируется необходимость целого спектра регуляторов безопасности и документирования обязанностей и процедур.

*Безопасное управление носителями* подразумевает контроль за съемными носителями, безвредную утилизацию отслуживших свой срок носителей, документирование процедур обработки и хранения информации, защиту системной документации от несанкционированного доступа.

*Обмен данными и программами с другими организациями.* Предлагается заключать формальные и неформальные соглашения, защищать носители при транспортировке, обеспечивать безопасность электронной коммерции, электронной почты, офисных систем, систем общего доступа и других средств обмена. В качестве универсальных защитных средств рекомендуются документированная политика безопасности, соответствующие процедуры и регуляторы.

*Седьмая группа регуляторов безопасности* относится к управлению доступом к системам и сетям. Она состоит из восьми подгрупп:

1. Производственные требования к управлению доступом.
2. Управление доступом пользователей.
3. Обязанности пользователей.
4. Управление доступом к сетям.
5. Управление доступом средствами операционных систем.
6. Управление доступом к приложениям.
7. Контроль за доступом и использованием систем.
8. Контроль мобильных пользователей и удаленного доступа.

*Производственные требования к управлению доступом* излагаются в документированной политике безопасности, которую необходимо проводить в жизнь.

*Управление доступом пользователей* должно обеспечить авторизацию, выделение и контроль прав в соответствии с политикой безопасности. Этой цели служат процедуры регистрации пользователей и ликвидации их системных счетов, управление привилегиями в соответствии с принципом их минимизации, управление паролями пользователей и дисциплина регулярной ревизии прав доступа.

*Обязанности пользователей* сводятся к правильному выбору и применению паролей, а также к защите оборудования, остающегося без присмотра.

*Управление доступом к сетям* опирается на следующие регуляторы:

- политика использования сетевых услуг (прямой доступ к услугам должен предоставляться только по явному разрешению);
- задание маршрута от пользовательской системы до используемых систем (предоставление выделенных линий, недопущение неограниченного перемещения по сети и т. д.);
- аутентификация удаленных пользователей;
- аутентификация удаленных систем;

- контроль доступа (особенно удаленного) к диагностическим портам;
- сегментация сетей (выделение групп пользователей, информационных сервисов и систем);
- контроль сетевых подключений (например, контроль по предоставляемым услугам и / или времени доступа);
- управление маршрутизацией;
- защита сетевых сервисов (должны быть описаны атрибуты безопасности всех сетевых сервисов, используемых организацией).

*Управление доступом средствами операционных систем* направлено на защиту от несанкционированного доступа к компьютерным системам. Для этого предусматриваются:

- автоматическая идентификация терминалов;
- безопасные процедуры входа в систему (следует выдавать как можно меньше информации о системе, ограничить разрешаемое количество неудачных попыток, контролировать минимальную и максимальную продолжительность входа и т. п.);
- идентификация и аутентификация пользователей;
- управление паролями, контроль их качества;
- разграничение доступа к системным средствам;
- уведомление пользователей об опасных ситуациях;
- контроль времени простоя терминалов (с автоматическим отключением по истечении заданного периода);
- ограничение времени подключения к критичным приложениям.

Для *управления доступом к приложениям* предусматривается разграничение доступа к данным и прикладным функциям, а также изоляция критичных систем, помещение их в выделенное окружение.

*Контроль за доступом и использованием систем* преследует цель выявления действий, нарушающих политику безопасности. Для ее достижения следует протоколировать события, относящиеся к безопасности, отслеживать и регулярно анализировать использование средств обработки информации, синхронизировать компьютерные часы.

*Контроль мобильных пользователей и удаленного доступа* должен основываться на документированных положениях политики безопасности.

*Восьмая группа регуляторов безопасности* – разработка и сопровождение информационных систем. Она охватывает весь жизненный цикл систем.

1. Первым шагом является анализ и задание требований безопасности. Основу анализа составляют:

- необходимость обеспечения конфиденциальности, целостности и доступности информационных активов;
- возможность использования различных регуляторов для предотвращения и выявления нарушений безопасности и для восстановления нормальной работы после отказа или нарушения безопасности.

В частности, следует рассмотреть необходимость:

- управления доступом к информации и сервисам, включая требования к разделению обязанностей и ресурсов;
- протоколирования для повседневного контроля или специальных расследований;
- контроля и поддержания целостности данных на всех или избранных стадиях обработки;
- обеспечения конфиденциальности данных, возможно, с использованием криптографических средств;
- выполнения требований действующего законодательства, договорных требований и т. п.;
- резервного копирования производственных данных;
- восстановления систем после отказов (особенно для систем с повышенными требованиями к доступности);
- защиты систем от несанкционированных модификаций;
- безопасного управления системами и их использования сотрудниками, не являющимися специалистами.

2. Подгруппа регуляторов, обеспечивающих безопасность прикладных систем, включает:

- проверку входных данных;
- встроенные проверки корректности данных в процессе их обработки;
- аутентификацию сообщений как элемент контроля их целостности;
- проверку выходных данных.

3. Третью подгруппу рассматриваемой группы составляют криптографические регуляторы. Их основой служит документированная политика использования средств криптографии. Стандартом предусматривается применение шифрования, электронных цифровых подписей, средств управления ключами.

4. Четвертая подгруппа – защита системных файлов. Она предусматривает:

- управление программным обеспечением, находящимся в эксплуатации;
- защиту тестовых данных систем;
- управление доступом к библиотекам исходных текстов.

5. Регуляторы пятой подгруппы направлены на обеспечение безопасности процесса разработки и вспомогательных процессов. В нее входят следующие регуляторы:

- процедуры управления внесением изменений;
- анализ и тестирование систем после внесения изменений;
- ограничение на внесение изменений в программные пакеты;
- проверка наличия скрытых каналов и троянских программ;
- контроль за разработкой ПО, выполняемой внешними организациями.

*Девятая группа регуляторов безопасности* – управление бесперебойной работой организации. Она включает пять регуляторов, направленных на предотвращение перерывов в деятельности предприятия и защиту критически важных бизнес-процессов от последствий крупных аварий и отказов:

- формирование процесса управления бесперебойной работой организации;
- выработка стратегии (на основе анализа рисков) обеспечения бесперебойной работы организации;
- документирование и реализация планов обеспечения бесперебойной работы организации;
- поддержание единого каркаса для планов обеспечения бесперебойной работы организации, чтобы гарантировать их согласованность и определить приоритетные направления тестирования и сопровождения;
- тестирование, сопровождение и регулярный пересмотр планов обеспечения бесперебойной работы организации на предмет их эффективности и соответствия текущему состоянию.

Процесс планирования бесперебойной работы организации должен включать в себя:

- идентификацию критически важных производственных процессов и их ранжирование по приоритетам;
- определение возможного воздействия аварий различных типов на производственную деятельность;

- определение и согласование всех обязанностей и планов действий в нештатных ситуациях;
- документирование согласованных процедур и процессов;
- подготовку персонала к выполнению согласованных процедур и процессов в нештатных ситуациях.

Для обеспечения бесперебойной работы организации необходимы процедуры трех типов:

1. Реагирование на нештатные ситуации.
2. Переход на аварийный режим.
3. Возобновление нормальной работы.

Примерами изменений, которые могут потребовать обновления планов, являются:

- приобретение нового оборудования или модернизация систем;
- новая технология выявления и контроля проблем, например, обнаружения пожаров;
- кадровые или организационные изменения;
- смена подрядчиков или поставщиков;
- изменения, внесенные в производственные процессы;
- изменения, внесенные в пакеты прикладных программ;
- изменения в эксплуатационных процедурах;
- изменения в законодательстве.

*Десятая группа регуляторов безопасности* – контроль соответствия требованиям. В первую подгруппу входят регуляторы соответствия действующему законодательству:

- идентификация применимых законов, нормативных актов и т. п.;
- обеспечение соблюдения законодательства по защите интеллектуальной собственности;
- защита деловой документации от утери, уничтожения или фальсификации;
- обеспечение защиты персональных данных;
- предотвращение незаконного использования средств обработки информации;
- обеспечение выполнения законов, касающихся криптографических средств;
- обеспечение сбора свидетельств на случай взаимодействия с правоохранительными органами.

Ко второй подгруппе отнесены регуляторы, контролирующие соответствие политике безопасности и техническим требованиям. Руководители всех уровней должны убедиться, что все защитные процедуры, входящие в их зону ответственности, выполняются должным образом и что все такие зоны регулярно анализируются на предмет соответствия политике и стандартам безопасности. Информационные системы нуждаются в регулярной проверке соответствия стандартам реализации защитных функций.

Регуляторы, относящиеся к аудиту информационных систем, объединены в третью подгруппу. Их цель – максимизировать эффективность аудита и минимизировать помехи, создаваемые процессом аудита, равно как и вмешательство в этот процесс. Ход аудита должен тщательно планироваться, а используемый инструментарий защищаться от несанкционированного доступа.

### **2.1.3. Британский стандарт BS 7799-3 «Руководство по управлению рисками информационной безопасности»**

Стандарт содержит вводную часть, разделы по оценке рисков, обработке рисков, непрерывным действиям по управлению рисками, а также имеет приложение с примерами активов, угроз, уязвимостей, методов оценки рисков. Стандарт придерживается самого общего понятия риска.

Под *риском* понимается комбинация вероятности события и его последствий (стоимости компрометируемого ресурса).

*Управление риском* – скоординированные непрерывные действия по управлению и контролю рисков в организации.

Непрерывный процесс управления спроецирован на четыре фазы менеджмента:

1. Планирование.
2. Реализация.
3. Проверка.
4. Совершенствование.

В контексте стандарта эти четыре фазы выглядят следующим образом:

1. Оценка рисков, включающая анализ и вычисление рисков.
2. Обработка риска – выбор и реализация мер и средств безопасности.

3. Контроль рисков путем мониторинга, тестирования, анализа механизмов безопасности, а также аудита системы.

4. Оптимизация рисков путем модификации и обновления правил, мер и средств безопасности.

### ***Оценка рисков***

Оценка рисков – первый этап в управлении системы информационной безопасности, предназначенный для идентификации источников рисков и определения его уровня значимости. Оценку разбивают на анализ рисков и оценивание рисков.

В рамках анализа проводится инвентаризация и категоризация защищаемых ресурсов, выясняются нормативные, технические, договорные требования к ресурсам в сфере ИБ, а затем с учетом этих требований определяется стоимость ресурсов. В стоимость входят все потенциальные затраты, связанные с возможной компрометацией защищаемых ресурсов.

Следующим этапом анализа рисков является составление перечня значимых угроз и уязвимостей для каждого ресурса, а затем вычисляется вероятность их реализации.

Стандарт допускает двоякое толкование понятия угрозы ИБ: как условие реализации уязвимости ресурса (в этом случае уязвимости и угрозы идентифицируются отдельно) и как общее потенциальное событие, способное привести к компрометации ресурса (когда наличие возможности реализации уязвимости и есть угроза). Не возбраняется разделение угроз ИБ на угрозы целостности, доступности и конфиденциальности.

Оценивание риска проводится путем его вычисления и сопоставления с заданной шкалой. Вычисление риска состоит в умножении вероятности компрометации ресурса на значение величины ущерба, связанного с его компрометацией. Сопоставление риска выполняется с целью упрощения процесса использования на практике точечных значений риска.

Стандарт допускает использование как количественных, так и качественных методов оценки рисков, но, к сожалению, в документе нет обоснования и рекомендаций по выбору математического и методического аппарата оценки рисков ИБ.

Приложение к стандарту содержит единственный пример, который условно можно отнести к качественному методу оценки. Данный пример использует трех- и пятибалльные оценочные шкалы:

1. Оцениваются уровни стоимости идентифицированного ресурса по пятибалльной шкале: «незначительный», «низкий», «средний», «высокий», «очень высокий».

2. Оцениваются уровни вероятности угрозы по трехбалльной шкале: «низкий», «средний», «высокий».

3. Оцениваются уровни вероятности уязвимости: «низкий», «средний», «высокий».

4. По заданной таблице рассчитываются уровни риска.

5. Проводится ранжирование инцидентов по уровню риска.

### ***Обработка риска***

После того как риск оценен, должно быть принято решение относительно его обработки, т. е. выбора и реализации мер и средств по минимизации риска.

Помимо оцененного уровня риска при принятии решения могут быть учтены затраты на внедрение и сопровождение механизмов безопасности, политика руководства, простота реализации, мнение экспертов и др.

Предлагается одна из четырех мер обработки риска:

1. Уменьшение риска. Риск считается неприемлемым, и для его уменьшения выбираются и реализуются соответствующие меры и средства безопасности.

2. Передача риска. Риск считается неприемлемым и на определенных условиях (например, в рамках страхования, поставки или аутсорсинга) переадресуется сторонней организации.

3. Принятие риска. Риск в конкретном случае считается осознанно допустимым – организация должна смириться с возможными последствиями. Обычно это означает, что стоимость контрмер значительно превосходит финансовые потери в случае реализации.

4. Отказ от риска. Отказ от бизнес-процессов организации, являющихся причиной риска. Например, отказ от электронных платежей по Сети.

В результате обработки риска остается так называемый остаточный риск, относительно которого принимается решение о завершении этапа отработки риска. В стандарте ничего не сказано об эффективности мер, средств и сервисов, которые могут быть использованы при обработке риска.

### ***Управление рисками***

Раздел 7 стандарта «Непрерывная деятельность по управлению рисками» затрагивает следующие две фазы менеджмента системы – контроль риска и оптимизация риска.

Для контроля риска рекомендуются:

- технические меры (мониторинг, анализ системных журналов и выполнения проверок);
- анализ со стороны руководства;
- независимые внутренние аудиты ИБ.

Фаза оптимизации риска содержит переоценку риска и, соответственно, пересмотр политик, руководств по управлению рисками, корректировку и обновление механизмов безопасности.

### ***Принцип осведомленности***

Отличительной чертой стандарта является принцип осведомленности о процессах оценки, отработки, контроля и оптимизации рисков в организации. На каждом этапе управления рисками предусмотрено информирование всех участников процесса управления безопасностью, а также фиксирование событий СУИБ.

Наряду с планом обеспечения непрерывности бизнеса к основным документам по управлению рисками в британском стандарте отнесены:

- описание методологии оценки рисков;
- отчет об оценке рисков;
- план обработки рисков.

Кроме того, в непрерывном цикле управления рисками задействовано огромное множество рабочей документации:

- реестры ресурсов;
- реестры рисков;
- декларации применимости;
- списки проверок;
- протоколы процедур и тестов;
- журналы безопасности;
- аудиторские отчеты;
- планы коммуникаций;
- инструкции;
- регламенты и др.

Стандарт определяет обязанности и требования к категории лиц, непосредственно участвующих при управлении рисками, а именно:

- экспертам по оценке рисков;
- менеджерам по безопасности;
- менеджерам рисков безопасности;
- владельцам ресурсов;

– руководству организации.

### ***Развитие стандарта***

Стандарт имеет описательный характер и не содержит конкретных требований к способам управления рисками. Стандарты позволяют самостоятельно учесть различные аспекты СУИБ:

1. Идентифицировать уровни риска.
2. Определить критерии для принятия риска.
3. Идентифицировать приемлемые уровни риска и т. д.

### ***Выводы***

Стандарты BS 7799 придерживаются непрерывного 4-процессного подхода к менеджменту систем качества, включают аналогичные этапы анализа, оценки и управления, правила и рекомендации, носят итеративный характер, не предъявляют конкретных требований к методам, содержат требования по информативности каждого этапа. Можно отметить некоторую тенденцию в детализации этапов и добавлении примеров в очередных версиях проекта 27005.

Все современные стандарты в области безопасности отражают сложившийся в международной практике общий процессный подход к организации управления рисками. При этом управление рисками представляется как базовая часть системы менеджмента качества организации. Стандарты носят откровенно концептуальный характер, что позволяет экспертам по ИБ реализовать любые методы, средства и технологии оценки, отработки и управления рисками.

С другой стороны, стандарты не содержат рекомендаций по выбору какого-либо аппарата оценки риска, а также по синтезу мер, средств и сервисов безопасности, используемых для минимизации рисков, что снижает полезность стандартов как технологических документов.

## **2.2. МЕЖДУНАРОДНЫЙ СТАНДАРТ ISO/IEC 17799 «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ТЕХНОЛОГИИ БЕЗОПАСНОСТИ. ПРАКТИЧЕСКИЕ ПРАВИЛА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Данный стандарт информационной безопасности, опубликованный в 2005 г. организациями ISO и IEC (ISO – Международная организация по стандартизации, IEC – Международная электротехническая комиссия).

Основным достоинством стандарта является его гибкость и универсальность. Описанный в нем набор лучших практик применим практически к любой организации независимо от формы собственности, вида деятельности, размера и внешних условий. Он нейтрален в технологическом плане и всегда оставляет возможность выбора технологий.

Стандарт поможет определить верное направление и не упустить из виду существенные моменты. Его можно использовать как авторитетный источник и один из инструментов для определения критериев и обоснования затрат на ИБ.

Однако гибкость и универсальность одновременно являются и недостатком этого стандарта. Критики говорят, что ISO 17799 является слишком абстрактным и нечетко структурированным, чтобы представлять реальную ценность. Недостаточно основательное его применение может давать ложное чувство защищенности.

ISO 17799 описывает меры по обеспечению безопасности в общем виде, но ничего не говорит о технических аспектах их реализации.

Например, стандарт рекомендует использовать механизмы контроля доступа и определяет конкретные технологии, такие как USB-ключи, смарт-карты, сертификаты и т. п. Однако он не рассматривает достоинства и недостатки этих технологий, особенности и способы их применения.

В стандарте при проектировании и создании эффективной системы безопасности организации основное внимание уделяется комплексному подходу к управлению ИБ, которое должно осуществляться с применением технических и направленных на обеспечение конфиденциальности, целостности и доступности защищаемой информации. Нарушение любого из этих принципов может привести как к незначительным убыткам организации, так и к ее банкротству.

С целью формирования комплексных требований к безопасности информации стандарт определяет три основных показателя:

1. Оценка рисков, с которыми сталкивается организация (определение угрозы для ресурсов, их уязвимость и вероятность возникновения угроз, а также возможный ущерб).

2. Соблюдение законодательных, нормативных и договорных требований, которые должны выполняться самой организацией, ее партнерами по бизнесу, подрядчиками и поставщиками услуг.

3. Формирование комплекса принципов, целей и требований к обработке информации, разработанных организацией для поддержки своей деятельности.

Оценка рисков должна помочь определить необходимые действия и приоритеты для управления ИБ и для реализации выбранных средств защиты. Процесс оценки рисков и выбора средств защиты может выполняться несколько раз, чтобы охватить различные части организации или отдельные информационные системы.

Средства защиты должны выбираться с учетом затрат на реализацию. При этом затраты должны соответствовать степени рисков и потенциальным убыткам при нарушении безопасности.

С целью определения необходимого уровня защиты информационных ресурсов должны быть составлены их перечни и проведена классификация информации по уровням конфиденциальности.

Кроме технической реализации средств защиты информации на основе результатов оценки рисков и выбранного уровня защиты должны быть разработаны организационные меры обеспечения ИБ, которые должны включать в себя следующие положения:

- разработка политики ИБ;
- распределение ответственности;
- обучение и подготовка персонала;
- создание отчетов;
- поддержка непрерывности бизнеса;
- определение ИБ, ее целей и области действия;
- общее описание принципов управления ИБ;
- краткое описание политики безопасности, принципов, стандартов, требований;
- описание обязанностей, правила распределения ответственности;
- ссылки на более детальные инструкции и описания правил безопасности.

### ***Практическая организация ИБ***

В разделах стандарта приведены практические рекомендации по организации ИБ, которые, как правило, отражаются в политике безопасности организации или в отдельных инструкциях с учетом специфики самой организации.

#### **1. Вопросы безопасности, связанные с персоналом –**

- безопасность при формулировке заданий и наборе сотрудников;
- обучение пользователей.
- реакция на инциденты и сбои в работе.

#### **2. Физическая безопасность и защита территорий –**

- защищенные территории;
- безопасность оборудования;
- общие меры.

#### **3. Обеспечение безопасности при эксплуатации –**

- правила работы и обязанности;
- планирование разработки и приемка системы;
- защита от злонамеренного программного обеспечения;
- служебные процедуры;
- управление вычислительными сетями;
- обращение с носителями и их безопасность;
- обмен информацией и программным обеспечением.

#### **4. Контроль доступа –**

- требования к контролю доступа в организации;
- управление доступом пользователей;
- обязанности пользователей;
- контроль доступа к вычислительной сети;
- контроль доступа к операционным системам;
- контроль доступа к приложениям;
- мониторинг доступа и использования системы;
- мобильные компьютеры и средства удаленной работы.

#### **5. Разработка и обслуживание систем –**

- требования к безопасности систем;
- безопасность в прикладных системах;
- криптографические средства;
- безопасность системных файлов;
- безопасность при разработке и поддержке.

#### **6. Обеспечение непрерывности бизнеса –**

- аспекты обеспечения непрерывности бизнеса.

#### **7. Соответствие требованиям –**

- соответствие требованиям законодательства;

- проверка политики безопасности и соответствие техническим требованиям;
- рекомендации по аудиту систем.

Требования безопасности информации должны учитываться во всех сферах жизнедеятельности организации, в том числе при формировании и распределении должностных обязанностей. Кроме того, должностные обязанности пользователей информационных ресурсов должны содержать более конкретизированные и расширенные (по сравнению с изложенными в общей политике безопасности организации) требования к обеспечению безопасности информации. Все сотрудники организации должны проходить соответствующую подготовку в области политики безопасности и процедур, принятых в организации с периодической переподготовкой.

### **2.3. СЕМЕЙСТВО МЕЖДУНАРОДНЫХ СТАНДАРТОВ ISO/IEC 27000**

Это семейство включает в себя международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.

Данный международный стандарт содержит общий обзор систем управления защитой информации и определяет соответствующие отраслевые термины.

В семейство входят стандарты, которые:

- устанавливают требования к самим системам обеспечения информационной безопасности и к органам, проводящим их сертификацию;
- обеспечивают прямую поддержку, всестороннее консультирование и / или интерпретацию в рамках всего процесса создания, внедрения, сопровождения и развития систем обеспечения информационной безопасности;
- содержат руководящие указания по использованию систем обеспечения информационной безопасности в рамках определенной сферы их назначения, касаются оценки соответствия систем обеспечения информационной безопасности предъявляемым требованиям.

Для этого семейства стандартов используется последовательная схема нумерации, начиная с 27000 и далее.

**ISO27000** – (ISO/IEC 27000:2009) Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности – Определения и основные принципы.

**ISO27001** – (ISO/IEC 27001:2013) Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности – Требования. Вторая редакция 01.10.2013.

**ISO27002** – (ISO/IEC 27002:2013) Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью. Вторая редакция 01.10.2013.

**ISO27003** – (ISO/IEC 27003:2010) Информационные технологии – Методы обеспечения безопасности – Руководство по внедрению системы управления информационной безопасностью.

**ISO27004** – (ISO/IEC 27004:2009) Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности – Измерение.

**ISO27005** – (ISO/IEC 27005:2011) Информационные технологии – Методы обеспечения безопасности – Управление рисками информационной безопасности (вторая редакция, 2011 г.).

**ISO27006** – (ISO/IEC 27006:2007) Информационные технологии – Методы обеспечения безопасности – Требования к органам аудита и сертификации систем управления информационной безопасностью.

**ISO27007** – (ISO/IEC 27007:2011) Информационные технологии – Методы обеспечения безопасности – Руководство по аудиту систем менеджмента информационной безопасности.

**ISO27008** – (ISO/IEC TR 27008:2011) Информационные технологии – Методы обеспечения безопасности – Руководство для аудиторов по механизмам контроля систем менеджмента информационной безопасности.

**ISO27010** – (ISO/IEC 27010:2012) Информационные технологии – Методы обеспечения безопасности – Управление информационной безопасностью при коммуникациях между секторами.

Стандарт представляет собой руководство по совместному использованию информации о рисках информационной безопасности, механизмах контроля, проблемах и / или инцидентах, выходящей за границы отдельных секторов экономики и государств, особенно в части, касающейся «критических инфраструктур».

**ISO27011** – (ISO/IEC 27011:2008) Информационные технологии – Методы обеспечения безопасности – Руководство по управлению информационной безопасностью для телекоммуникаций.

**ISO27013** – (ISO/IEC 27013:2012) Информационные технологии – Методы обеспечения безопасности – Руководство по интегрированному внедрению ISO/IEC 20000-1 и ISO/IEC 27001.

**ISO27014** – (ISO/IEC 27014:2013) Информационные технологии – Методы обеспечения безопасности – Базовая структура управления информационной безопасностью.

**ISO27015** – (ISO/IEC TR 27015:2012) Информационные технологии – Методы обеспечения безопасности – Руководство по внедрению систем управления информационной безопасностью в финансовом и страховом секторе.

**ISO27018** – (ISO/IEC 27018:2014) Информационные технологии – Методы обеспечения безопасности – Практическое руководство по защите персонально идентифицируемой информации в публичных облаках, используемых для обработки персонально идентифицируемой информации (первая редакция, 2014 г.).

**ISO27031** – (ISO/IEC 27031:2011) Информационные технологии – Методы обеспечения безопасности – Руководство по обеспечению готовности информационных и коммуникационных технологий к их использованию для управления непрерывностью бизнеса.

**ISO27032** – (ISO/IEC 27032:2012) Информационные технологии – Методы обеспечения безопасности – Руководство по обеспечению кибербезопасности.

**ISO27033-1** – (ISO/IEC 27033-1:2009) Информационные технологии – Методы обеспечения безопасности – Сетевая безопасность – Основные концепции управления сетевой безопасностью.

**ISO27033-2** – (ISO/IEC 27033-2:2012) Информационные технологии – Методы обеспечения безопасности – Сетевая безопасность – Руководство по проектированию и внедрению системы обеспечения сетевой безопасности.

**ISO27033-3** – (ISO/IEC 27033-3:2010) Информационные технологии – Методы обеспечения безопасности – Сетевая безопасность – Базовые сетевые сценарии – угрозы, методы проектирования и механизмы контроля.

**ISO27033-4** – (ISO/IEC 27033-4:2014) Информационные технологии – Методы обеспечения безопасности – Сетевая безопасность – Обеспечение безопасности межсетевых взаимодействий при по-

мощи шлюзов безопасности – угрозы, методы проектирования и механизмы контроля.

**ISO27033-5** – (ISO/IEC 27033-5) Информационные технологии – Методы обеспечения безопасности – Сетевая безопасность – Обеспечение безопасности виртуальных частных сетей – угрозы, методы проектирования и механизмы контроля.

**ISO27033-6** – (ISO/IEC 27033-6) Информационные технологии – Методы обеспечения безопасности – Сетевая безопасность – Конвергенция в IP-сетях.

**ISO27033-7** – (ISO/IEC 27033-7) Информационные технологии – Методы обеспечения безопасности – Сетевая безопасность – Руководство по обеспечению безопасности беспроводных сетей – Риски, методы проектирования и механизмы контроля.

ISO 27033 заменяет известный международный стандарт сетевой безопасности ISO 18028, состоящий из пяти частей.

**ISO27034-1** – (ISO/IEC 27034-1:2011) Информационные технологии – Методы обеспечения безопасности – Обзор и основные концепции в области обеспечения безопасности приложений.

**ISO27034-2** – (ISO/IEC 27034-2) Информационные технологии – Методы обеспечения безопасности – Безопасность приложений – Нормативная база организации (проект).

**ISO27034-3** – (ISO/IEC 27034-3) Информационные технологии – Методы обеспечения безопасности – Процесс управления безопасностью приложений (проект).

**ISO27034-4** – (ISO/IEC 27034-4) Информационные технологии – Методы обеспечения безопасности – Оценка безопасности приложений (проект).

**ISO27034-5** – (ISO/IEC 27034-5) Информационные технологии – Методы обеспечения безопасности – Протоколы и структура управляющей информации для обеспечения безопасности приложений (XML-схема) (проект).

**ISO27034-6** – (ISO/IEC 27034-6) Информационные технологии – Методы обеспечения безопасности – Руководство по обеспечению безопасности конкретных приложений (проект).

**ISO27035** – (ISO/IEC 27035:2011) Информационные технологии – Методы обеспечения безопасности – Управление инцидентами безопасности.

**ISO27036-1** – (ISO/IEC 27036-1:2014) Информационные технологии – Методы обеспечения безопасности – Информационная бе-

зопасность при взаимодействии с поставщиками – Часть 1: Обзор и концепции.

**ISO27036-2** – (ISO/IEC 27036-2:2014) Информационные технологии – Методы обеспечения безопасности – Руководство по взаимодействию с поставщиками – Часть 2: Требования.

**ISO27036-3** – (ISO/IEC 27036-3:2013) Информационные технологии – Методы обеспечения безопасности – Информационная безопасность при взаимодействии с поставщиками – Часть 3: Руководящие указания по защите цепей поставки информационных и коммуникационных технологий.

**ISO27037** – (ISO/IEC 27037:2012) Информационные технологии – Методы обеспечения безопасности – Руководство по идентификации, сбору и / или получению и обеспечению сохранности цифровых свидетельств.

Разработан на базе британского стандарта BS 10008:2008.

**ISO27040** – (ISO/IEC 27040:2015) Информационные технологии – Методы обеспечения безопасности – Безопасность хранения данных.

**ISO27041** – (ISO/IEC 27041:2015) Информационные технологии – Методы обеспечения безопасности – Руководство по предоставлению гарантий пригодности и адекватности метода расследования инцидента.

**ISO27042** – (ISO/IEC 27042:2015) Информационные технологии – Методы обеспечения безопасности – Руководство по анализу и интерпретации цифровых свидетельств.

**ISO27799** – (ISO 27799:2008) Информатика в здравоохранении – Менеджмент безопасности информации по стандарту ISO/IEC 27002.

### **2.3.1. Международный стандарт ISO/IEC 27001**

**«Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования»**

Это международный стандарт, базирующийся на BS 7799-2:2005.

В стандарте собраны описания лучших мировых практик в области управления информационной безопасностью. Он устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы. Стандарт подготовлен в качестве модели

для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ) (рисунок).

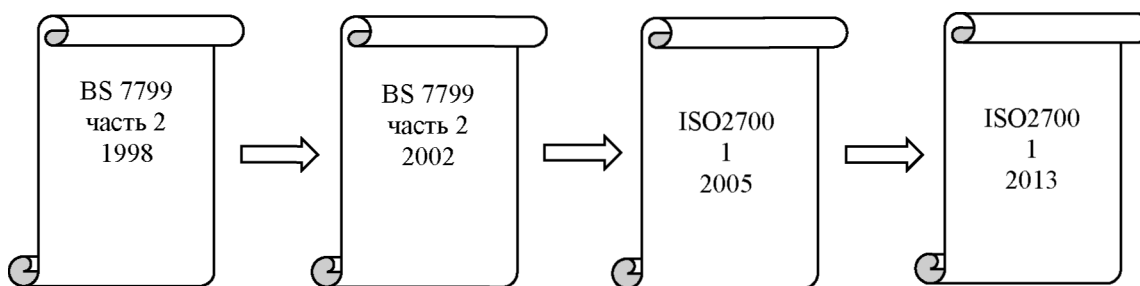


Рис. Развитие до ISO/IEC 27001:2013

Цель СМИБ – выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

Основные задачи стандарта:

- установление единых требований по обеспечению информационной безопасности организаций;
- обеспечение взаимодействия руководства и сотрудников;
- повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности организаций.

#### **Основные понятия**

*Информационная безопасность* – сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность.

*Конфиденциальность* – обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи).

*Целостность* – обеспечение точности и полноты информации, а также методов ее обработки.

*Доступность* – обеспечение доступа к информации авторизованным пользователям, когда это необходимо (по требованию).

Само понятие защиты информации трактуется международным стандартом как обеспечение конфиденциальности, целостности и доступности информации.

*Основа стандарта* – система управления рисками, связанными с информацией. Система управления рисками позволяет получать ответы на следующие вопросы:

- на каком направлении информационной безопасности требуется сосредоточить внимание;
- сколько времени и средств можно потратить на данное техническое решение для защиты информации.

В 2013 г. Международной организацией по сертификации была разработана и принята новая версия стандарта ISO/IEC 27001:2013. Изменения коснулись как структуры стандарта, так и требований.

Изменения в структуре стандарта ISO/IEC 27001:2013:

1. Четко сформулированы требования к целям системы менеджмента информационной безопасности.
2. Упрощены требования к текстовому описанию рисков.
3. Исключена обязательность выпуска «Положения о принятии остаточных рисков» со стороны высшего руководства.
4. Установлена четкая связка «Положения о применимости – SoA».
5. Введено понятие и требование по определению «Владельца риска» вместо «Владельца актива».
6. Четко сформулированы и дополнены требования по мониторингу системы менеджмента информационной безопасности.
7. Упрощены требования к управлению документацией и записями системы менеджмента информационной безопасности.
8. Четко определены требования по коммуникациям в рамках системы менеджмента информационной безопасности.

Наиболее существенным изменением в основной части является требование по определению «Владельцев рисков».

Приложение «А» ISO/IEC 27001 содержит перечень целей и средств управления, которые совпадают с аналогичными целями и средствами управления в ISO 27002, но не столь детализированы.

### **2.3.2. Международный стандарт ISO/IEC 27002 «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности»**

#### ***Область действия***

Этот международный стандарт устанавливает руководящие и общие принципы начинания, реализации, поддержания в рабочем состоянии и улучшения управления защитой информации в организации.

Цели, очерченные этим международным стандартом, дают общие руководящие принципы по обычно принимаемым целям управления защитой информации. Цели и средства управления этого международного стандарта разработаны для реализации, осуществляемой с целью выполнить требования, выявленные оценкой рисков. Этот международный стандарт может служить в качестве практического руководства по разработке организационных стандартов защиты и практик эффективного управления защитой, а также для того, чтобы помочь создать доверие в межорганизационной деятельности.

Для целей этого документа применяются следующие термины и определения:

- *актив* – что-либо, что имеет ценность для организации;
- *средство управления* – средства управления рисками, включая политику, процедуры, руководящие принципы, практики или организационные структуры, которые могут носить административный, технический, управленческий или юридический характер;

Примечание. Термин «средство управления» также используется как синоним термина «мера безопасности» или «контрмера».

- *руководящий принцип* – описание, которое разъясняет, что и как следует сделать, чтобы достичь целей, установленных политикой;

- *средства обработки информации* – любая система, служба или инфраструктура обработки информации или фактическое месторасположение, где они находятся;

- *защита информации* – сохранение конфиденциальности, целостности и доступности информации (кроме того, также могут быть включены другие свойства, такие как аутентичность, подотчетность, неотрекаемость и надежность);

- *событие в системе защиты информации* – выявленный случай системы, услуги или состояния сети, указывающий на возможное нарушение в политике защиты информации или в работе средств защиты, или прежде неизвестная ситуация, которая может иметь значение для защиты;

- *инцидент в системе защиты информации* – одно или серия нежелательных, или неожиданных событий в системе защиты информации, которые имеют большой шанс подвергнуть риску деловые операции и поставить под угрозу защиту информации;

- *политика* – общее намерение и направление, официально выраженное руководством;

- *риск* – комбинация вероятности события и его последствий;
- *анализ риска* – систематическое использование информации для выявления источников и для оценки степени риска;
- *оценка риска* – целостный процесс анализа риска и оценки значительности риска;
- *оценка значительности риска* – процесс сравнения расчетного риска с заданными критериями риска с целью определить значительность риска;
- *менеджмент рисков* – согласованные виды деятельности по руководству и управлению организацией в том, что касается рисков;
- *обработка риска* – процесс выбора и реализации мер по изменению риска;
- *третья сторона* – лицо или организация, которые признаются независимыми от вовлеченных сторон в том, что касается рассматриваемой проблемы;
- *угроза* – возможная причина нежелательного инцидента, который может закончиться ущербом для системы или организации;
- *слабое место* – слабость актива или группы активов, которой могут воспользоваться одна угроза или более.

### ***Структура стандарта***

Этот стандарт содержит 11 разделов по средствам управления защитой информации, вместе содержащих в общей сложности 39 основных категорий защиты и один вступительный раздел, вводящий в оценку и обработку рисков.

### ***Разделы***

Каждый раздел содержит некоторое количество основных категорий защиты.

Одиннадцать разделов (вслед за названием указано количество основных категорий защиты, включенных в каждый раздел) –

1. Политика в области защиты (1).
2. Организация защиты информации (2).
3. Менеджмент активов (2).
4. Защита человеческих ресурсов (3).
5. Физическая и экологическая безопасность (2).
6. Управление средствами связи и операциями (10).
7. Управление доступом (7).
8. Приобретение, разработка и поддержание в рабочем состоянии информационных систем (6).
9. Управление инцидентами в системе защиты информации (2).
10. Менеджмент непрерывности бизнеса (1).

## 11. Соответствие (3).

Примечание. Порядок разделов в этом стандарте не означает их важность. В зависимости от обстоятельств все статьи могут быть важны; поэтому каждой организации, применяющей этот стандарт, следует определить применимые разделы, то, насколько они важны, а также их приложение к отдельным деловым процессам. Также все списки в этом стандарте даны не в порядке приоритета, если это не указано.

### ***Основные категории защиты***

Каждая основная категория защиты содержит следующее:

- цель управления, формулирующая, чего надо достичь;
- одно или более средств управления, которые могут быть применены для достижения цели управления.

Описания средств управления структурированы следующим образом:

1. Средство управления. Определяет конкретную стратегию управления для выполнения цели управления.

2. Руководство по реализации. Дает более подробную информацию для того, чтобы поддержать реализацию средства управления и выполнение цели управления. Некоторые из этих руководств могут не быть подходящими во всех случаях, так что другие способы реализации средств управления могут оказаться более подходящими.

3. Прочая информация. Дает дополнительную дальнейшую информацию, которую может понадобиться рассмотреть, например, вопросы юридического характера и ссылки на другие стандарты.

### **Глава 3. НАЦИОНАЛЬНЫЕ СТАНДАРТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации – ГОСТ Р 1.0-2013 «Стандартизация в Российской Федерации. Основные положения».

#### **3.1. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р 50922-2006 «ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ»**

Дата введения стандарта – 1 февраля 2008 г.

##### ***Сведения о стандарте***

1. Разработан Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»).

2. Внесен Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии.

3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст.

4. В стандарте реализованы нормы Федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

5. Взамен ГОСТ Р 50922-96.

##### ***Содержание***

1. Область применения
2. Термины и определения
  - 2.1. Общие понятия
  - 2.2. Термины, относящиеся к видам защиты информации
  - 2.3. Термины, относящиеся к способам защиты информации
  - 2.4. Термины, относящиеся к замыслу защиты информации

- 2.5. Термины, относящиеся к объекту защиты информации
- 2.6. Термины, относящиеся к угрозам безопасности информации
- 2.7. Термины, относящиеся к технике защиты информации
- 2.8. Термины, относящиеся к способам оценки соответствия требованиям по защите информации
- 2.9. Термины, относящиеся к эффективности защиты информации

Алфавитный указатель терминов

Приложение А (справочное). Термины и определения общетехнических понятий

Библиография

### ***Область применения***

Стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации.

Термины, установленные стандартом, рекомендуется использовать в правовой, нормативной, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.

### ***Термины и определения***

#### ***Общие понятия***

*Защита информации; ЗИ* – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

#### ***Термины, относящиеся к видам защиты информации***

*Правовая защита информации* – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

*Техническая защита информации; ТЗИ* – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

*Криптографическая защита информации* – защита информации с помощью ее криптографического преобразования.

*Физическая защита информации* – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

***Термины, относящиеся к способам защиты информации***

*Способ защиты информации* – порядок и правила применения определенных принципов и средств защиты информации.

*Защита информации от утечки* – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными) разведками и другими заинтересованными субъектами.

Примечание. Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

*Защита информации от несанкционированного воздействия; ЗИ от НСВ* – защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

*Защита информации от непреднамеренного воздействия* – защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

*Защита информации от разглашения* – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

*Защита информации от несанкционированного доступа; ЗИ от НСД* – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми докумен-

тами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Примечание. Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

*Защита информации от преднамеренного воздействия; ЗИ от ПДВ* – защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

*Защита информации от (иностранной) разведки* – защита информации, направленная на предотвращение получения защищаемой информации (иностранной) разведкой.

#### ***Термины, относящиеся к замыслу защиты информации***

*Замысел защиты информации* – основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

*Цель защиты информации* – заранее намеченный результат защиты информации.

Примечание. Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

*Система защиты информации* – совокупность органов и (или) исполнителей используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

*Политика безопасности (информации в организации)* – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

*Безопасность информации (данных)* – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

***Термины, относящиеся к объекту защиты информации***

***Объект защиты информации*** – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

***Защищаемая информация*** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Примечание. Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

***Носитель защищаемой информации*** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

***Защищаемый объект информатизации*** – объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

***Защищаемая информационная система*** – информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.

***Термины, относящиеся к угрозам безопасности информации***

***Угроза (безопасности информации)*** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

***Фактор, воздействующий на защищаемую информацию*** – явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

***Источник угрозы безопасности информации*** – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

***Уязвимость (информационной системы); брешь*** – свойство информационной системы, обуславливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

Примечание. Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или сла-

бое место в информационной системе. Если уязвимость соответствует угрозе, то существует риск.

*Вредоносная программа* – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

*Несанкционированное воздействие на информацию* – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

*Преднамеренное силовое электромагнитное воздействие на информацию* – несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем.

*Модель угроз (безопасности информации)* – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Примечание. Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ.

### ***Термины, относящиеся к технике защиты информации***

*Техника защиты информации* – средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

*Средство защиты информации* – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

*Средство контроля эффективности защиты информации* – средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации.

*Средство физической защиты информации* – средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации.

*Криптографическое средство защиты информации* – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

***Термины, относящиеся к способам оценки соответствия требованиям по защите информации***

*Оценка соответствия требованиям по защите информации* – прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации.

*Лицензирование в области защиты информации* – деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ.

*Сертификация на соответствие требованиям по безопасности информации* – форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Примечание. К объектам оценки могут относиться средство защиты информации, средство контроля эффективности защиты информации.

*Специальное исследование (объекта защиты информации)* – исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации.

*Специальная проверка* – проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

*Аудиторская проверка информационной безопасности в организации; аудит информационной безопасности в организации* – периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению информационной безопасности.

Примечание. Аудит информационной безопасности в организации может осуществляться независимой организацией (третьей стороной) по договору с проверяемой организацией, а также подразделением или должностным лицом организации (внутренний аудит).

*Мониторинг безопасности информации* – постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

*Экспертиза документа по защите информации* – рассмотрение документа по защите информации физическим или юридическим лицом, имеющим право на проведение работ в данной области, с целью подготовить соответствующее экспертное заключение.

Примечание. Экспертиза документа по защите информации может включать в себя научно-техническую, правовую, метрологическую, патентную и терминологическую экспертизу.

*Анализ информационного риска* – систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации.

*Оценка информационного риска* – общий процесс анализа информационного риска и его оценивания.

***Термины, относящиеся к эффективности защиты информации***

*Эффективность защиты информации* – степень соответствия результатов защиты информации цели защиты информации.

*Требование по защите информации* – установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

*Показатель эффективности защиты информации* – мера или характеристика для оценки эффективности защиты информации.

*Норма эффективности защиты информации* – значение показателя эффективности защиты информации, установленное нормативными и правовыми документами.

## **3.2. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ Р 50.1.053-2005 «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

### ***Сведения о стандарте***

1. Разработаны Государственным научно-исследовательским испытательным институтом проблем технической защиты информации Гостехкомиссии России.

2. Внесены Техническим комитетом по стандартизации ТК 362 «Защита информации».

3. Утверждены и введены в действие Приказом Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. № 77-ст.

4. Введены впервые.

### ***Содержание***

1. Область применения

2. Нормативные ссылки

3. Стандартизованные термины и определения

3.1. Объекты технической защиты информации

3.2. Угрозы безопасности информации

3.3. Меры технической защиты информации

Алфавитный указатель терминов

Алфавитный указатель иноязычных эквивалентов стандартизованных терминов

Приложение А (справочное) Термины и определения общетехнических понятий

Приложение Б (рекомендуемое) Схема взаимосвязи стандартизованных терминов

### ***Область применения***

Рекомендации по стандартизации устанавливают термины и определения понятий в области технической защиты информации при применении информационных технологий.

Термины, установленные данными рекомендациями по стандартизации, рекомендуются для использования во всех видах документации и литературы по вопросам технической защиты информации при применении информационных технологий, входящих в сферу работ по стандартизации и (или) использующих результаты этих работ.

Настоящие рекомендации по стандартизации должны применяться совместно с ГОСТ Р 50922.

### ***Стандартизованные термины и определения***

#### ***Объекты технической защиты информации***

*Защищаемая автоматизированная информационная система* – автоматизированная информационная система, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности.

*Защищаемые информационные ресурсы (автоматизированной информационной системы)* – информационные ресурсы автоматизированной информационной системы, для которых должен быть обеспечен требуемый уровень их защищенности.

Примечание. Информационные ресурсы включают в себя документы и массивы документов, используемые в автоматизированных информационных системах.

*Защищаемая информационная технология* – информационная технология, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности.

*Безопасность информации (данных)* – состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность.

Примечание. Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии.

*Безопасность информации (при применении информационных технологий)* – состояние защищенности информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

*Безопасность автоматизированной информационной системы* – состояние защищенности автоматизированной информационной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчетность и подлинность ее ресурсов.

*Конфиденциальность (информации (ресурсов автоматизированной информационной системы))* – состояние информации (ресурсов автоматизированной информационной системы), при кото-

ром доступ к ней (к ним) осуществляют только субъекты, имеющие на него право.

*Целостность (информации (ресурсов автоматизированной информационной системы))* – состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право.

*Доступность (информации (ресурсов автоматизированной информационной системы))* – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно.

Примечание. К правам доступа относятся право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

*Подотчетность (ресурсов автоматизированной информационной системы)* – состояние ресурсов автоматизированной информационной системы, при котором обеспечиваются их идентификация и регистрация.

*Подлинность (ресурсов автоматизированной информационной системы)* – состояние ресурсов автоматизированной информационной системы, при котором обеспечивается реализация информационной технологии с использованием именно тех ресурсов, к которым субъект, имеющий на это право, обращается.

### ***Угрозы безопасности информации***

*Угроза (безопасности информации)* – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации.

*Источник угрозы безопасности информации* – субъект, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

*Уязвимость (автоматизированной информационной системы)* – недостаток или слабое место в автоматизированной информационной системе, которые могут быть условием реализации угрозы безопасности, обрабатываемой в ней информации.

*Утечка (информации) по техническому каналу* – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

*Перехват (информации)* – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

*Информативный сигнал* – сигнал, по параметрам которого может быть определена защищаемая информация.

*Доступ (в автоматизированной информационной системе)* – получение возможности ознакомления с информацией, ее обработки и (или) воздействия на информацию и (или) ресурсы автоматизированной информационной системы с использованием программных и (или) технических средств.

Примечание. Доступ осуществляется субъектами доступа, к которым относятся лица, а также логические и физические объекты.

*Субъект доступа (в автоматизированной информационной системе)* – лицо или единица ресурса автоматизированной информационной системы, действия которой по доступу к ресурсам автоматизированной информационной системы регламентируются правилами разграничения доступа.

*Объект доступа (в автоматизированной информационной системе)* – единица ресурса автоматизированной информационной системы, доступ к которой регламентируется правилами разграничения доступа.

*Несанкционированный доступ (к информации (ресурсам автоматизированной информационной системы)); НСД* – доступ к информации (ресурсам автоматизированной информационной системы), осуществляемый с нарушением установленных прав и (или) правил доступа к информации (ресурсам автоматизированной информационной системы).

Примечания:

1. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.

2. Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них.

*Несанкционированное воздействие (на информацию (ресурсы автоматизированной информационной системы)) (при применении информационных технологий); НСВ* – изменение информации (ресурсов автоматизированной информационной системы), осуществляемое с нарушением установленных прав и (или) правил.

Примечания:

1. Несанкционированное воздействие может быть осуществлено преднамеренно или непреднамеренно. Преднамеренные несанкционированные воздействия являются специальными воздействиями.

2. Изменение может быть осуществлено в форме замены информации (ресурсов автоматизированной информационной системы), введения новой информации (новых ресурсов автоматизированной информационной системы), а также уничтожения или повреждения информации (ресурсов автоматизированной информационной системы).

*Атака (при применении информационных технологий)* – действия, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы с применением программных и (или) технических средств.

*Вторжение (в автоматизированную информационную систему)* – выявленный факт попытки несанкционированного доступа к ресурсам автоматизированной информационной системы.

*Блокирование доступа (к информации) (при применении информационных технологий)* – создание условий, препятствующих доступу к информации субъекту, имеющему право на него.

Примечание. Создание условий, препятствующих доступу к информации, может быть осуществлено по времени доступа, функциям по обработке информации (видам доступа) и (или) доступным информационным ресурсам.

*Закладочное устройство* – техническое средство, скрытно устанавливаемое на объекте информатизации или в контролируемой зоне с целью перехвата информации или несанкционированного воздействия на информацию и (или) ресурсы автоматизированной информационной системы.

Примечание. Местами установки закладочных устройств на охраняемой территории могут быть любые элементы контролируемой зоны, например, ограждение, конструкции, оборудование, предметы интерьера, транспортные средства.

*Программное воздействие* – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

*Вредоносная программа* – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия

на информацию или ресурсы автоматизированной информационной системы.

*Вирус (компьютерный)* – вредоносная программа, способная создавать вредоносные программы и (или) свои копии.

*Недекларированные возможности (программного обеспечения)* – функциональные возможности программного обеспечения, не описанные в документации.

*Программная закладка* – преднамеренно внесенные в программное обеспечение функциональные объекты, которые при определенных условиях инициируют реализацию недекларированных возможностей программного обеспечения.

Примечание. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

### ***Меры технической защиты информации***

*Техническая защита информации (ТЗИ)* – обеспечение защиты некриптографическими методами информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию и носители информации в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации.

Примечание. Техническая защита информации при применении информационных технологий осуществляется в процессах сбора, обработки, передачи, хранения, распространения информации с целью обеспечения ее безопасности на объектах информатизации.

*Политика безопасности (информации в организации)* – одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

*Профиль защиты* – совокупность типовых требований по обеспечению безопасности информации, которые должны быть реализованы в защищаемой автоматизированной информационной системе.

Примечание. Профиль защиты может разрабатываться для автоматизированной информационной системы, средства вычислительной техники, а также их технических и программных средств.

*Аудит безопасности (информации)*. – совокупность действий по независимой проверке и изучению документации автоматизированной информационной системы, а также по испытаниям средств защиты информации, направленная на обеспечение выполнения

установленной политики безопасности информации и правил эксплуатации автоматизированной информационной системы, на выявление уязвимостей автоматизированной информационной системы и на выработку рекомендаций по устранению выявленных недостатков в средствах защиты информации, политике безопасности информации и правилах эксплуатации автоматизированной информационной системы.

**Примечание.** Аудит безопасности может осуществляться независимой организацией (третьей стороной) по договору с проверяемой организацией (внешний аудит), а также подразделением или должностным лицом организации (внутренний аудит).

*Аудит безопасности автоматизированной информационной системы* – проверка реализованных в автоматизированной информационной системе процедур обеспечения безопасности с целью оценки их эффективности и корректности, а также разработки предложений по их совершенствованию.

*Мониторинг безопасности информации (при применении информационных технологий)* – процедуры регулярного наблюдения за процессом обеспечения безопасности информации при применении информационных технологий.

*Правила разграничения доступа (в автоматизированной информационной системе)* – правила, регламентирующие условия доступа субъектов доступа к объектам доступа в автоматизированной информационной системе.

*Аутентификация (субъекта доступа)* – действия по проверке подлинности субъекта доступа в автоматизированной информационной системе.

*Идентификация* – действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

### **3.1. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р 51188-1998 «ЗАЩИТА ИНФОРМАЦИИ. ИСПЫТАНИЕ ПРОГРАММНЫХ СРЕДСТВ НА НАЛИЧИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ»**

Дата введения стандарта – 1 июля 1999 г.

#### ***Сведения о стандарте***

1. Разработан и внесен 27 Центральным научно-исследовательским институтом Министерства обороны Российской Федерации (27 ЦНИИ МО РФ) и Научно-консультационным центром по созданию и применению информационных технологий (НКЦ «ЦНИИКА-СПИН»).

2. Принят и введен в действие Постановлением Госстандарта России от 14 июля 1998 г. № 295.

3. Введен впервые.

#### **1. Область применения**

Стандарт распространяется на испытания программных средств (ПС) и их компонентов, цели которых – обнаружить в этих ПС и устранить из них компьютерные вирусы (КВ) силами специальных предприятий (подразделений), и устанавливает общие требования к организации и проведению таких испытаний.

Требования, установленные стандартом, направлены на обеспечение специальной обработки ПС в целях выявления КВ, а также на устранение последствий, вызванных возможными воздействиями КВ на операционные системы, системные и пользовательские файлы с программами и данными, начальные секторы магнитных дисков, таблицы размещения файлов и др.

Стандарт устанавливает типовые требования, предъявляемые к испытаниям ПС на наличие КВ, в том числе:

- к составу мероприятий по подготовке и проведению испытаний;
- к составу, структуре и назначению основных частей программно-аппаратного стенда, обеспечивающего проведение испытаний;
- к выбору и использованию методов проведения испытаний;
- к тестовым (антивирусным) программам, обнаруживающим и уничтожающим КВ;
- к составу и содержанию документации, фиксирующей порядок проведения испытаний и их результаты.

Стандарт предназначен для применения в испытательных лабораториях, проводящих сертификационные испытания ПС на выполнение требований защиты информации.

<...>

### **3. Определения и сокращения**

В стандарте применены следующие термины с соответствующими определениями.

*Защита программных средств* – организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий.

*Сертификация* – действия третьей стороны, цель которых – подтвердить (с помощью сертификата соответствия) то, что изделие (в том числе программное средство) или услуга соответствует определенным стандартам или другим нормативным документам.

*Профилактика* – систематические действия эксплуатационного персонала, цель которых – выявить и устранить неблагоприятные изменения в свойствах и характеристиках используемых программных средств, в частности проверить эксплуатируемые, хранимые и (или) вновь полученные программные средства на наличие компьютерных вирусов.

*Ревизия* – проверка вновь полученных программ специальными средствами, проводимая путем их запуска в контролируемой среде.

*Несанкционированный доступ к программным средствам* – доступ к программам, записанным в памяти ЭВМ или на машинном носителе, а также отраженным в документации на эти программы, осуществленный с нарушением установленных правил.

*Вакцинирование* – обработка файлов, дисков, каталогов, проводимая с применением специальных программ, создающих условия, подобные тем, которые создаются определенным компьютерным вирусом, и затрудняющих повторное его появление.

*Компьютерный вирус* – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

Сокращения:

- ПС – программные средства;
- КВ – компьютерные вирусы;

- ПЭВМ – персональная электронно-вычислительная машина (персональный компьютер);
- ЭВМ – электронно-вычислительная машина.

#### ***4. Порядок проведения испытаний программных средств на наличие компьютерных вирусов***

Испытания ПС на наличие КВ следует проводить на специально оборудованном программно-аппаратном испытательном стенде, в составе которого должны быть необходимые технические и программные средства, в том числе антивирусные программы.

Предприятие (подразделение (далее – организация)), проводящее проверку ПС на наличие КВ, должно поддерживать испытательный стенд в работоспособном состоянии и не допускать проникновения КВ в программы и данные до начала проведения испытаний.

Организация, проводящая проверку ПС на наличие КВ, должна определить и зафиксировать в программе испытаний цель и объем испытаний, а также свои обязательства, касающиеся мер защиты, проверяемых ПС от их заражения КВ с учетом требований ГОСТ 19.301.

Меры по защите проверяемых ПС от заражения КВ могут включать в себя:

- разработку и выполнение комплекса мероприятий по профилактике, ревизии и вакцинированию используемых ПС;
- подготовку должностных лиц, отвечающих за проведение испытаний ПС;
- разработку и выбор способов применения программно-технических средств для обнаружения КВ в ПС;
- взаимодействие организаций, заказывающих и проводящих испытания ПС;
- контроль за проведением испытаний ПС;
- оценку эффективности применяемых антивирусных средств;
- совершенствование системы мероприятий по защите ПС от КВ на основе современных достижений информационной технологии;
- установление административной ответственности должностных лиц за выполнение требований защиты ПС от КВ;
- назначение ответственных должностных лиц и определение их полномочий, относящихся к организации и проведению мероприятий по защите ПС от КВ.

Организация, выполняющая проверку ПС на наличие КВ, должна обеспечить весь процесс проверки необходимыми вычислительными техническими и программными средствами, а также назначить специально обученных сотрудников для проведения испытаний.

Организация, выполняющая проверку ПС на наличие КВ, должна назначить постоянного представителя, который получает определенные полномочия и несет постоянную ответственность за выполнение требований, установленных настоящим стандартом.

В состав технических средств испытательного стенда должны входить:

- совместимые ПЭВМ;
- необходимые элементы телекоммуникационных сетей;
- каналы связи.

Конкретный набор технических компонентов испытательного стенда должен быть таким, чтобы были обеспечены условия воспроизведения всех необходимых внешних воздействий на ПС в процессе проведения испытаний.

Перед началом испытаний состав технических средств, используемых для проведения проверок ПС на наличие КВ, должен быть согласован с организацией, заказывающей эти проверки. При этом согласование должно быть оформлено соответствующим актом.

Помимо этого, в состав испытательного стенда могут входить соответствующие аппаратные антивирусные средства:

- компьютеры специальной конструкции, благодаря которой несанкционированный доступ к данным и заражение файлов КВ могут быть существенно затруднены;
- специальные платы, подключаемые к одному из разъемов ПЭВМ и выполняющие те или иные функции защиты информации;
- электронные ключи защиты информации, главным достоинством которых является их многофункциональность.

Состав и функциональное назначение программных средств испытательного стенда определяются системой защиты, применяемой при проведении испытаний ПС на наличие КВ.

Программные средства, входящие в состав испытательного стенда, должны обеспечивать:

- регулярное ведение архивов измененных файлов;
- контрольную проверку соответствия длины и значения контрольных сумм, указываемых в сертификате и полученных программах;

- систематическое обнуление первых трех байтов сектора начальной загрузки на полученных несистемных дискетах;
- другие виды контроля целостности программ перед считыванием с дискеты;
- проверку программ на наличие известных видов КВ;
- обнаружение попыток несанкционированного доступа к испытательным (инструментальным) и (или) испытуемым программам и данным;
- вакцинирование файлов, дисков, каталогов с использованием резидентных программ-вакцин, создающих при функционировании условия для обнаружения КВ данного вида;
- автоматический контроль целостности программ перед их запуском;
- удаление обнаруженного КВ из зараженных программ или данных и восстановление их первоначального состояния.

Состав программных средств, используемых при проведении испытаний по просьбе заказчика, должен быть документально оформлен в соответствии с требованиями заказчика.

Сроки проведения испытаний должны быть установлены в программе и методике испытаний по договоренности между заказчиком и организацией, проводящей испытания.

Проверяемые ПС должны быть переданы для испытаний на магнитных носителях (дискетах) вместе с документацией.

Состав работ по подготовке и проведению испытаний ПС на наличие КВ в общем случае следующий:

- ознакомление с документацией на ПС;
- выбор методов проверки ПС на наличие КВ;
- определение конфигурации программных и аппаратных средств испытательного стенда;
- подготовка программно-аппаратного испытательного стенда к проведению испытаний;
- организация и проведение испытаний;
- оформление протокола проверки ПС и его передача в орган по сертификации;
- передача заказчику проверенных ПС на магнитных носителях (дискетах);
- установление по согласованию с заказчиком правил (порядка) гарантийного сопровождения проверенных ПС.

Проверка ПС на наличие КВ в общем случае включает в себя:

- поиск вирусоподобных фрагментов кодов ПС;
- моделирование ситуаций, предположительно способных вызвать активизацию КВ;
- анализ особенностей взаимодействия компонентов ПС с окружающей операционной средой;
- отражение результатов проверки в соответствующей документации.

### ***5. Методы проведения испытаний программных средств на наличие компьютерных вирусов***

5.1. При испытаниях ПС на наличие КВ используют две основные группы методов обнаружения КВ и защиты программ от них: программные и аппаратно-программные.

К программным методам относятся:

- сканирование;
- обнаружение изменений;
- эвристический анализ;
- резидентные «сторожа»;
- вакцинирование ПС.

Аппаратно-программные методы основаны на реализации любого (любых) из указанных выше программных методов защиты ПС от КВ с помощью специальных технических устройств.

5.2. При выборе методов испытаний и защиты ПС от КВ следует руководствоваться сведениями о сущности каждого из них, приведенными в 5.4–5.9, а также дополнительными пояснениями об их возможностях, достоинствах и недостатках, приведенными в приложении А.

5.3. В конкретных испытаниях могут быть использованы способы и средства обнаружения КВ, реализующие один из методов, указанных в 5.1, или их комбинации.

5.4. Метод сканирования заключается в том, что специальная антивирусная программа, называемая сканером, последовательно просматривает проверяемые файлы в поиске так называемых «сигнатур» известных КВ. При этом под сигнатурой понимают уникальную последовательность байтов, принадлежащую конкретному известному КВ и не встречающуюся в других программах.

5.5. Метод обнаружения изменений заключается в том, что антивирусная программа предварительно запоминает характеристики всех областей диска, которые могут подвергаться нападению КВ, а затем периодически проверяет их. Если изменение этих характери-

стик будет обнаружено, то такая программа сообщит пользователю, что, возможно, в компьютер попал КВ.

Антивирусные программы, основанные на обнаружении изменений программной среды, называются ревизорами.

5.6. Метод эвристического анализа реализуется с помощью антивирусных программ, которые проверяют остальные программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для КВ. Так, например, эвристический анализатор может обнаружить, что в проверяемой программе присутствует код, устанавливающий резидентный модуль в памяти.

5.7. В методе резидентных сторожей используются антивирусные программы, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. Резидентный сторож сообщит пользователю о том, что какая-либо программа пытается изменить загрузочный сектор жесткого диска или дискеты, а также выполнимый файл.

5.8. Вакцинирование устанавливает способ защиты любой конкретной программы от КВ, при котором к этой программе присоединяется специальный модуль контроля, следящий за ее целостностью.

При этом проверяются контрольная сумма программы или какие-либо другие ее характеристики. Если КВ заражает вакцинированный файл, модуль контроля обнаруживает изменение контрольной суммы файла и сообщает об этом пользователю.

5.9. Аппаратно-программные методы защиты ПС от КВ реализуются с помощью специализированного устройства – контроллера, вставляемого в один из разъемов расширения компьютера, и специального программного обеспечения, управляющего работой этого контроллера и реализующего один или несколько из программных методов, указанных выше.

## ***6. Требования документации на испытания программных средств***

Документация, оформляемая при подготовке и проведении испытаний ПС на наличие КВ, должна содержать сведения, отражающие цель, объем, порядок проведения и результаты таких испытаний.

Выпуск документа вида «Протокол проверки программных средств на отсутствие компьютерных вирусов» является обязательным. Форму документа «Протокол проверки программных средств

на отсутствие компьютерных вирусов» определяют в установленном порядке и передают в орган по сертификации.

Другие виды документов, выпускаемых по результатам испытаний ПС на наличие КВ, и дополнительные требования к их содержанию определяют по согласованию между организацией, выполняющей проверку ПС, и организацией, заказывающей эту проверку.

Документация, относящаяся к испытаниям ПС на наличие КВ, может быть представлена на магнитных носителях данных.

## **ПРИЛОЖЕНИЕ А (справочное)**

### **Возможности различных методов обнаружения и устранения компьютерных вирусов**

*А.1. Метод сканирования* является самым простым программным методом поиска КВ. Антивирусные программы-сканеры могут гарантированно обнаружить только уже известные КВ, которые были предварительно изучены и для которых была определена сигнатура. Программам-сканерам не обязательно хранить в себе сигнатуры всех известных КВ. Они могут, например, хранить только контрольные суммы сигнатур. Антивирусные программы-сканеры, которые могут удалить обнаруженные КВ, обычно называются полифагами. Для эффективного использования антивирусных программ, реализующих метод сканирования, необходимо постоянно обновлять их, получая самые последние версии.

*А.2. Метод обнаружения изменений* основан на использовании антивирусных программ-ревизоров, которые запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, параметры всех контролируемых файлов, а также информацию о структуре каталогов и номера плохих кластеров диска. Могут быть проверены и другие характеристики компьютера: объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры.

Программы-ревизоры потенциально могут обнаружить любые КВ, даже те, которые ранее не были известны. Однако следует учитывать, что не все изменения вызваны вторжением КВ. Так, загрузочная запись может измениться при обновлении версии операционной системы, а некоторые программы записывают изменяемые данные внутри своего исполнимого файла. Командные файлы из-

меняются еще чаще (например, файл AUTOEXEC. BAT обычно изменяется во время установки нового программного обеспечения).

Программы-ревизоры не помогут и в том случае, когда пользователь записывает в компьютер новый файл, зараженный КВ. При этом, если КВ заразит другие программы, уже учтенные ревизором, он будет обнаружен.

Дополнительной возможностью программ-ревизоров является способность восстановить измененные (зараженные) файлы и загрузочные секторы на основании запомненной ранее информации.

Антивирусные программы-ревизоры нельзя использовать для обнаружения КВ в файлах документов, так как эти файлы постоянно изменяются. Поэтому для контроля за данными файлами следует использовать программы-сканеры или эвристический анализ.

А.3. *Эвристический анализ* позволяет обнаруживать ранее неизвестные КВ, причем для этого не надо предварительно собирать данные о файловой системе, как требует метод обнаружения изменений.

К основным недостаткам эвристического метода относятся следующие:

- принципиально не могут быть обнаружены все КВ;
- возможно появление некоторого количества ложных сигналов об обнаружении КВ в программах, использующих вирусоподобные технологии (например, антивирусы).

А.4. Большинство *резидентных сторожей* позволяет автоматически проверять все запускаемые программы на заражение известными КВ. Такая проверка будет занимать некоторое время, и процесс загрузки программы замедлится, но зато пользователь будет уверен, что известные КВ не смогут активизироваться на его компьютере.

Резидентные сторожа имеют очень много недостатков, которые делают этот класс программ малоприменимым для использования:

1. Многие программы, даже не содержащие КВ, могут выполнять действия, на которые реагируют резидентные сторожа. Например, обычная команда LABEL изменяет данные в загрузочном секторе и вызывает срабатывание сторожа. Поэтому работа пользователя будет постоянно прерываться раздражающими сообщениями антивируса. Кроме того, пользователь должен будет каждый раз решать, вызвано ли это срабатывание компьютерным вирусом или нет. Как показывает практика, рано или поздно пользователь отключает резидентный сторож.

2. Резидентные сторожа должны быть постоянно загружены в оперативную память и, следовательно, уменьшают объем памяти, доступной другим программам.

А.5. Основными недостатками *метода вакцинирования* являются возможность обхода такой защиты при использовании компьютерным вирусом так называемой «стелс-технологии», а также необходимость изменения кода программ, из-за чего некоторые программы начинают работать некорректно или могут перестать работать.

А.6. *Аппаратно-программные методы* представляют собой один из самых надежных способов защиты ПС от заражения КВ. Благодаря тому, что контроллер такой защиты подключен к системной шине компьютера, он получает полный контроль над всеми обращениями к дисковой подсистеме компьютера. Программное обеспечение аппаратной защиты позволяет указать области файловой системы, которые нельзя изменять. Пользователь может защитить главную загрузочную запись, загрузочные секторы, выполнимые файлы, файлы конфигурации и т. д. Если аппаратно-программный комплекс обнаружит, что какая-либо программа пытается нарушить установленную защиту, он может не только сообщить об этом пользователю, но и заблокировать дальнейшую работу компьютера.

Аппаратный уровень контроля за дисковой подсистемой компьютера не позволяет КВ замаскировать себя. Как только КВ проявит себя, он сразу будет обнаружен. При этом совершенно безразлично, как именно «работает» КВ и какие средства он использует для доступа к дискам и дискетам.

Аппаратно-программные средства защиты позволяют не только защитить компьютер от КВ, но также вовремя пресечь выполнение программ, нацеленных на разрушение файловой системы компьютера. Кроме того, аппаратно-программные средства позволяют защитить компьютер от неквалифицированного пользователя, не давая ему удалить важную информацию, переформатировать диск, изменить файлы конфигурации.

Недостатком аппаратно-программных методов является принципиальная возможность пропустить КВ, если они не пытаются изменять защищенные файлы и системные области.

**3.2. НАЦИОНАЛЬНЫЙ СТАНДАРТ  
РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р 51275-2006  
«ЗАЩИТА ИНФОРМАЦИИ. ОБЪЕКТ ИНФОРМАТИЗАЦИИ.  
ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ.  
ОБЩИЕ ПОЛОЖЕНИЯ»**

Дата введения – 1 февраля 2008 г.

***Сведения о стандарте***

1. Разработан Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»).

2. Внесен Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии.

3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст.

4. Взамен ГОСТ Р 51275-99.

***Содержание***

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Основные положения
5. Классификация факторов, воздействующих на безопасность защищаемой информации

6. Перечень объективных и субъективных факторов, воздействующих на безопасность защищаемой информации

6.1. Перечень объективных факторов, воздействующих на безопасность защищаемой информации

6.2. Перечень субъективных факторов, воздействующих на безопасность защищаемой информации

Библиография

***Область применения***

Стандарт устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации.

Стандарт распространяется на объекты информатизации, создаваемые и эксплуатируемые в различных областях деятельности (обороны, экономики, науки и других областях).

### ***Термины и определения***

В настоящем стандарте применены термины по ГОСТ Р 50922, а также следующие термины с соответствующими определениями:

*Объект информатизации* – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

*Система обработки информации* – совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации.

*Побочное электромагнитное излучение* – электромагнитное излучение, наблюдаемое при работе технических средств обработки информации.

*Паразитное электромагнитное излучение* – электромагнитное излучение, являющееся результатом паразитной генерации в электрических цепях технических средств обработки информации.

*Наведенный в токопроводящих линейных элементах технических средств сигнал; наводка*: ток и напряжение в токопроводящих элементах, вызванные электромагнитным излучением, емкостными и индуктивными связями.

*Закладочное средство (устройство)* – техническое средство (устройство) приема, передачи и обработки информации, преднамеренно устанавливаемое на объекте информатизации или в контролируемой зоне в целях перехвата информации или несанкционированного воздействия на информацию и (или) ресурсы автоматизированной информационной системы.

Примечание. Местами установки закладочных средств (устройств) на охраняемой территории могут быть любые элементы контролируемой зоны (например, ограждение, конструкции, оборудование, предметы интерьера, транспортные средства).

*Программная закладка* – преднамеренно внесенный в программное обеспечение функциональный объект, который при опре-

деленных условиях инициирует реализацию недекларированных возможностей программного обеспечения.

Примечание. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

*Недекларированные возможности (программного обеспечения)* – Функциональные возможности программного обеспечения, не описанные в документации.

*Вредоносная программа* – программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

*Вирус (компьютерный)* – вредоносная программа способная создавать свои копии и (или) другие вредоносные программы.

*Компьютерная атака* – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

*Сетевая атака* – компьютерная атака с использованием протоколов межсетевого взаимодействия.

*Программное воздействие* – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

### ***Основные положения***

1. Выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и проведения эффективных мероприятий, направленных на защиту информации на объекте информатизации (ОИ).

2. Полнота и достоверность выявленных факторов, воздействующих или могущих воздействовать на защищаемую информацию, достигаются путем рассмотрения полного множества факторов, воздействующих на все элементы ОИ (технические и программные средства обработки информации, средства обеспечения ОИ и т. д.) и на всех этапах обработки информации.

3. Выявление факторов, воздействующих на защищаемую информацию, должно осуществляться с учетом следующих требований:

– достаточности уровней классификации факторов, воздействующих на защищаемую информацию, позволяющих формировать их полное множество;

– гибкости классификации, позволяющей расширять множества классифицируемых факторов, группировок и признаков, а также вносить необходимые изменения без нарушения структуры классификации.

### ***Классификация факторов, воздействующих на безопасность защищаемой информации***

Факторы, воздействующие или могущие воздействовать на безопасность защищаемой информации и подлежащие учету при организации защиты информации, по признаку отношения к природе возникновения подразделяют на классы:

- объективные;
- субъективные.

По отношению к ОИ факторы, воздействующие на безопасность защищаемой информации, подразделяют на внутренние и внешние.

Факторы, воздействующие на безопасность защищаемой информации, в соответствии с признаками классификации подразделяют:

- на подклассы;
- группы;
- подгруппы;
- виды;
- подвиды.

Перечень основных подклассов (групп, подгрупп и т. д.) факторов, воздействующих на безопасность защищаемой информации (объективных и субъективных), в соответствии с их классификацией представлен в разделе 6.

<...>

### ***Раздел 6. Перечень объективных и субъективных факторов, воздействующих на безопасность защищаемой информации***

6.1. Перечень объективных факторов, воздействующих на безопасность защищаемой информации

6.1.1. Внутренние факторы

6.1.1.1. Передача сигналов:

- а) по проводным линиям связи;
- б) по оптико-волоконным линиям связи;
- в) в диапазоне радиоволн и в оптическом диапазоне длин волн.

6.1.1.2. Излучения сигналов, функционально присущие техническим средствам (устройствам) (далее – ТС) ОИ:

а) излучения акустических сигналов:

1) сопутствующие работе технических средств (устройств) обработки и передачи информации (далее – ТС ОПИ);

2) сопутствующие произносимой или воспроизводимой ТС речи;

б) электромагнитные излучения и поля:

1) излучения в радиодиапазоне;

2) излучения в оптическом диапазоне.

6.1.1.3. Побочные электромагнитные излучения:

а) элементов (устройств) ТС ОПИ;

б) на частотах работы высокочастотных генераторов устройств, входящих в состав ТС ОПИ:

1) модуляция побочных электромагнитных излучений информативным сигналом, сопровождающим работу ТС ОПИ;

2) модуляция побочных электромагнитных излучений акустическим сигналом, сопровождающим работу ТС ОПИ;

в) на частотах самовозбуждения усилителей, входящих в состав ТС ОПИ.

6.1.1.4. Паразитное электромагнитное излучение:

а) модуляция паразитного электромагнитного излучения информационными сигналами;

б) модуляция паразитного электромагнитного излучения акустическими сигналами.

6.1.1.5. Наводка:

а) в электрических цепях ТС, имеющих выход за пределы ОИ;

б) в линиях связи:

1) вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию;

2) вызванная внутренними емкостными и (или) индуктивными связями;

в) в цепях электропитания:

1) вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию;

2) вызванная внутренними емкостными и (или) индуктивными связями;

3) через блоки питания ТС ОИ;

г) в цепях заземления:

1) вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию;

2) вызванная внутренними емкостными и (или) индуктивными связями;

3) обусловленная гальванической связью схемной (рабочей) «земли» узлов и блоков ТС ОИ;

д) в технических средствах, проводах, кабелях и иных токопроводящих коммуникациях и конструкциях, гальванически не связанных с ТС ОИ, вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию.

6.1.1.6. Наличие акустоэлектрических преобразователей в элементах ТС ОИ.

6.1.1.7. Дефекты, сбои и отказы, аварии ТС и систем ОИ.

6.1.1.8. Дефекты, сбои и отказы программного обеспечения ОИ.

6.1.2. Внешние факторы

6.1.2.1. Явления техногенного характера:

а) непреднамеренные электромагнитные облучения ОИ;

б) радиационные облучения ОИ;

в) сбои, отказы и аварии систем обеспечения ОИ.

6.1.2.2. Природные явления, стихийные бедствия:

а) термические факторы (пожары и т. д.);

б) климатические факторы (наводнения и т. д.);

в) механические факторы (землетрясения и т. д.);

г) электромагнитные факторы (грозовые разряды и т. д.);

д) биологические факторы (микробы, грызуны и т. д.);

е) химические факторы (химически агрессивные среды и т. д.).

6.2. Перечень субъективных факторов, воздействующих на безопасность защищаемой информации

6.2.1. Внутренние факторы

6.2.1.1. Разглашение защищаемой информации лицами, имеющими к ней право доступа, через:

а) лиц, не имеющих права доступа к защищаемой информации;

б) передачу информации по открытым линиям связи;

в) обработку информации на незащищенных ТС обработки информации;

г) опубликование информации в открытой печати и других средствах массовой информации;

д) копирование информации на незарегистрированный носитель информации;

е) передачу носителя информации лицам, не имеющим права доступа к ней;

ж) утрату носителя информации.

6.2.1.2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации, путем:

- а) несанкционированного изменения информации;
- б) несанкционированного копирования защищаемой информации.

6.2.1.3. Несанкционированный доступ к информации путем:

- а) подключения к техническим средствам и системам ОИ;
- б) использования закладочных средств (устройств);
- в) использования программного обеспечения технических средств ОИ через:

- 1) маскировку под зарегистрированного пользователя;
- 2) дефекты и уязвимости программного обеспечения ОИ;
- 3) внесение программных закладок;
- 4) применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

г) хищения носителя защищаемой информации;

д) нарушения функционирования ТС обработки информации.

6.2.1.4. Недостатки организационного обеспечения защиты информации при:

- а) задании требований по защите информации (требования противоречивы, не обеспечивают эффективную защиту информации);
- б) несоблюдении требований по защите информации;
- в) контроле эффективности защиты информации.

6.2.1.5. Ошибки обслуживающего персонала ОИ при:

- а) эксплуатации ТС;
- б) эксплуатации программных средств;
- в) эксплуатации средств и систем защиты информации.

6.2.2. Внешние факторы

6.2.2.1. Доступ к защищаемой информации с применением технических средств:

- а) разведки:
  - 1) радиоэлектронной;
  - 2) оптико-электронной;
  - 3) фотографической;
  - 4) визуально-оптической;
  - 5) акустической;
  - 6) гидроакустической;
  - 7) технической компьютерной;
- б) съема информации.

6.2.2.2. Несанкционированный доступ к защищаемой информации путем:

- а) подключения к техническим средствам и системам ОИ;
- б) использования закладочных средств (устройств);
- в) использования программного обеспечения технических средств ОИ через:

- 1) маскировку под зарегистрированного пользователя;
- 2) дефекты и уязвимости программного обеспечения ОИ;
- 3) внесение программных закладок;
- 4) применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

- г) несанкционированного физического доступа к ОИ;

- д) хищения носителя информации.

6.2.2.3. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.

6.2.2.4. Действия криминальных групп и отдельных преступных субъектов:

- а) диверсия в отношении ОИ;

- б) диверсия в отношении элементов ОИ.

6.2.2.5. Искажение, уничтожение или блокирование информации с применением технических средств путем:

- а) преднамеренного силового электромагнитного воздействия:

- 1) по сети электропитания на порты электропитания постоянного и переменного тока;

- 2) по проводным линиям связи на порты ввода-вывода сигналов и порты связи;

- 3) по металлоконструкциям на порты заземления и порты корпуса;

- 4) посредством электромагнитного быстроизменяющегося поля на порты корпуса, порты ввода-вывода сигналов и порты связи;

- б) преднамеренного силового воздействия различной физической природы;

- в) использования программных или программно-аппаратных средств при осуществлении:

- 1) компьютерной атаки;

- 2) сетевой атаки;

- г) воздействия программными средствами в комплексе с преднамеренным силовым электромагнитным воздействием.

**3.5. НАЦИОНАЛЬНЫЙ СТАНДАРТ  
РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р ИСО/МЭК 15408-2008  
«ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. МЕТОДЫ  
И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.  
КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»**

Если имеют в виду все три части стандарта, используют обозначение ИСО/МЭК 15408.

***Сведения о стандарте***

1. Подготовлен Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»), Федеральным государственным учреждением «4 Центральный научно-исследовательский институт Министерства обороны России» (ФГУ «4 ЦНИИ Минобороны России»), Федеральным государственным унитарным предприятием «Научно-технический и сертификационный центр по комплексной защите информации» ФГУП Центр «Атомзащитаинформ», Федеральным государственным унитарным предприятием «Центральный научно-исследовательский институт управления, экономики и информации Росатома» (ФГУП «ЦНИИАТОМИНФОРМ») при участии экспертов Международной рабочей группы по общим критериям на основе собственного аутентичного перевода стандарта, указанного в пункте 4.

2. Внесен Техническим комитетом по стандартизации ТК 362 «Защита информации».

3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 519-ст.

4. Стандарт идентичен международному стандарту ИСО/МЭК 15408-1:2005 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» (ISO/IEC 15408-1:2005 «Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model»).

При применении стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении С.

ИСО/МЭК 15408 под общим наименованием «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» состоит из следующих частей:

- 1 часть. Введение и общая модель;
- 2 часть. Функциональные требования безопасности;
- 3 часть. Требования доверия к безопасности.

ИСО/МЭК 15408 дает возможность сравнения результатов независимых оценок безопасности. Это достигается предоставлением общего набора требований к функциям безопасности продуктов или систем ИТ и мерам доверия, применяемым к ним при оценке безопасности. В процессе оценки достигается определенный уровень уверенности в том, что функции безопасности таких продуктов или систем, а также предпринимаемые меры доверия отвечают предъявляемым требованиям. Результаты оценки могут помочь потребителям решить, являются ли продукты или системы ИТ достаточно безопасными для их предполагаемого применения и приемлемы ли прогнозируемые риски при их использовании.

ИСО/МЭК 15408 полезен в качестве руководства как при разработке продуктов или систем с функциями безопасности ИТ, так и при приобретении коммерческих продуктов или систем с функциями безопасности. При оценке продукт или систему ИТ с функциями безопасности называют объектом оценки (ОО). К таким ОО, например, относятся операционные системы, вычислительные сети, распределенные системы и приложения.

ИСО/МЭК 15408 направлен на защиту информации от несанкционированного раскрытия, модификации или потери возможности ее использования. Характеристики защищенности, относящиеся к данным трем типам нарушения безопасности, обычно называют конфиденциальностью, целостностью и доступностью соответственно. ИСО/МЭК 15408 может быть также применим к тем аспектам безопасности ИТ, которые выходят за пределы этих трех понятий. ИСО/МЭК 15408 сосредоточен на угрозах информации, возникающих в результате действий человека как злоумышленных, так и иных, но возможно также применение ИСО/МЭК 15408 и для некоторых угроз, не связанных с человеческим фактором. Кроме того, ИСО/МЭК 15408 может быть применим и в других областях ИТ, но не декларируется их правомочность вне строго ограниченной сферы безопасности ИТ.

ИСО/МЭК 15408 применим к мерам безопасности ИТ, реализуемым аппаратными, программно-аппаратными и программными средствами. Если предполагается, что отдельные аспекты оценки применимы только для некоторых способов реализации, это будет отмечено при изложении соответствующих критериев.

### ***Область применения***

ИСО/МЭК 15408 предназначен для использования в качестве основы при оценке характеристик безопасности продуктов или систем информационных технологий (ИТ). Устанавливая общую базу критериев, ИСО/МЭК 15408 позволяет сделать результаты оценки безопасности ИТ значимыми для более широкой аудитории.

Некоторые вопросы рассматриваются как лежащие вне области действия ИСО/МЭК 15408, поскольку они требуют привлечения специальных методов или являются смежными по отношению к безопасности ИТ. Часть из них перечислена ниже:

- ИСО/МЭК 15408 не содержит критериев оценки безопасности, касающихся административных мер безопасности, непосредственно не относящихся к мерам безопасности ИТ. Известно, что безопасность ОО в значительной степени может быть достигнута административными мерами, такими как организационные меры, меры управления персоналом, меры управления физической защитой и процедурные меры. Административные меры безопасности в среде эксплуатации ОО рассматриваются в качестве предположений о безопасном использовании там, где они влияют на способность мер безопасности ИТ противостоять установленным угрозам;

- оценка специальных физических аспектов безопасности ИТ, таких как контроль электромагнитного излучения, прямо не затрагивается, хотя многие концепции ИСО/МЭК 15408 применимы и в этой области. В частности, рассмотрены некоторые аспекты физической защиты ОО;

- в ИСО/МЭК 15408 не рассматривается ни методология оценки, ни административно-правовая структура, в рамках которой критерии могут применяться органами оценки. Тем не менее, ИСО/МЭК 15408 может использоваться для целей оценки в контексте такой структуры и такой методологии;

- процедуры использования результатов оценки безопасности при аттестации продуктов и систем ИТ находятся вне области действия ИСО/МЭК 15408. Аттестация продукта или системы ИТ является административным процессом, посредством которого предоставляются полномочия на их использование в конкретной среде

эксплуатации. Оценка концентрируется на тех аспектах безопасности продукта или системы ИТ и среды эксплуатации, которые могут непосредственно влиять на безопасное использование элементов ИТ. Результаты процесса оценки безопасности являются, следовательно, важными исходными материалами для процесса аттестации. Однако, поскольку для оценки не связанных с ИТ характеристик безопасности продукта или системы, а также их соотнесения с аспектами безопасности ИТ более приемлемы другие способы, аттестующим следует предусмотреть для этих аспектов особый подход.

– ИСО/МЭК 15408 не включает в себя критерии для оценки специфических качеств криптографических алгоритмов. Если требуется независимая оценка математических свойств криптографии, встроенной в ОО, то в системе оценки, в рамках которой применяется ИСО/МЭК 15408, должно быть предусмотрено проведение таких оценок.

ИСО/МЭК 15408 состоит из трех отдельных, но взаимосвязанных частей.

– часть 1 «Введение и общая модель» является введением в ИСО/МЭК 15408. В ней определены общие принципы и концепции оценки безопасности ИТ и приведена общая модель оценки. Представлены конструкции для выражения целей безопасности ИТ, выбора и определения требований безопасности ИТ и написания высокоуровневых спецификаций для продуктов и систем. Кроме того, в этой части указано, в чем заключается полезность каждой из частей ИСО/МЭК 15408 применительно к каждой из основных групп пользователей ИСО/МЭК 15408;

– часть 2 «Функциональные требования безопасности» устанавливает совокупность функциональных компонентов как стандартный способ выражения функциональных требований к ОО и содержит каталог всех функциональных компонентов, семейств и классов;

– часть 3 «Требования доверия к безопасности» устанавливает совокупность компонентов доверия как стандартный способ выражения требований доверия к ОО и содержит каталог всех компонентов, семейств и классов доверия. Кроме того, в данной части определены критерии оценки профилей защиты и заданий по безопасности и представлены оценочные уровни доверия (ОУД), которые устанавливают predeterminedную в ИСО/МЭК 15408 шкалу ранжирования доверия к ОО.

В таблице показано, в каком качестве различные части ИСО/МЭК 15408 будут представлять интерес для каждой из трех основных групп пользователей ИСО/МЭК 15408.

**Путеводитель по критериям оценки безопасности  
информационных технологий**

Часть	Потребитель	Разработчик	Оценщик
1	Общие сведения по применению. Руководство по структуре профилей защиты	Общие сведения и руководство по разработке требований и формулированию спецификаций безопасности для объектов оценки	Общие сведения и руководство по применению. Руководство по структуре профилей защиты и заданий по безопасности
2	Руководство и справочник по формулированию требований к функциям безопасности	Справочник по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки	Критерии оценки, используемые при определении эффективности выполнения объектом оценки заявленных функций безопасности
3	Руководство по определению требуемого уровня доверия	Справочник по интерпретации требований доверия и определению подходов к установлению доверия к объектам оценки	Критерии оценки, используемые при определении доверия к объектам оценки и оценке профилей защиты и заданий по безопасности

**3.5.1. Национальный стандарт Российской Федерации  
ГОСТ Р ИСО/МЭК 15408-1-2008**

**«Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»**

Дата введения – 1 октября 2009 г.

Первая часть ИСО/МЭК 15408 устанавливает две формы представления функциональных требований и требований доверия к безопасности ИТ. Конструкция «профиль защиты» (ПЗ) предусматривает создание обобщенного, предназначенного для многократного использования набора этих требований безопасности. ПЗ может быть использован предполагаемыми потребителями для спецификации и идентификации продуктов с характеристиками безопасности ИТ, которые будут удовлетворять их потребностям. Задание по безопасности (ЗБ) содержит требования безопасности и специфицирует

функции безопасности для конкретного продукта или системы, подлежащих оценке и называемых объектом оценки (ОО). ЗБ используется оценщиками в качестве основы для оценки, проводимой в соответствии с ИСО/МЭК 15408.

### ***Термины и определения***

*Активы* – информация или ресурсы, подлежащие защите контрмерами ОО.

*Назначение* – спецификация определенного параметра в компоненте.

*Доверие* – основание для уверенности в том, что сущность отвечает своим целям безопасности.

*Потенциал нападения* – прогнозируемый потенциал для успешного (в случае реализации) нападения, выраженный в показателях компетентности, ресурсов и мотивации нарушителя.

*Усиление* – добавление одного или нескольких компонентов доверия из ИСО/МЭК 15408-3 в оценочный уровень доверия (ОУД) или пакет требований доверия.

*Аутентификационные данные* – информация, используемая для верификации предъявленного идентификатора пользователя.

*Уполномоченный пользователь* – пользователь, которому в соответствии с политикой безопасности объекта оценки (ПБО) разрешено выполнять некоторую операцию.

*Класс* – группа семейств, объединенных общим назначением.

*Компонент* – наименьшая выбираемая совокупность элементов, которая может быть включена в профиль защиты (ПЗ), задание по безопасности (ЗБ) или пакет.

*Связность* – свойство объекта оценки (ОО), позволяющее ему взаимодействовать с сущностями ИТ, внешними по отношению к ОО. Данное взаимодействие включает в себя обмен данными по проводным или беспроводным средствам на любом расстоянии, в любой среде или при любой конфигурации.

*Зависимость* – соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть, как правило, удовлетворено с тем, чтобы и другие требования могли отвечать своим целям.

*Элемент* – неделимое требование безопасности.

*Оценка* – оценка ПЗ, ЗБ или ОО по определенным критериям.

*Оценочный уровень доверия* – пакет компонентов доверия из ИСО/МЭК 15408-3, представляющий некоторое положение на определенной в ИСО/МЭК 15408 шкале доверия.

*Орган оценки* – организация, которая посредством системы оценки обеспечивает реализацию ИСО/МЭК 15408 для определенного сообщества и в связи с этим устанавливает стандарты и контролирует качество оценок, проводимых организациями в пределах данного сообщества.

*Система оценки* – административно-правовая структура, в рамках которой в определенном сообществе органы оценки применяют ИСО/МЭК 15408.

*Расширение* – добавление в ЗБ или ПЗ функциональных требований, не содержащихся в ИСО/МЭК 15408-2, и/или требований доверия, не содержащихся в ИСО/МЭК 15408-3.

*Внешняя сущность ИТ* – любой продукт или система ИТ, доверенные или нет, находящиеся вне ОО и взаимодействующие с ним.

*Семейство* – группа компонентов, которые направлены на достижение одних и тех же целей безопасности, но могут отличаться акцентами или строгостью.

*Формальный* – выраженный на языке с ограниченным синтаксисом и определенной семантикой, основанной на установившихся математических понятиях.

*Документация руководств* – документация руководств, описывающая поставку, установку, конфигурирование, эксплуатацию, управление и использование ОО в той части, в которой эти виды деятельности имеют отношение к пользователям, администраторам и интеграторам ОО. Требования к области применения и содержанию документированных руководств определяются в ПЗ и ЗБ.

*Человек-пользователь* – любое лицо, взаимодействующее с ОО.

*Идентификатор* – представление уполномоченного пользователя (например, строка символов), однозначно его идентифицирующее. Таким представлением может быть полное или сокращенное имя этого пользователя или его псевдоним.

*Неформальный* – выраженный на естественном языке.

*Внутренний канал связи* – канал связи между разделенными частями ОО.

*Передача в пределах ОО* – передача данных между разделенными частями ОО.

*Передача между ФБО* – передача данных между функциями безопасности объекта оценки (ФБО) и функциями безопасности других доверенных продуктов ИТ.

*Итерация* – более чем однократное использование компонента при различном выполнении операций.

*Объект* – сущность в пределах области действия ФБО (ОДФ), которая содержит или получает информацию и над которой субъекты выполняют операции.

*Политика безопасности организации* – одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

*Пакет* – предназначенная для многократного использования совокупность функциональных компонентов или компонентов доверия, объединенных для удовлетворения совокупности определенных целей безопасности.

*Продукт* – совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы.

*Профиль защиты* – независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя.

*Монитор обращений* – концепция абстрактной машины, осуществляющей политики управления доступом ОО.

*Механизм проверки правомочности обращений* – реализация концепции монитора обращений, обладающая следующими свойствами: защищенностью от проникновения; постоянной готовностью; простотой, достаточной для проведения исчерпывающего анализа и тестирования.

*Уточнение* – дополнение компонента деталями.

*Роль* – заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и ОО.

*Секрет* – информация, которая должна быть известна только уполномоченным пользователям и/или ФБО для осуществления определенной политики функции безопасности (ПФБ).

*Атрибут безопасности* – характеристики субъектов, пользователей объектов, информации и/или ресурсов, которые используются для осуществления ПБО.

*Функция безопасности* – функциональные возможности части или частей ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО.

*Политика функции безопасности* – политика безопасности, осуществляемая функцией безопасности (ФБ).

*Цель безопасности* – изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям.

*Задание по безопасности* – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО.

*Выбор* – выделение одного или нескольких элементов из перечня в компоненте.

*Полуформальный* – выраженный на языке с ограниченным синтаксисом и определенной семантикой.

*Базовая СФБ* – уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения.

*Высокая СФБ* – уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения.

*Средняя СФБ* – уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения.

*Стойкость функции безопасности* – характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного поведения при прямой атаке на лежащие в ее основе механизмы безопасности.

*Субъект* – сущность в пределах ОДФ, инициирующая выполнение операций.

*Система* – специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

*Объект оценки* – продукт или система ИТ и связанная с ними документация руководств, являющиеся предметом оценки.

*Ресурс ОО* – все, что может быть использовано или потреблено ОО.

*Функции безопасности ОО* – совокупность всех функций безопасности ОО, направленных на осуществление ПБО.

*Интерфейс функций безопасности ОО* – совокупность интерфейсов как интерактивных (человеко-машинные интерфейсы), так и

программных (интерфейсы прикладных программ), с использованием которых осуществляется доступ к ресурсам ОО при посредничестве ФБО или получение от ФБО какой-либо информации.

*Политика безопасности ОО* – совокупность правил, регулирующих управление активами, их защиту и распределение в пределах ОО.

*Модель политики безопасности ОО* – структурированное представление политики безопасности, которая должна быть осуществлена ОО.

*Передача за пределы области действия ФБО* – передача данных сущностям, не контролируемым ФБО.

*Доверенный канал* – средство взаимодействия между ФБО и удаленным доверенным продуктом ИТ, обеспечивающее необходимую степень уверенности в поддержании ПБО.

*Доверенный маршрут* – средство взаимодействия между пользователем и ФБО, обеспечивающее необходимую степень уверенности в поддержании ПБО.

*Данные ФБО* – данные, созданные ФБО или для ФБО, которые могут повлиять на выполнение ФБО.

*Область действия ФБО* – совокупность возможных взаимодействий с ОО или в его пределах, которые подчинены правилам ПБО.

*Пользователь* – любая сущность (человек-пользователь или внешняя сущность ИТ) вне ОО, которая взаимодействует с ОО.

*Данные пользователя* – данные, созданные пользователем и для пользователя, которые не влияют на выполнение ФБО.

#### Обозначения и сокращения

Сокращения	Обозначения
ЗБ	Задание по безопасности
ИТ	Информационная технология
ИФБО	Интерфейс функции безопасности объекта оценки
ОДФ	Область действия функции безопасности объекта оценки
ОО	Объект оценки
ОУД	Оценочный уровень доверия
ПБО	Политика безопасности объекта оценки
ПЗ	Профиль защиты
ПФБ	Политика функции безопасности
СФБ	Стойкость функции безопасности
ФБ	Функция безопасности
ФБО	Функции безопасности объекта оценки

### ***Краткий обзор***

В разделе определены категории пользователей, контекст оценки и принятый подход к представлению материала.

Информация, содержащаяся в системах или продуктах ИТ, является критическим ресурсом, позволяющим организациям успешно решать свои задачи. Кроме того, частные лица вправе ожидать, что их персональная информация, размещенная в продуктах или системах ИТ, останется приватной, доступной им по мере необходимости и не будет подвергнута несанкционированной модификации.

При выполнении продуктами или системами ИТ своих функций следует осуществлять надлежащее управление информацией для обеспечения ее защиты от опасностей нежелательного или неоправданного распространения, изменения или потери. Термин «безопасность ИТ» используется для того, чтобы рассмотреть предотвращение и уменьшение этих и подобных опасностей.

Чтобы повысить свою уверенность в мерах безопасности продукта или системы ИТ, потребители могут заказать проведение анализа безопасности этого продукта или системы (т. е. оценку безопасности).

ИСО/МЭК 15408 может использоваться для выбора приемлемых мер безопасности ИТ. В нем содержатся критерии оценки требований безопасности.

В оценке характеристик безопасности продуктов и систем ИТ заинтересованы в основном потребители, разработчики и оценщики. Критерии, изложенные в стандарте, структурированы в интересах этих групп, потому что именно они рассматриваются как основные группы пользователей ИСО/МЭК 15408.

ИСО/МЭК 15408 не содержит требований к правовой базе. Однако согласованность правовой базы различных органов оценки является необходимым условием достижения взаимного признания результатов оценок. Основные элементы формирования контекста для оценок показаны на рис. 1.

Использование общей методологии оценки позволяет достичь повторяемости и объективности результатов, но только этого недостаточно. Многие критерии оценки требуют привлечения экспертных решений и базовых знаний, добиться согласованности которых бывает нелегко. Для повышения согласованности выводов, полученных при оценке, ее конечные результаты могут быть представлены на сертификацию. Процедура сертификации представляет собой независимую экспертизу результатов оценки, которая заверша-

ется их утверждением или выдачей сертификата. Сведения о сертификатах обычно публикуются и являются общедоступными. Сертификация является средством обеспечения большей согласованности в применении критериев безопасности ИТ.



Рис. 1. Контекст оценки

Система оценки, методология и процедуры сертификации находятся в ведении органов оценки, управляющих системами оценки, и выходят за рамки действия ИСО/МЭК 15408.

### ***Общая модель***

Безопасность рассматривается в ИСО/МЭК 15408 с использованием совокупности понятий и терминологии в области безопасности. Их понимание является предпосылкой эффективного использования ИСО/МЭК 15408.

Безопасность связана с защитой активов от угроз, при этом угрозы классифицированы на основе потенциала злоупотребления защищаемыми активами. Во внимание следует принимать все разновидности угроз, но в сфере безопасности наибольшее внимание уделяется тем из них, которые связаны со злонамеренными или иными действиями человека. Высокоуровневые понятия безопасности и их взаимосвязь представлены на рис. 2.

За сохранность рассматриваемых активов отвечают их владельцы, для которых эти активы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельцев. Владельцы будут воспринимать подобные угрозы как потенциал воздействия на активы, приводящего к понижению их ценности для владельцев. К специфическим нарушениям безопасности обычно относят (но не ограничиваются) – наносящее ущерб раскры-

тие актива несанкционированным получателям (потеря конфиденциальности), ущерб активу вследствие несанкционированной модификации (потеря целостности) или несанкционированное лишение доступа к активу (потеря доступности).

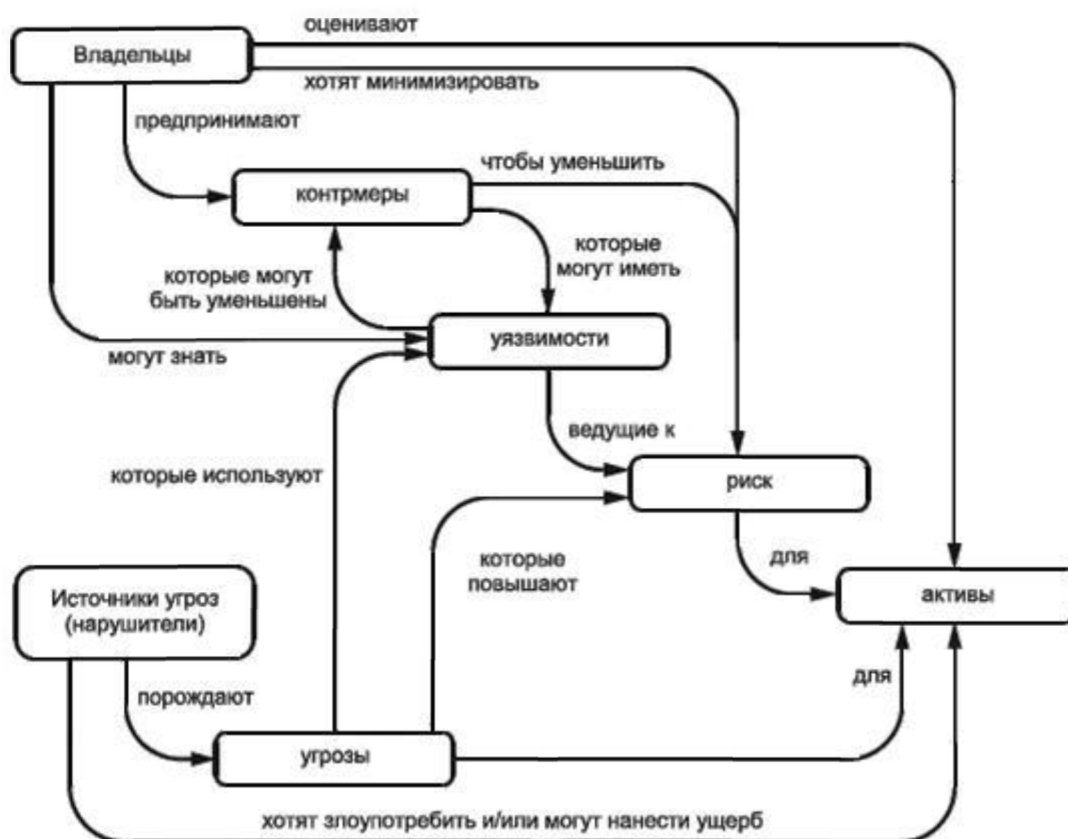


Рис. 2. Понятия безопасности и их взаимосвязь

Владельцы активов будут анализировать угрозы, применимые к их активам и среде, определяя связанные с ними риски. Анализ угроз может помочь при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня.

Контрмеры предпринимают для уменьшения уязвимостей и выполнения политики безопасности владельцев активов (прямо или косвенно распределяя их между этими составляющими). Но и после введения контрмер могут сохраняться остаточные уязвимости. Такие уязвимости могут использоваться нарушителями, определяя уровень остаточного риска для активов. Владельцы будут стремиться минимизировать этот риск с учетом имеющихся ограничений.

Прежде чем подвергнуть активы опасности воздействия выявленных угроз, владельцам активов необходимо убедиться, что принятые контрмеры обеспечат адекватное противостояние этим угрозам. Сами владельцы активов не всегда в состоянии судить обо

всех аспектах предпринимаемых контрмер и поэтому могут потребовать проведение их оценки. Результатом такой оценки является заключение о степени доверия контрмерам по уменьшению рисков для защищаемых активов. В данном заключении устанавливают уровень доверия как результат применения контрмер. Доверие является той характеристикой контрмер, которая дает основание для уверенности в их надлежащем действии. Заключение о результатах оценки может быть использовано владельцем активов при принятии решения о приемлемости риска для активов, создаваемого угрозами. Взаимосвязь данных понятий, используемых при оценке, представлена на рис. 3.

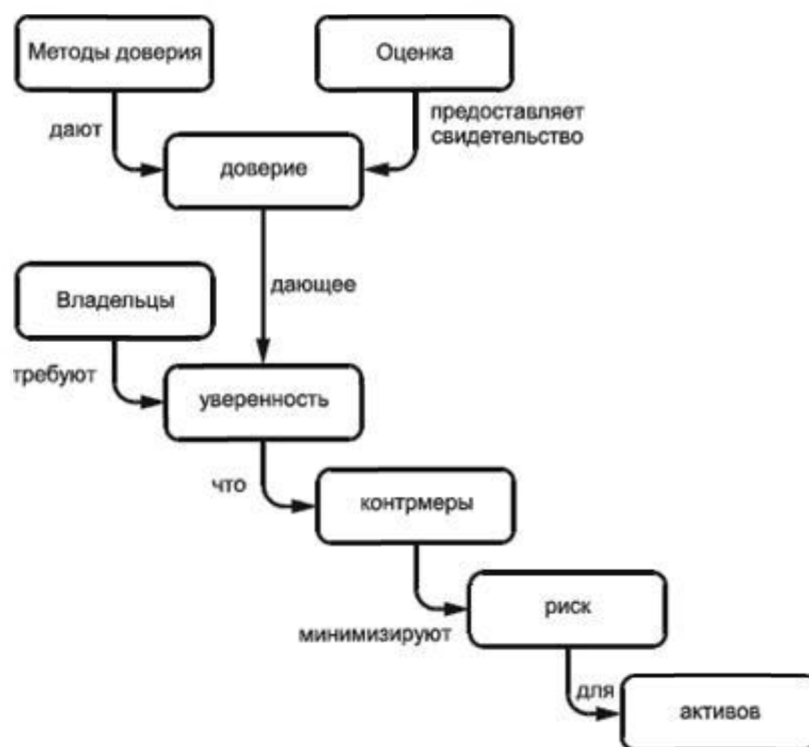


Рис. 3. Понятия, используемые при оценке, и их взаимосвязь

Поскольку ответственность за активы несут их владельцы, им следует иметь возможность отстаивать принятое решение о приемлемости для активов риска, создаваемого угрозами. Для этого требуется, чтобы результаты оценки были обоснованными. Следовательно, оценка должна приводить к объективным и повторяемым результатам, что позволит использовать их в качестве доказательств.

Уверенность в безопасности ИТ может быть достигнута в результате действий, предпринятых в процессе разработки, оценки и эксплуатации ОО.

ИСО/МЭК 15408 не предписывает конкретную методологию разработки или модель жизненного цикла. основополагающие предположения о соотношениях между требованиями безопасности и собственно ОО представлены на рис. 4.

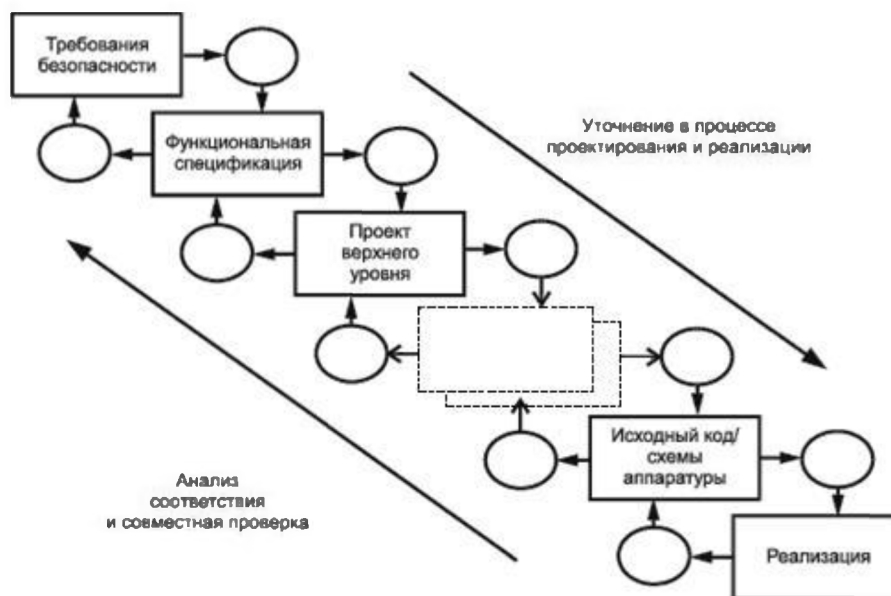


Рис. 4. Модель разработки ОО

Процесс оценки ОО, как показано на рис. 5, может проводиться параллельно с разработкой или следовать за ней. Основными исходными материалами для оценки ОО являются:

- совокупность свидетельств, характеризующих ОО, включая ЗБ в качестве основы оценки ОО;
- ОО, безопасность которого требуется оценить;
- критерии, методология и система оценки.

Потребители могут выбрать оцененный продукт для использования в конкретных условиях. Не исключено, что при эксплуатации ОО могут быть выявлены не обнаруженные до этого ошибки или уязвимости, а также может возникнуть необходимость пересмотра предположений относительно среды функционирования. Тогда по результатам эксплуатации потребуется внесение разработчиком исправлений в ОО либо переопределение требований безопасности или предположений относительно среды эксплуатации. Такие изменения могут привести к необходимости проведения новой оценки ОО или потребовать повышения безопасности среды его эксплуата-

ции. В некоторых случаях для восстановления доверия к ОО достаточно оценить только требующиеся обновления. Детальное описание процедур переоценки, включая использование результатов ранее проведенных оценок, выходит за рамки ИСО/МЭК 15408.

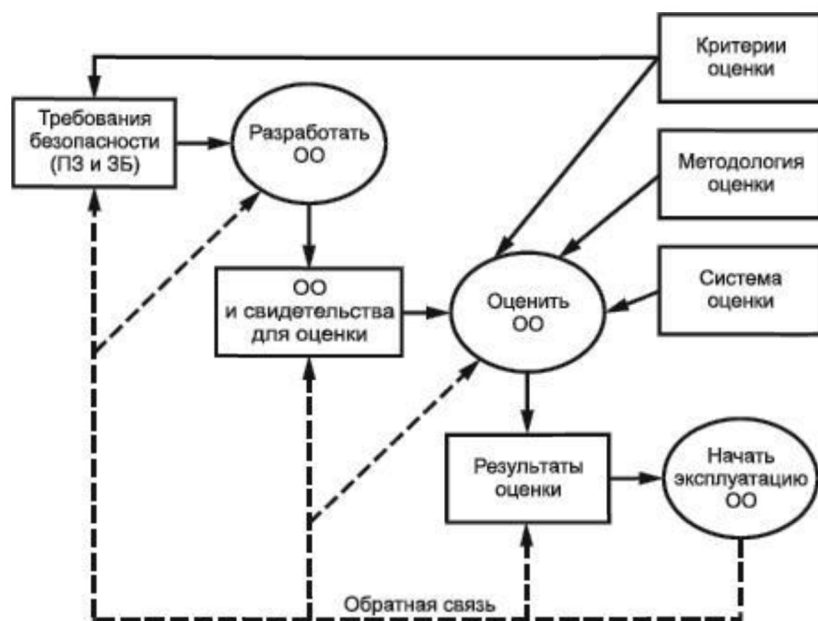


Рис. 5. Процесс оценки ОО

### ***Требования ИСО/МЭК 15408 и результаты оценки***

В разделе представлены ожидаемые результаты оценки ПЗ и ОО. Оценки профилей защиты или объектов оценки позволяют создавать каталоги ПЗ или ОО, прошедших оценку. Оценка ЗБ дает промежуточные результаты, которые затем используют при оценке ОО.

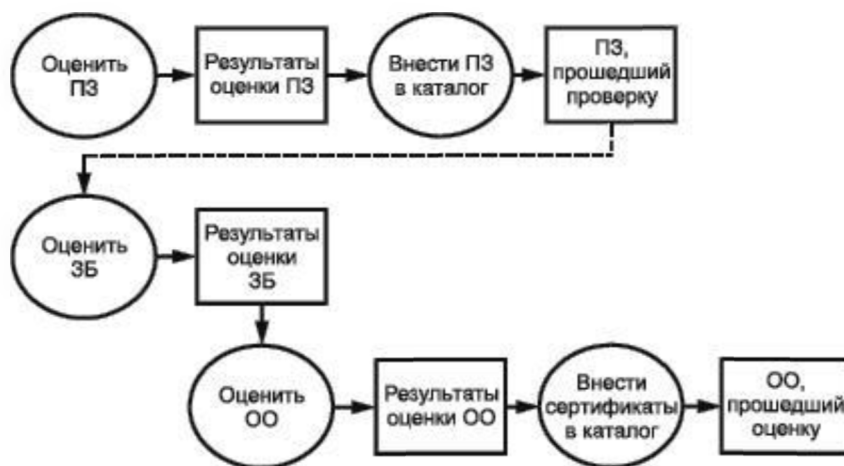


Рис. 6. Результаты оценки

Необходимо, чтобы оценка ПЗ и ОО приводила к объективным и повторяемым результатам, на которые затем можно ссылаться как на свидетельство даже при отсутствии объективной шкалы для представления результатов оценки безопасности ИТ. Наличие совокупности критериев оценки является необходимым предварительным условием для того, чтобы оценка приводила к значимому результату, предоставляя техническую основу для взаимного признания результатов оценки различными органами оценки. Практическое применение критериев включает в себя как объективные, так и субъективные элементы оценки, поэтому получение абсолютно точных и универсальных рейтингов безопасности ИТ невозможно.

Рейтинг, полученный в соответствии с ИСО/МЭК 15408, представляет итоговые данные специфического типа исследования характеристик безопасности ОО. Такой рейтинг не гарантирует пригодность к использованию в какой-либо конкретной среде применения. Решение о приемке ОО к использованию в конкретной среде применения основывается на учете многих аспектов безопасности, включая также выводы оценки.

**3.5.2. Национальный стандарт Российской Федерации  
ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология.  
Методы и средства обеспечения безопасности.  
Критерии оценки безопасности информационных технологий.  
Часть 2. Функциональные компоненты безопасности»**

Дата введения – 1 сентября 2014 г.

1. Подготовлен Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»).

2. Внесен Техническим комитетом по стандартизации «Защита информации» ТК 362.

3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 г. №1339-ст.

4. Настоящий стандарт идентичен международному стандарту ИСО/МЭК 15408-2:2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности

информационных технологий. Часть 2. Функциональные компоненты безопасности» (ISO/IEC 15408-2:2008 «Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components»).

5. Взамен ГОСТ Р ИСО/МЭК 15408-2-2008.

### ***Область применения***

Стандарт устанавливает структуру и содержание компонентов функциональных требований безопасности для оценки безопасности. Он также включает в себя каталог функциональных компонентов, отвечающих общим требованиям к функциональным возможностям безопасности многих продуктов и систем ИТ.

### ***Краткий обзор***

ИСО/МЭК 15408-2 и соответствующие функциональные требования безопасности не предназначены для окончательного решения всех задач безопасности ИТ. Скорее стандарт предлагает совокупность хорошо продуманных функциональных требований безопасности, которые могут применяться при создании доверенных продуктов или систем ИТ, отвечающих потребностям рынка. Эти функциональные требования безопасности представляют современный уровень спецификации требований и оценки.

В стандарт предполагалось включать только те функциональные требования безопасности, которые на момент издания стандарта были известны и одобрены его разработчиками.

Так как знания и потребности пользователей могут меняться, функциональные требования, представленные в стандарте, нуждаются в дальнейшем сопровождении.

Предполагается, что некоторые разработчики ПЗ/ЗБ могут иметь потребности в безопасности, не охваченные компонентами функциональных требований, представленными в стандарте. В данном случае разработчик ПЗ/ЗБ может предпочесть использование нестандартных функциональных требований (так называемую «расширяемость») в соответствии с ИСО/МЭК 15408-1, приложения А и В.

### ***Структура***

В разделе 5 описывается парадигма, используемая в функциональных компонентах безопасности данной части ИСО/МЭК 15408.

Раздел 6 представляет каталог функциональных компонентов.

В разделах 7–17 приведено описание функциональных классов.

Приложение А содержит пояснительную информацию для потенциальных пользователей функциональных компонентов, вклю-

чая таблицы перекрестных ссылок зависимостей функциональных компонентов.

Приложения В–М представляют пояснительную информацию для функциональных классов. Этот материал должен рассматриваться в качестве нормативных инструкций по применению соответствующих операций и выбору необходимой информации для аудита и документирования; конкретная инструкция является предпочтительной, но и другие могут быть обоснованы. Когда даются различные варианты, выбор остается за автором ПЗ / ЗБ.

### ***Парадигма функциональных требований***

Стандарт содержит каталог функциональных компонентов безопасности, которые могут быть предъявлены к объекту оценки (ОО). ОО – это набор программных, аппаратно-программных и/или аппаратных средств, сопровождаемый руководствами пользователя и администратора. ОО может включать ресурсы в виде электронных носителей данных (таких, как основная память, дисковое пространство), периферийных устройств (таких, как принтеры) и вычислительных возможностей (таких, как процессорное время), которые могут использоваться для обработки и хранения информации и являются предметом оценки.

Оценка прежде всего подтверждает, что в отношении ресурсов ОО применяется определенный набор *функциональных требований безопасности* (ФТБ). ФТБ определяют правила, по которым ОО управляет использованием и доступом к своим ресурсам и, таким образом, к информации и сервисам, контролируемым ОО.

ФТБ могут определять различные *политики функций безопасности* (ПФБ). Каждая такая ПФБ должна специфицировать свою область действия, определяющую субъекты, объекты, ресурсы или информацию и операции, по отношению к которым она применяется. Все ПФБ реализуются ФБО (см. ниже), чьи механизмы осуществляют правила, определенные в ФТБ, и предоставляют необходимые возможности.

В совокупности те части ОО, которые направлены на корректную реализацию ФТБ, определяются как *функции безопасности объекта оценки* (ФБО). ФБО объединяют функциональные возможности всех аппаратных, программных и программно-аппаратных средств ОО, на которые как непосредственно, так и косвенно возложено обеспечение безопасности.

ОО может быть единым продуктом, включающим аппаратные, программно-аппаратные и программные средства.

В ином случае ОО может быть распределенным, состоящим из нескольких разделенных частей. Каждая часть ОО обеспечивает выполнение конкретного сервиса для ОО и взаимодействуют с другими частями ОО через *внутренний канал связи*. Этот канал может быть всего лишь шиной процессора, а может являться внутренней сетью для ОО.

Если ОО состоит из нескольких частей, то каждая часть может иметь собственное подмножество ФБО, которое обменивается данными ФБО и пользователей через внутренние каналы связи с другими подмножествами ФБО. Это взаимодействие называется *внутренней передачей ОО*. В этом случае части ФБО формируют объединенные ФБО, которые реализуют ФТБ для этого ОО.

Интерфейсы ОО могут быть локализованы в конкретном ОО или же могут допускать взаимодействие с другими продуктами ИТ по *внешним каналам связи*. Внешние взаимодействия с другими продуктами ИТ могут принимать две формы:

- ФТБ другого «доверенного продукта ИТ» и ФТБ рассматриваемого ОО скоординированы и оценены в административном порядке, и предполагается, что рассматриваемый другой «доверенный продукт ИТ» реализует свои ФТБ корректно (например, был отдельно оценен). Обмен информацией в этом случае назван *передачей между ФБО*, поскольку он осуществляется между ФБО различных доверенных продуктов;

- другой продукт ИТ может быть недоверенным, он может быть обозначен как «недоверенный продукт ИТ». Поэтому его ФТБ либо неизвестны, либо их реализация не рассматривается как в достаточной степени доверенная. Опосредованный ФБО обмен информацией в этом случае назван *передачей за пределы ОО*, так как рассматриваемый другой продукт ИТ не имеет ФБО (или характеристики его политики безопасности неизвестны).

Совокупность интерфейсов как интерактивных (человеко-машинный интерфейс), так и программных (интерфейс программных приложений), через которые могут быть получены доступ к ресурсам при посредничестве ФБО или информация от ФБО, называется *интерфейсом ФБО (ИФБО)*. ИФБО определяет границы функциональных возможностей ОО, которые предоставлены для реализации ФТБ.

Пользователи не включаются в состав ОО. Однако пользователи взаимодействуют с ОО, который является предметом применения правил, определенных в ФТБ, через ИФБО при запросе услуг,

которые будут выполняться ОО. Существуют два типа пользователей, учитываемых в настоящем стандарте: *человек-пользователь* и *внешняя сущность ИТ*. Человека-пользователя можно далее дифференцировать как локального человека-пользователя, взаимодействующего непосредственно с ОО через устройства ОО (такие, как рабочие станции), и как *удаленного человека-пользователя*, взаимодействующего с ОО через другой продукт ИТ.

Период взаимодействия пользователя и ФБО называется *сеансом пользователя*. Открытие сеансов пользователей может контролироваться на основе ряда условий, таких как аутентификация пользователя, время суток, метод доступа к ОО, число разрешенных параллельных сеансов (для каждого пользователя или в целом).

В стандарте используется термин *уполномоченный* для обозначения пользователя, который обладает правами и/или привилегиями, необходимыми для выполнения операций. Поэтому термин *уполномоченный пользователь* указывает, что пользователю разрешается выполнять конкретную операцию или совокупность операций в соответствии с ФТБ.

Для выражения требований разделения административных обязанностей соответствующие функциональные компоненты безопасности (из семейства FMT\_SMR) явно устанавливают обязательность административных *ролей*. Роль – это заранее определенная совокупность правил, устанавливающих допустимые взаимодействия пользователя, действующего в данной роли, и ОО. ОО может поддерживать определение произвольного числа ролей. Например, роли, связанные с операциями безопасности ОО, могут включать в себя роли «Администратор аудита» и «Администратор учета пользователей».

ОО содержит ресурсы, которые могут использоваться для обработки и хранения информации. Основной целью ФБО является полная и правильная реализация ФТБ для ресурсов и информации, которыми управляет ОО.

Ресурсы ОО могут иметь различную структуру и использоваться различными способами. Тем не менее в настоящем стандарте проводится специальное разграничение, позволяющее специфицировать желательные свойства безопасности. Все сущности, которые могут быть созданы на основе ресурсов, характеризуются одним из двух способов. Сущности могут быть активными, т. е. являться причиной действий, которые происходят в пределах ОО, и инициировать операции, выполняемые с информацией. Напротив, сущности

могут быть пассивными, т. е. являться контейнером – источником информации или контейнером – местом хранения информации.

Активные сущности в ОО, которые выполняют операции над объектами, названы *субъектами*. В пределах ОО могут существовать несколько типов субъектов:

- действующие от имени уполномоченного пользователя (например, процессы UNIX);

- действующие как особый функциональный процесс, который может, в свою очередь, действовать от имени многих пользователей (например, функции, которые характерны для архитектуры клиент/сервер);

- действующие как часть собственно ОО (например, процессы, действующие не от имени пользователя).

В стандарте рассматривается реализация ФТБ для субъектов всех типов, перечисленных выше.

Пассивные сущности (в ОО, которые хранят или получают информацию), над которыми субъекты выполняют операции, названы *объектами* в функциональных требованиях безопасности настоящего стандарта. В случае, когда субъект (активная сущность) сам является предметом операции (например, при установлении связи между процессами), над субъектом могут производиться действия как над объектом.

Объекты могут содержать *информацию*. Это понятие требуется, чтобы специфицировать политики управления информационными потоками в соответствии с классом FDP.

Пользователи, субъекты, информация, объекты, сеансы и ресурсы, контролируемые посредством правил, в ФТБ могут обладать определенными *атрибутами*, которые содержат информацию, используемую ОО для правильного функционирования. Некоторые атрибуты, такие как имена файлов, могут предназначаться только для информирования или использоваться для идентификации отдельных ресурсов, в то время как другие, например, различные параметры управления доступом, – исключительно для реализации ФТБ. Эти последние обобщенно названы «*атрибутами безопасности*». В дальнейшем слово «атрибут» используется в некоторых местах настоящего стандарта как сокращение для словосочетания «атрибут безопасности». Вместе с тем, независимо от предназначения информации атрибута, могут потребоваться средства управления этим атрибутом в соответствии с ФТБ.

В ОО содержатся данные пользователей и данные ФБО. На рис. 1 показана их взаимосвязь. *Данные пользователей* – это информация, содержащаяся в ресурсах ОО, которая может применяться пользователями в соответствии с ФТБ и не предназначена специально для ФБО. Например, содержание сообщения электронной почты является данными пользователя. *Данные ФБО* – это информация, используемая ФБО для принятия решения в соответствии с ФТБ. Допустимо воздействие пользователей на данные ФБО, если это разрешено ФТБ. Примерами данных ФБО являются атрибуты безопасности, аутентификационные данные, переменные внутреннего состояния ФБО, используемые в соответствии с правилами, определенными в ФТБ, или для защиты ФБО, а также списки управления доступом.

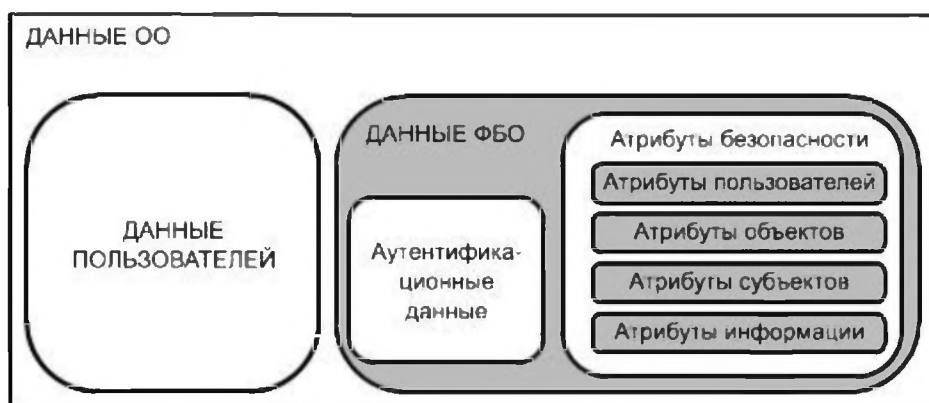


Рис. 1. Связь между данными пользователей и данными ФБО

Выделяются ПФБ, которые применяются при защите данных, такие как *ПФБ управления доступом* и *ПФБ управления информационными потоками*. Действия механизмов, реализующих ПФБ управления доступом, основаны на атрибутах пользователей, ресурсов, субъектов, объектов, сеансов, данных состояния ФБО и операций в пределах области действия. Эти атрибуты используются в совокупности правил, управляющих операциями, которые субъектам разрешено выполнять на объектах.

Функционирование механизмов, реализующих ПФБ управления информационными потоками, основано на атрибутах субъектов и информации в пределах области действия и совокупности правил, по которым выполняются операции субъектов над информацией. Атрибуты информации, которые могут быть ассоциированы с атрибутами места хранения (контейнерами) или могут быть производными от данных в контейнере, остаются с информацией при ее об-

работке ФБО. Два специфических типа данных ФБО, рассматриваемых в настоящем стандарте, могут, хотя и необязательно, совпадать. Это *аутентификационные данные* и *секреты*.

Аутентификационные данные используются, чтобы верифицировать заявленный идентификатор пользователя, обращающегося к ОО за услугами. Самая распространенная форма аутентификационных данных – пароль, который необходимо хранить в секрете, чтобы механизм безопасности был эффективен. Однако в секрете необходимо хранить не все формы аутентификационных данных. Биометрические опознавательные устройства (такие, как считыватели отпечатка пальца или сканеры сетчатки глаза) основываются не на предположении, что аутентификационные данные хранятся в секрете, а на том, что эти данные являются неотъемлемым свойством пользователя, которое невозможно подделать. Термин «секрет», используемый в стандарте по отношению к аутентификационным данным, применим и к данным других типов, которые необходимо хранить в тайне при осуществлении определенной ПФБ. Например, стойкость механизма доверенного канала, в котором применена криптография для сохранения конфиденциальности передаваемой через канал информации, зависит от надежности способа сохранения в секрете криптографических ключей от несанкционированного раскрытия.

Следовательно, некоторые, но не все аутентификационные данные необходимо хранить в секрете, и некоторые, но не все секреты используют как аутентификационные данные. Рис. 2 показывает эту взаимосвязь секретов и аутентификационных данных. На этом рисунке указаны типы данных, которые часто относят к аутентификационным данным и секретам.

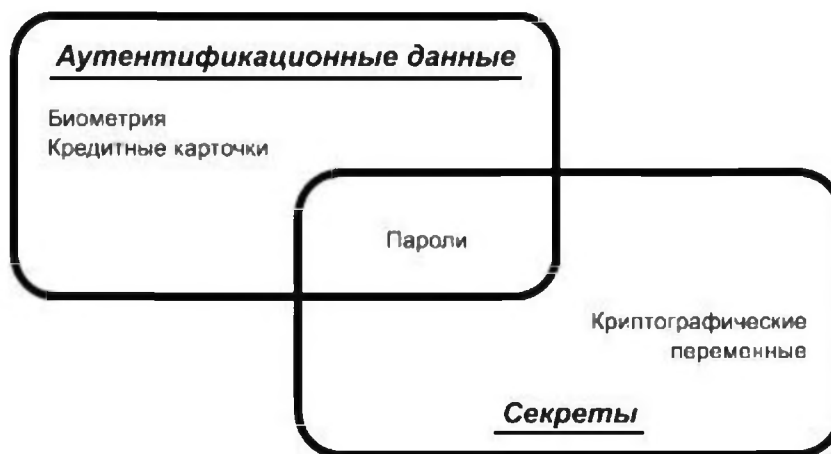


Рис. 2. Связь между понятиями «аутентификационные данные» и «секреты»

### ***Функциональные компоненты безопасности***

Раздел определяет содержание и форму представления функциональных требований настоящего стандарта и предоставляет руководство по организации требований для новых компонентов, включаемых в ЗБ. Функциональные требования объединены в классы, семейства и компоненты.

Структура функционального класса приведена на рисунке. Каждый функциональный класс содержит имя класса, представление класса и одно или несколько функциональных семейств.



Рис. 3. Структура функционального класса

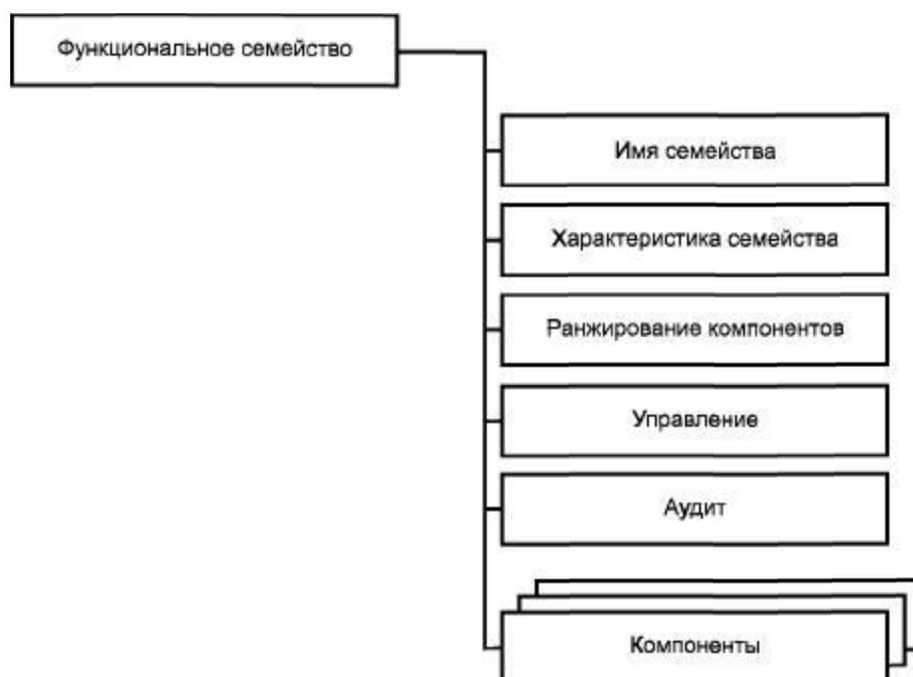


Рис. 4. Структура функционального семейства

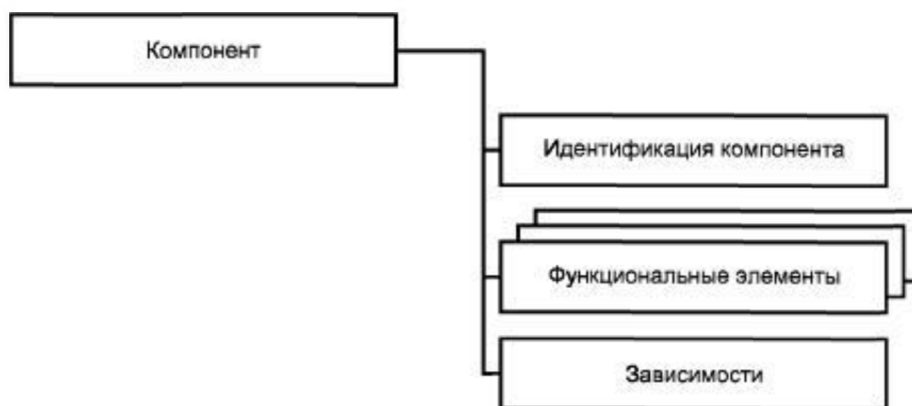


Рис. 5. Структура функционального компонента

Далее приведено описание функциональных классов.

***Класс FAU. Аудит безопасности***

Аудит безопасности включает в себя распознавание, запись, хранение и анализ информации, связанной с действиями, относящимися к безопасности (например, с действиями, контролируруемыми ПБО). Записи аудита, получаемые в результате, могут быть проанализированы с тем, чтобы определить, какие действия, относящиеся к безопасности, происходили, и кто из пользователей за них отвечает.

***Класс FCO. Связь***

Класс FCO содержит два семейства, связанные с уверенностью в идентичности сторон, участвующих в обмене данными: идентичностью отправителя переданной информации (доказательство отправления) и идентичностью получателя переданной информации (доказательство получения). Эти семейства обеспечивают то, что отправитель не сможет отрицать факт отправления сообщения, а получатель не сможет отрицать факт его получения.

***Класс FCS. Криптографическая поддержка***

ФБО могут использовать криптографические функциональные возможности для содействия достижению некоторых, наиболее важных целей безопасности. К ним относятся (но ими не ограничиваются) следующие цели: идентификация и аутентификация, неотказуемость, доверенный маршрут, доверенный канал, разделение данных. Класс FCS применяют, если ОО имеет криптографические функции, которые могут быть реализованы аппаратными, программно-аппаратными и/или программными средствами. Класс FCS «Криптографическая поддержка» состоит из двух семейств: FCS\_CKM «Управление криптографическими ключами» и FCS\_COP «Криптографические операции». В семействе FCS\_CKM

«Управление криптографическими ключами» рассмотрены аспекты управления криптографическими ключами, тогда как в семействе FCS\_COP «Криптографические операции» рассмотрено практическое применение этих криптографических ключей.

***Класс FDP. Защита данных пользователя***

Класс FDP «Защита данных пользователя» содержит семейства, определяющие требования к функциям безопасности ОО и политикам функций безопасности ОО, связанным с защитой данных пользователя. Он разбит на четыре группы семейств.

***Класс FIA. Идентификация и аутентификация***

Семейства класса FIA содержат требования к функциям установления и верификации заявленного идентификатора пользователя.

Идентификация и аутентификация требуются для обеспечения ассоциации пользователей с соответствующими атрибутами безопасности (такими как идентификатор, группы, роли, уровни безопасности или целостности).

Однозначная идентификация уполномоченных пользователей и правильная ассоциация атрибутов безопасности с пользователями и субъектами критичны для осуществления принятых политик безопасности. Семейства этого класса связаны с определением и верификацией идентификаторов пользователей, определением их полномочий на взаимодействие с ОО, а также с правильной ассоциацией атрибутов безопасности с каждым уполномоченным пользователем. Эффективность требований других классов (таких как «Защита данных пользователя», «Аудит безопасности») во многом зависит от правильно проведенных идентификации и аутентификации пользователей.

***Класс FMT. Управление безопасностью***

Класс FMT предназначен для спецификации управления некоторыми аспектами ФБО: атрибутами безопасности, данными и отдельными функциями. Могут быть установлены различные роли управления, а также определено их взаимодействие, например, распределение обязанностей.

Класс FMT позволяет решать следующие задачи:

- управление данными ФБО, которые включают в себя, например, предупреждающие сообщения;
- управление атрибутами безопасности, которые включают в себя, например, списки управления доступом и перечни возможностей;

- управление функциями из числа ФБО, которое включает в себя, например, выбор функций, а также правил или условий, влияющих на режим выполнения ФБО;
- определение ролей безопасности.

### ***Класс FPR. Приватность***

Класс FPR содержит требования приватности. Эти требования предоставляют пользователю защиту от раскрытия его идентификатора и злоупотребления этим другими пользователями.

### ***Класс FPT. Защита ФБО***

Класс FPT содержит семейства функциональных требований, связанных с целостностью и управлением механизмами, реализованными в ФБО (не завися при этом от особенностей ПБО), а также с целостностью данных ФБО (не завися от специфического содержания данных ПБО). В некотором смысле, компоненты семейств этого класса дублируют компоненты из класса FDP и могут даже использовать одни и те же механизмы. Однако класс FDP «Защита данных пользователя» сфокусирован на защите данных пользователя, в то время как класс FPT «Защита ФБО» – на защите данных ФБО. Фактически, компоненты из класса FPT необходимы для обеспечения требований невозможности нарушения и обхода политик ФБ данного ОО.

В рамках данного класса выделяют три важные составные части ФБО:

- 1) *абстрактная машина ФБО*, т. е. виртуальная или физическая машина, на которой выполняется оцениваемая реализация ФБО;
- 2) *реализация ФБО*, которая выполняется на абстрактной машине и реализует механизмы, осуществляющие ПБО;
- 3) *данные ФБО*, которые являются административными базами данных, управляющими осуществлением ПБО.

### ***Класс FRU. Использование ресурсов***

Класс FRU содержит три семейства, которые поддерживают доступность требуемых ресурсов, таких как вычислительные возможности и/или объем памяти. Семейство FRU\_FLT «Отказоустойчивость» предоставляет защиту от недоступности ресурсов, вызванной сбоем ОО. Семейство FRU\_PRS «Приоритет обслуживания» обеспечивает, чтобы ресурсы выделялись наиболее важным или критичным по времени задачам и не могли быть монополизированы задачами с более низким приоритетом. Семейство FRU\_RSA «Распределение ресурсов» устанавливает ограничения использования доступ-

ных ресурсов, предотвращая монополизацию ресурсов пользователями.

### ***Класс FTA. Доступ к ОО***

Класс FTA определяет функциональные требования к управлению открытием сеанса пользователя.

### ***Класс FTP. Доверенный маршрут/канал***

Семейства класса FTP содержат требования как к доверенному маршруту связи между пользователями и ФБО, так и к доверенному каналу связи между ФБО и другими доверенными продуктами ИТ. Доверенные маршруты и каналы имеют следующие общие свойства:

- маршрут связи создается с использованием внутренних и внешних каналов связи (в соответствии с компонентом), которые изолируют идентифицированное подмножество данных и команд ФБО от остальной части данных пользователей и ФБО;
- использование маршрута связи может быть инициировано пользователем и/или ФБО (в соответствии с компонентом);
- маршрут связи способен обеспечить доверие тому, что пользователь взаимодействует с требуемыми ФБО или ФБО – с требуемым пользователем (в соответствии с компонентом).

В данной парадигме доверенный канал – это канал связи, который может быть инициирован любой из связывающихся сторон и обеспечивает характеристики неотказуемости по отношению к идентификационным признакам сторон канала.

Доверенный маршрут предоставляет пользователям средства для выполнения функций путем обеспечения прямого взаимодействия с ФБО. Доверенный маршрут обычно желателен при начальной идентификации и/или аутентификации пользователя, но может быть также применен на протяжении всего сеанса пользователя. Обмены по доверенному маршруту могут быть инициированы пользователем или ФБО. Гарантируется, что ответы пользователя с применением доверенного маршрута будут защищены от модификации или раскрытия недоверенными приложениями.

### ***Приложение А (обязательное)***

Приложение содержит дополнительное руководство по использованию семейств и компонентов, определенных в разделах настоящего стандарта, которое может понадобиться потребителям, разработчикам или оценщикам при использовании компонентов. Для упрощения поиска требуемой информации порядок следования

классов, семейств и компонентов в приложениях тот же, что и в разделах настоящего стандарта.

**Приложения В–М** содержат информацию для функциональных классов. Этот материал должен рассматриваться в качестве нормативных инструкций по применению соответствующих операций и выбору необходимой информации для аудита и документирования; использование глагола «следует» означает, что конкретная инструкция является предпочтительной, но и другие могут быть обоснованы. В случае, если приводят различные варианты, выбор остается за автором ПЗ/ЗБ.

**3.5.3. Национальный стандарт Российской Федерации  
ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология.  
Методы и средства обеспечения безопасности. Критерии оценки  
безопасности информационных технологий.  
Часть 3. Требования доверия к безопасности»**

Дата введения – 1 октября 2009 г.

***Сведения о стандарте***

1. Подготовлен Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»), Федеральным государственным учреждением «4 Центральный научно-исследовательский институт Министерства обороны России» (ФГУ «4 ЦНИИ Минобороны России»), Федеральным государственным унитарным предприятием «Научно-технический и сертификационный центр по комплексной защите информации» ФГУП Центр «Атомзащитаинформ», Федеральным государственным унитарным предприятием «Центральный научно-исследовательский институт управления, экономики и информации Росатома» (ФГУП «ЦНИИАТОМИНФОРМ») при участии экспертов Международной рабочей группы по Общим критериям на основе собственного аутентичного перевода стандарта, указанного в пункте 4.

2. Внесен техническим комитетом по стандартизации ТК 362 «Защита информации».

3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 521-ст.

4. Настоящий стандарт идентичен международному стандарту ИСО/МЭК 15408-3:2005 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности

информационных технологий. Часть 3. Требования доверия к безопасности» (ISO/IEC 15408-3:2005 «Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements»).

5. Взамен ГОСТ Р ИСО/МЭК 15408-3-2002.

Стандарт состоит из следующих частей:

- часть 1. Введение и общая модель;
- часть 2. Функциональные требования безопасности;
- часть 3. Требования доверия к безопасности.

Компоненты доверия к безопасности, определенные в данной части ИСО/МЭК 15408, являются основой для выражения требований доверия к безопасности в профиле защиты (ПЗ) или задании по безопасности (ЗБ).

Данные требования устанавливают стандартный способ выражения требований доверия для объекта оценки (ОО). Данная часть ИСО/МЭК 15408 каталогизирует наборы компонентов, семейств и классов доверия. Данная часть ИСО/МЭК 15408 также определяет критерии для оценки ПЗ и ЗБ и представляет оценочные уровни доверия, которые определяют предопределенную ИСО/МЭК 15408 шкалу для рейтинга доверия к ОО, называемую «оценочными уровнями доверия» (ОУД).

Аудитория для этой части ИСО/МЭК 15408 включает в себя потребителей, разработчиков и оценщиков безопасных ИТ-систем и продуктов. Дополнительная информация о потенциальных пользователях ИСО/МЭК 15408 и использовании ИСО/МЭК 15408 группами, которые включают в себя потенциальных пользователей, представлена в ИСО/МЭК 15408-1, раздел 4.

Эти группы могут использовать данную часть ИСО/МЭК 15408 следующим образом:

- потребители используют данную часть ИСО/МЭК 15408, выбирая компоненты, чтобы сформулировать требования доверия для удовлетворения целей безопасности, приведенных в ПЗ или ЗБ, определяя требуемые уровни доверия к безопасности ОО. Более подробная информация о взаимосвязях требований безопасности и целей безопасности приведена в ИСО/МЭК 15408-1, подраздел 5.3;
- разработчики, несущие ответственность за выполнение существующих или предполагаемых требований безопасности потребителя при разработке ОО, ссылаются на данную часть ИСО/МЭК 15408, интерпретируя утверждения требований доверия и определяя подходы доверия к ОО;

– оценщики используют требования доверия, определенные в данной части ИСО/МЭК 15408, как обязательное утверждение критериев оценки, которые определяют доверие к ОО и оценивание ПЗ и ЗБ.

### ***Область применения***

Настоящий стандарт устанавливает требования доверия ИСО/МЭК 15408 и включает в себя оценочные уровни доверия (ОУД), определяющие шкалу для измерения доверия, собственно компоненты доверия, из которых составлены уровни доверия, и критерии для оценки ПЗ и ЗБ.

### ***Структура стандарта***

В разделе 5 приведено описание парадигмы, используемой в требованиях доверия к безопасности настоящего стандарта.

В разделе 6 приведена структура представления классов, семейств и компонентов доверия, оценочных уровней доверия и их взаимосвязь, а также дана характеристика классам и семействам доверия, представленным в разделах 12-18.

В разделах 7, 8 и 9 приведено краткое введение в критерии оценки ПЗ и ЗБ, сопровождаемое подробными объяснениями семейств и компонентов, применяемых для этих оценок.

В разделе 10 приведены детализированные определения оценочных уровней доверия.

В разделе 11 приведено краткое введение в классы доверия, за которым следуют разделы с 12 по 18, содержащие детализированные определения этих классов доверия.

В приложении А приведена сводка зависимостей между компонентами доверия.

В приложении В приведены перекрестные ссылки между ОУД и компонентами доверия.

### ***Парадигма доверия***

Цель данного раздела состоит в изложении основных принципов и подходов к установлению доверия к безопасности. Данный раздел позволит понять логику построения требований доверия в стандарте.

Основные принципы стандарта состоят в том, что следует четко сформулировать угрозы безопасности и положения политики безопасности организации, а достаточность предложенных мер безопасности должна быть продемонстрирована.

Более того, следует принять меры по уменьшению вероятности наличия уязвимостей, возможности их проявления (т. е. преднаме-

ренного использования или непреднамеренной активизации), а также степени ущерба, который может явиться следствием проявления уязвимостей. Дополнительно следует предпринять меры по облегчению последующей идентификации уязвимостей, а также их устранению, ослаблению и/или оповещению об их использовании или активизации.

### ***Подход к доверию***

Основная концепция стандарта– обеспечение доверия, основанное на оценке (активном исследовании) продукта или системы ИТ, которые должны соответствовать определенным критериям безопасности. Оценка была традиционным способом обеспечения доверия и являлась основой предшествующих критериев оценки. Для согласования с существующими подходами в стандарте принят тот же основной принцип.

Предполагается, что проверку правильности документации и разработанного продукта или системы ИТ будут проводить опытные оценщики, уделяя особое внимание области, глубине и строгости оценки.

Стандарт не отрицает и не комментирует относительные достоинства других способов получения доверия. Продолжаются исследования альтернативных путей достижения доверия. Если в результате этих исследований будут выявлены другие отработанные альтернативные подходы, то они могут в дальнейшем быть включены в стандарт, который структурно организован так, что предусматривает такую возможность.

### ***Значимость уязвимостей***

Предполагается, что существуют нарушители, которые будут пытаться активно использовать возможности нарушения политики безопасности как для получения незаконной выгоды, так и для незапланированных, но, тем не менее, опасных действий. Нарушители могут также случайно активизировать уязвимости безопасности, причиняя вред организации. При необходимости обрабатывать чувствительную информацию и отсутствии в достаточной степени доверенных продуктов или систем имеется значительный риск из-за отказов ИТ. Поэтому нарушения безопасности ИТ могут вызвать значительные потери.

Нарушения безопасности ИТ возникают вследствие преднамеренного использования или случайной активизации уязвимостей при применении ИТ по назначению.

Следует предпринять ряд шагов для предотвращения уязвимостей, возникающих в продуктах и системах ИТ. По возможности уязвимости должны быть:

- устранены, т. е. следует предпринять активные действия для выявления, а затем удаления или нейтрализации всех уязвимостей, которые могут проявиться;
- минимизированы, т. е. следует предпринять активные действия для снижения до допустимого остаточного уровня возможного ущерба от любого проявления уязвимостей;
- отслежены, т. е. следует предпринять активные действия для обнаружения любой попытки использовать оставшиеся уязвимости с тем, чтобы ограничить ущерб.

### ***Причины уязвимостей***

Уязвимости могут возникать из-за недостатков:

- требований, т. е. продукт или система ИТ могут обладать требуемыми от них функциями и свойствами, но содержать уязвимости, которые делают их непригодными или неэффективными в части безопасности;
- проектирования, т. е. продукт или система ИТ не отвечают спецификации, и/или уязвимости являются следствием некачественных стандартов проектирования или неправильных проектных решений;
- эксплуатации, т. е. продукт или система ИТ разработаны в полном соответствии с корректными спецификациями, но уязвимости возникают как результат неадекватного управления при эксплуатации.

### ***Доверие в стандарте***

Доверие – основа для уверенности в том, что продукт или система ИТ отвечают целям безопасности. Доверие могло бы быть получено путем обращения к таким источникам, как бездоказательное утверждение, предшествующий аналогичный опыт или специфический опыт. Однако стандарт обеспечивает доверие с использованием активного исследования. Активное исследование – это оценка продукта или системы ИТ для определения его свойств безопасности.

### ***Доверие через оценку***

Оценка является традиционным способом достижения доверия, и она положена в основу стандарта. Методы оценки могут, в частности, включать в себя:

- анализ и проверку процессов и процедур;

- проверку того, что процессы и процедуры действительно применяются;
- анализ соответствия между представлениями проекта ОО;
- анализ соответствия каждого представления проекта ОО требованиям;
- верификацию доказательств;
- анализ руководств;
- анализ разработанных функциональных тестов и полученных результатов;
- независимое функциональное тестирование;
- анализ уязвимостей, включающий в себя предположения о недостатках;
- тестирование проникновения.

### ***Шкала оценки доверия***

Основные принципы стандарта содержат утверждение, что большее доверие является результатом приложения больших усилий при оценке и что цель состоит в применении минимальных усилий, требуемых для обеспечения необходимого уровня доверия. Повышение уровня усилий может быть основано на:

- области охвата, т. е. увеличении рассматриваемой части продукта или системы ИТ;
- глубине, т. е. детализации рассматриваемых проектных материалов и реализации;
- строгости, т. е. применении более структурированного и формального подхода.

## **3.6. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р ИСО/МЭК 17799-2005 «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»**

Дата введения – 1 января 2007 г.

### ***Сведения о стандарте***

1. Подготовлен Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»).

2. Внесен Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии.

3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 447-ст.

4. Настоящий стандарт идентичен международному стандарту ИСО/МЭК 17799:2000 «Информационная технология. Практические правила управления информационной безопасностью» (ISO/IEC 17799:2000 «Information technology. Code of practice for security management»).

5. Введен впервые.

### ***Введение***

#### ***Что такое информационная безопасность?***

*Информация* – это актив, который, подобно другим активам организации, имеет ценность и, следовательно, должен быть защищен надлежащим образом. Информационная безопасность защищает информацию от широкого диапазона угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации ущерба, получения максимальной отдачи от инвестиций, а также реализации потенциальных возможностей бизнеса.

Информация может существовать в различных формах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных средств связи, демонстрироваться на пленке или быть выражена устно. Безотносительно формы выражения информации, средств ее распространения или хранения она должна всегда быть адекватно защищена.

*Информационная безопасность* – механизм защиты, обеспечивающий:

- конфиденциальность: доступ к информации только авторизованных пользователей;
- целостность: достоверность и полноту информации и методов ее обработки;
- доступность: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и

функциями программного обеспечения. Указанные мероприятия должны обеспечить достижение целей информационной безопасности организации.

### ***Необходимость информационной безопасности***

Информация, поддерживающие ее процессы, информационные системы и сетевая инфраструктура являются существенными активами организации. Конфиденциальность, целостность и доступность информации могут существенно способствовать обеспечению конкурентоспособности, ликвидности, доходности, соответствия законодательству и деловой репутации организации.

Организации, их информационные системы и сети все чаще сталкиваются с различными угрозами безопасности, такими как компьютерное мошенничество, шпионаж, вредительство, вандализм, пожары или наводнения. Такие источники ущерба, как компьютерные вирусы, компьютерный взлом и атаки типа отказа в обслуживании, становятся более распространенными, более агрессивными и все более изощренными.

Зависимость от информационных систем и услуг означает, что организации становятся все более уязвимыми по отношению к угрозам безопасности. Взаимодействие сетей общего пользования и частных сетей, а также совместное использование информационных ресурсов затрудняет управление доступом к информации. Тенденция к использованию распределенной обработки данных ослабляет эффективность централизованного контроля.

При проектировании многих информационных систем вопросы безопасности не учитывались. Уровень безопасности, который может быть достигнут техническими средствами, имеет ряд ограничений и, следовательно, должен сопровождаться надлежащими организационными мерами. Выбор необходимых мероприятий по управлению информационной безопасностью требует тщательного планирования и внимания к деталям.

Управление информационной безопасностью нуждается, как минимум, в участии всех сотрудников организации. Также может потребоваться участие поставщиков, клиентов или акционеров. Кроме того, могут потребоваться консультации специалистов сторонних организаций.

Мероприятия по управлению в области информационной безопасности обойдутся значительно дешевле и окажутся более эффективными, если будут включены в спецификацию требований на стадии проектирования системы.

### ***Как определить требования к информационной безопасности***

Организация должна определить свои требования к информационной безопасности с учетом следующих трех факторов.

Во-первых, оценка рисков организации. Посредством оценки рисков происходит выявление угроз активам организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий.

Во-вторых, юридические, законодательные, регулирующие и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг.

В-третьих, специфический набор принципов, целей и требований, разработанных организацией в отношении обработки информации.

### ***Оценка рисков информационной безопасности***

Требования к информационной безопасности определяются с помощью систематической оценки рисков. Решения о расходах на мероприятия по управлению информационной безопасностью должны приниматься, исходя из возможного ущерба, нанесенного бизнесу в результате нарушений информационной безопасности. Методы оценки риска могут применяться как для всей организации, так и для какой-либо ее части, отдельных информационных систем, определенных компонентов систем или услуг, а именно там, где это практически выполнимо и целесообразно.

Оценка риска – это систематический анализ:

- вероятного ущерба, наносимого бизнесу в результате нарушений информационной безопасности с учетом возможных последствий от потери конфиденциальности, целостности или доступности информации и других активов;

- вероятности наступления такого нарушения с учетом существующих угроз и уязвимостей, а также внедренных мероприятий по управлению информационной безопасностью.

Результаты этой оценки помогут в определении конкретных мер и приоритетов в области управления рисками, связанными с информационной безопасностью, а также внедрению мероприятий по управлению информационной безопасностью с целью минимизации этих рисков.

Может потребоваться неоднократное проведение оценки рисков и выбора мероприятий по управлению информационной без-

опасностью для того, чтобы охватить различные подразделения организации или отдельные информационные системы.

Важно периодически проводить анализ рисков в области информационной безопасности и внедренных мероприятий по управлению информационной безопасностью для того, чтобы учесть:

- изменения требований и приоритетов бизнеса;
- появление новых угроз и уязвимостей;
- снижение эффективности существующих мероприятий по управлению информационной безопасностью.

Уровень детализации такого анализа следует определять в зависимости от результатов предыдущих проверок и изменяющегося уровня приемлемого риска. Оценка рисков обычно проводится сначала на верхнем уровне, при этом ресурсы направляются в области наибольшего риска, а затем на более детальном уровне, что позволяет рассмотреть специфические риски.

#### ***Выбор мероприятий по управлению информационной безопасностью***

После того, как определены требования к информационной безопасности, следует выбрать и внедрить такие мероприятия по управлению информационной безопасностью, которые обеспечат снижение рисков до приемлемого уровня. Эти мероприятия могут быть выбраны из настоящего стандарта, других источников, а также могут быть разработаны собственные мероприятия по управлению информационной безопасностью, удовлетворяющие специфическим потребностям организации. Имеется множество различных подходов к управлению рисками; в настоящем стандарте приводятся примеры наиболее распространенных методов. Однако следует отметить, что некоторые из мероприятий по управлению информационной безопасностью неприменимы к отдельным информационным системам и средам и могут оказаться неприемлемыми для конкретных организаций. Например, в 8.1.4 приводится описание того, как могут быть распределены должностные обязанности, чтобы предотвратить ошибки и мошенничество. В небольших организациях может оказаться невозможным разделение всех должностных обязанностей; тогда для достижения той же цели может быть необходимо принятие альтернативных мероприятий по управлению информационной безопасностью. В качестве другого примера можно привести 9.7 и 12.1 – осуществление мониторинга использования системы и сбора доказательств. Указанные мероприятия по управлению информационной безопасностью, такие, как регистрация событий в

системе, могут вступать в конфликт с законодательством, действующим, например, в отношении защиты от вторжения в личную жизнь клиентов или сотрудников.

Выбор мероприятий по управлению информационной безопасностью должен основываться на соотношении стоимости их реализации к эффекту от снижения рисков и возможным убыткам в случае нарушения безопасности. Также следует принимать во внимание факторы, которые не могут быть представлены в денежном выражении, например, потерю репутации.

Некоторые мероприятия по управлению информационной безопасностью, приведенные в настоящем стандарте, могут рассматриваться как руководящие принципы для управления информационной безопасностью и применяться для большинства организаций. Более подробно такие мероприятия рассматриваются в стандарте.

#### ***Отправная точка для внедрения информационной безопасности***

Отдельные мероприятия по управлению информационной безопасностью могут рассматриваться как руководящие принципы для управления информационной безопасностью и служить отправной точкой для ее внедрения. Такие мероприятия либо основываются на ключевых требованиях законодательства, либо рассматриваются как общепринятая практика в области информационной безопасности.

Ключевыми мерами контроля с точки зрения законодательства являются:

- обеспечение конфиденциальности персональных данных (12.1.4);
- защита учетных данных организации (12.1.3);
- права на интеллектуальную собственность (12.1.2).

Мероприятия по управлению информационной безопасностью, рассматриваемые как общепринятая практика в области информационной безопасности, включают:

- наличие документа, описывающего политику информационной безопасности (3.1);
- распределение обязанностей по обеспечению информационной безопасности (4.1.3);
- обучение вопросам информационной безопасности (6.2.1);
- информирование об инцидентах, связанных с информационной безопасностью (6.3.1);
- управление непрерывностью бизнеса (11.1).

Перечисленные мероприятия применимы для большинства организаций и информационных сред. Следует отметить, что, хотя все приведенные в настоящем стандарте мероприятия являются важными, уместность какой-либо меры должна определяться в свете конкретных рисков, с которыми сталкивается организация. Следовательно, несмотря на то, что вышеописанный подход рассматривается как отправная точка для внедрения мероприятий по обеспечению информационной безопасности, он не заменяет выбор мероприятий по управлению информационной безопасностью, основанный на оценке рисков.

### ***Важнейшие факторы успеха***

Практика показывает, что для успешного внедрения информационной безопасности в организации решающими являются следующие факторы:

- соответствие целей, политик и процедур информационной безопасности целям бизнеса;
- согласованность подхода к внедрению системы безопасности с корпоративной культурой;
- видимая поддержка и заинтересованность со стороны руководства;
- четкое понимание требований безопасности, оценка рисков и управление рисками;
- обеспечение понимания необходимости применения мер информационной безопасности руководством и сотрудниками организации;
- передача инструкций в отношении политики информационной безопасности и соответствующих стандартов всем сотрудникам и контрагентам;
- обеспечение необходимого обучения и подготовки;
- всесторонняя и сбалансированная система измеряемых показателей, используемых для оценки эффективности управления информационной безопасностью и предложений по ее улучшению, поступивших от исполнителей.

### ***Разработка собственных руководств организации***

Настоящий стандарт должен расцениваться как отправная точка для разработки руководства под конкретные нужды организации. Не все инструкции и мероприятия, приведенные в настоящем стандарте, могут быть применимыми.

Более того, могут потребоваться дополнительные меры, не включенные в настоящий стандарт. В этом случае может быть по-

лезным сохранение перекрестных ссылок, которые облегчат проверку соответствия, проводимую аудиторами и партнерами по бизнесу.

### ***Область применения***

Настоящий стандарт устанавливает рекомендации по управлению информационной безопасностью лицам, ответственным за планирование, реализацию или поддержку решений безопасности в организации. Он предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями. Рекомендации настоящего стандарта следует выбирать и использовать в соответствии с действующим законодательством.

### ***Термины и определения***

В стандарте применены следующие термины с соответствующими определениями:

*Информационная безопасность* – защита конфиденциальности, целостности и доступности информации.

Примечания:

*Конфиденциальность* – обеспечение доступа к информации только авторизованным пользователям.

*Целостность* – обеспечение достоверности и полноты информации и методов ее обработки.

*Доступность* – обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

*Оценка рисков* – оценка угроз, их последствий, уязвимости информации и средств ее обработки, а также вероятности их возникновения.

*Управление рисками* – процесс выявления, контроля и минимизации или устранения рисков безопасности, оказывающих влияние на информационные системы, в рамках допустимых затрат.

### ***Политика безопасности***

Цель: обеспечение решения вопросов информационной безопасности и вовлечение высшего руководства организации в данный процесс.

Разработка и реализация политики информационной безопасности организации осуществляется высшим руководством путем выработки четкой позиции в решении вопросов информационной безопасности.

Политика информационной безопасности должна быть утверждена, издана и надлежащим образом доведена до сведения всех сотрудников организации. Она должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью.

### **3.7. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ГОСТ Р ИСО/МЭК 27001-2006 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Дата введения – 1 февраля 2008.

#### ***Сведения о стандарте***

1. ПОДГОТОВЛЕН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России») и Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») на основе собственного аутентичного перевода стандарта, указанного в пункте 4.

2. Внесен Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии.

3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст.

4. Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements»).

5. При применении настоящего стандарта рекомендуется использовать вместо ссылочного международного стандарта соответствующий ему национальный стандарт Российской Федерации, сведения о котором приведены в дополнительном приложении D.

6. Введен впервые.

### ***Общие положения***

Стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ). Внедрение СМИБ является стратегическим решением организации. На проектирование и внедрение СМИБ организации влияют потребности и цели организации, требования безопасности, используемые процессы, а также масштабы деятельности и структура организации. Предполагается, что вышеуказанные факторы и поддерживающие их системы будут изменяться во времени. Предполагается также, что СМИБ будет изменяться пропорционально потребностям организации, т. е. для простой ситуации потребуется простое решение по реализации СМИБ.

Положения настоящего стандарта могут быть использованы как внутри организации, так и внешними организациями для оценки соответствия.

### ***Процессный подход***

Стандарт предполагает использовать процессный подход для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ организации.

Для успешного функционирования организация должна определить и осуществить менеджмент многочисленных видов деятельности. Деятельность, использующая ресурсы и управляемая в целях преобразования входов в выходы, может быть рассмотрена как процесс. Часто выход одного процесса непосредственно формирует вход для следующего процесса.

Использование внутри организации системы процессов наряду с идентификацией и взаимодействием этих процессов, а также менеджмент процессов могут быть определены как «процессный подход».

Согласно предлагаемому стандартом процессному подходу применительно к менеджменту информационной безопасности (ИБ) особую значимость для пользователей имеют следующие факторы:

- понимание требований информационной безопасности организации и необходимости установления политики и целей информационной безопасности;
- внедрение и использование мер управления для менеджмента рисков ИБ среди общих бизнес-рисков организации;
- мониторинг и проверка производительности и эффективности СМИБ;

– непрерывное улучшение СМИБ, основанное на результатах объективных измерений.

В стандарте представлена модель «Планирование (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (PDCA), которая может быть применена при структурировании всех процессов СМИБ. На рисунке показано, как СМИБ, используя в качестве входных данных требования ИБ и ожидаемые результаты заинтересованных сторон, с помощью необходимых действий и процессов выдает выходные данные по результатам обеспечения информационной безопасности, которые соответствуют этим требованиям и ожидаемым результатам. Рисунок иллюстрирует также связи между процессами, описанными в разделах 4, 5, 6, 7 и 8.

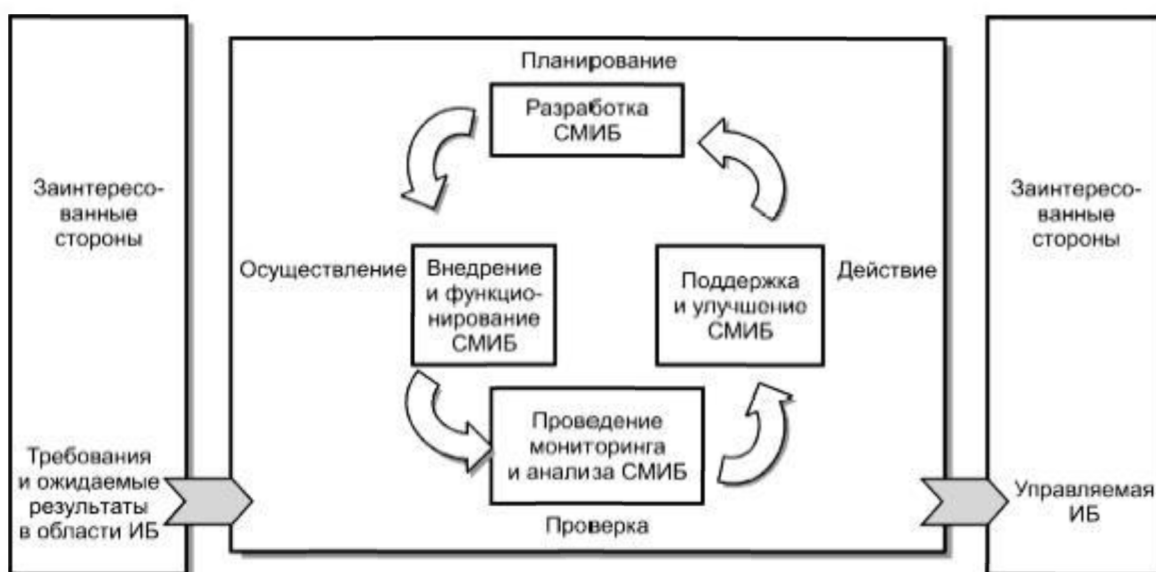


Рис. Модель PDCA

Принятие модели PDCA также отражает принципы, установленные в Директивах Организации экономического сотрудничества и развития (ОЭСР) и определяющие безопасность информационных систем и сетей. Стандарт представляет наглядную модель для реализации на практике указанных принципов, которые позволяют осуществить оценку рисков, проектирование и реализацию системы информационной безопасности, ее менеджмент и переоценку.

### **Примеры**

1. Требование может заключаться в том, чтобы нарушения информационной безопасности не приводили к значительному финансовому ущербу для организации и/или к существенным затруднениям в ее деятельности.

2. Ожидаемым результатом может быть наличие в организации достаточно хорошо обученных сотрудников для проведения процедур, позволяющих минимизировать возможные неблагоприятные последствия в случае серьезного инцидента, например, несанкционированного проникновения (атаки хакеров) на веб-сайт организации, через который она осуществляет электронную торговлю.

Связи между процессами, описанными в разделах 4, 5, 6, 7 и 8, представлены также в таблице.

Планирование (разработка СМИБ)	Разработка политики, установление целей, процессов и процедур СМИБ, относящихся к менеджменту риска и улучшению информационной безопасности, для достижения результатов, соответствующих общей политике и целям организации
Осуществление (внедрение и обеспечение функционирования СМИБ)	Внедрение и применение политики информационной безопасности, мер управления, процессов и процедур СМИБ
Проверка (проведение мониторинга и анализа СМИБ)	Оценка, в том числе, по возможности, количественная, результативности процессов относительно требований политики, целей безопасности и практического опыта функционирования СМИБ и информирование высшего руководства о результатах для последующего анализа
Действие (поддержка и улучшение СМИБ)	Проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения СМИБ

#### ***Совместимость с другими системами менеджмента***

Настоящий стандарт согласован со стандартами ИСО 9001:2000 «Системы менеджмента качества. Требования» и ИСО 14001:2004

«Системы управления окружающей средой. Требования и руководство по применению» в целях поддержки последовательного и интегрированного внедрения и взаимодействия с другими подобными взаимосвязанными стандартами в области менеджмента. Таким образом, одна правильно построенная система менеджмента в организации может удовлетворять требованиям всех этих стандартов.

### ***Область применения***

Стандарт предназначен для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими организациями). Стандарт устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности (СМИБ) среди общих бизнес-рисков организации. Кроме этого, стандарт устанавливает требования по внедрению мер управления информационной безопасностью и ее контроля, которые могут быть использованы организациями или их подразделениями в соответствии с установленными целями и задачами обеспечения информационной безопасности (ИБ).

Целью построения СМИБ является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

### ***Применение***

Требования, устанавливаемые стандартом, предназначены для применения во всех организациях независимо от типа, масштабов и сферы их деятельности. Исключение любого из требований, указанных в разделах 4, 5, 6, 7 и 8, не допускается, если организация заявляет о соответствии ее СМИБ стандарту.

Любой отказ от применения той или иной меры управления, обусловленный необходимостью удовлетворения критериев принятия рисков, должен быть обоснован. Необходимо также наличие адекватных доказательств того, что подобные риски были уже приняты ответственными лицами. При исключении каких-либо мер управления заявления о соответствии организации настоящему стандарту неправомерны, кроме случаев, когда эти исключения не влияют на способность и/или обязанность организации обеспечивать информационную безопасность, которая соответствует требованиям безопасности, установленным соответствующими законодательными актами или определенными на основе оценок рисков.

### ***Нормативные ссылки***

В настоящем стандарте использованы нормативные ссылки на следующий стандарт:

ИСО/МЭК 17799:2005 Информационная технология. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности.

### ***Термины и определения***

В настоящем стандарте применены следующие термины с соответствующими определениями:

*Активы (asset)* – все, что имеет ценность для организации.

*Доступность (availability)* – свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

*Конфиденциальность (confidentiality)* – свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

*Информационная безопасность; ИБ (information security)* – свойство информации сохранять конфиденциальность, целостность и доступность.

*Событие информационной безопасности (information security event)* – идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

*Инцидент информационной безопасности (information security incident)* – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

*Система менеджмента информационной безопасности; СМИБ (information security management system; ISMS)* – часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

*Целостность (integrity)* – свойство сохранять правильность и полноту активов.

*Остаточный риск (residual risk)* – риск, остающийся после его обработки.

*Принятие риска (risk acceptance)* – решение по принятию риска.

*Анализ риска (risk analysis)* – систематическое использование информации для определения источников риска и количественной оценки риска.

*Оценка риска (risk assessment)* – общий процесс анализа риска и его оценивания.

*Оценивание риска (risk evaluation)* – процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости.

*Менеджмент риска (risk management)* – скоординированные действия по руководству и управлению организацией в отношении риска.

*Обработка риска (risk treatment)* – процесс выбора и осуществления мер по модификации риска.

*Положение о применимости (statement of applicability)* – документированное предписание, определяющее цели и меры управления, соответствующие и применимые к системе менеджмента информационной безопасности организации.

### ***Система менеджмента информационной безопасности***

Организация должна разработать, внедрить, обеспечить функционирование, вести мониторинг, анализировать, поддерживать и непрерывно улучшать документированную СМИБ применительно ко всей деловой деятельности организации и рискам, с которыми она сталкивается. С учетом целей стандарта используемый процесс основан на применении модели PDCA (Планирование (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)), приведенной на рисунке.

### ***Ответственность руководства***

Руководство организации должно предоставлять доказательства выполнения своих обязательств в отношении разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ.

### ***Внутренние аудиты системы менеджмента информационной безопасности***

Организация должна в соответствии с утвержденным графиком проводить внутренние аудиты СМИБ, позволяющие установить, что цели управления, меры управления, процессы и процедуры СМИБ:

- соответствуют требованиям стандарта и соответствующим законам или нормативным документам;
- соответствуют установленным требованиям ИБ;
- результативно внедряются и поддерживаются;

– функционируют должным образом.

***Анализ системы менеджмента информационной безопасности со стороны руководства***

Руководство должно в соответствии с утвержденным графиком периодически (не менее одного раза в год) проводить анализ СМИБ организации в целях обеспечения ее постоянной пригодности, адекватности и результативности. Результаты анализа должны содержать предложения по изменению СМИБ и оценку их реализации в интересах обеспечения выполнения требований политики и целей информационной безопасности. Результаты таких проверок должны быть зафиксированы документально, а учетные записи должны быть сохранены.

***Улучшение системы менеджмента информационной безопасности***

Организация должна постоянно повышать результативность СМИБ посредством уточнения политики ИБ, целей ИБ, использования результатов аудитов, анализа контролируемых событий, корректирующих и предупреждающих действий, а также использования руководством результатов анализа СМИБ.

## Глава 4. РУКОВОДЯЩИЕ ДОКУМЕНТЫ ГОСТЕХКОМИССИИ РОССИИ

Гостехкомиссия России при Президенте Российской Федерации разработала ряд документов в области защиты информации, которые обязательны для исполнения в государственном секторе, а для коммерческих структур они носят рекомендательно-консультативный характер.

### 4.1. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Документ устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Установленные термины обязательны для применения во всех видах документации. Для каждого понятия установлен один термин. Применение терминов-синонимов не допускается. В качестве справочных приведены иностранные эквиваленты русских терминов на английском языке.

#### Термины и определения

Термин	Определение
Доступ к информации (Доступ) Access to information	Ознакомление с информацией, ее обработка, в частности, копирование модификация или уничтожение информации
Правила разграничения доступа (ПРД) Security policy	Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
Санкционированный доступ к информации Authorized access to information	Доступ к информации, не нарушающий правила разграничения доступа
Несанкционированный доступ к информации (НСД) Unauthorized access to information	Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем

Термин	Определение
Защита от несанкционированного доступа (Защита от НСД) Protection from unauthorized access	Предотвращение или существенное затруднение несанкционированного доступа
Субъект доступа (Субъект) Access subject	Лицо или процесс, действия которого регламентируются правилами разграничения доступа
Объект доступа (Объект) Access object	Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа
Матрица доступа Access matrix	Таблица, отображающая правила разграничения доступа
Уровень полномочий субъекта доступа Subject privilege	Совокупность прав доступа субъекта доступа
Нарушитель правил разграничения доступа (Нарушитель ПРД) Security policy violator	Субъект доступа; осуществляет несанкционированный доступ к информации
Модель нарушителя правил разграничения доступа (Модель нарушителя ПРД) Security policy violator's model	Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа
Комплекс средств защиты (КСЗ) Trusted computing base	Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации
Система разграничения доступа (СРД) Security policy realization	Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах
Идентификатор доступа Access identifier	Уникальный признак субъекта или объекта доступа
Идентификация Identification	Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
Пароль Password	Идентификатор субъекта доступа, который является его (субъекта) секретом
Аутентификация Authentication	Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности
Защищенное средство вычислительной техники (Защищенная автоматизированная система) Trusted computer system	Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты
Средство защиты от несанкционированного доступа (Средство защиты от НСД) Protection facility	Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа

Термин	Определение
Модель защиты Protection model	Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа
Безопасность информации Information security	Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз
Целостность информации Information integrity	Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения)
Конфиденциальная информация Sensitive information	Информация, требующая защиты
Дискреционное управление доступом Discretionary access control	Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту
Мандатное управление Mandatory access control	Разграничение доступа субъектов к объектам, основанное на характеризующей метке конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности
Многоуровневая защита Multi-level secure	Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности
Концепция диспетчера доступа Reference monitor concept	Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам
Диспетчер доступа Security kernel	Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа; ядро защиты
Администратор защиты Security administrator	Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации
Метка конфиденциальности (Метка) Sensitivity label	Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте

Термин	Определение
Верификация Verification	Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие
Класс защищенности средств вычислительной техники (автоматизированной системы) Protection class of computer systems	Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации
Показатель защищенности средств вычислительной техники (Показатель защищенности) Protection criterion of computer systems	Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники
Система защиты секретной информации (СЗСИ) Secret information security system	Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах
Система защиты информации от несанкционированного доступа (СЗИ НСД) System of protection from unauthorized access to information	Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах
Средство криптографической защиты информации (СКЗИ) Cryptographic information protection facility	Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности
Сертификат защиты (Сертификат) Protection certificate	Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных
Сертификация уровня защиты (Сертификация) Protection level certification	Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите

## **4.2. КОНЦЕПЦИЯ ЗАЩИТЫ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (НСД) К ИНФОРМАЦИИ**

Документ излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа (НСД), являющейся частью общей проблемы безопасности информации.

Концепция предназначена для заказчиков, разработчиков и пользователей СВТ и АС, которые используются для обработки, хранения и передачи требующей защиты информации.

Концепция является методологической базой нормативно-технических и методических документов, направленных на решение следующих задач:

- выработка требований по защите СВТ и АС от НСД к информации;
- создание защищенных от НСД к информации СВТ и АС;
- сертификация защищенных СВТ и АС.

Концепция предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от НСД: направление, связанное с СВТ, и направление, связанное с АС.

Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

В связи с этим, если понятия защищенность (защита) информации от НСД в АС и защищенность (защита) АС от НСД к информации эквивалентны, то в случае СВТ можно говорить лишь о защищенности (защите) СВТ от НСД к информации, для обработки, хранения и передачи которой оно предназначено.

При этом, защищенность СВТ есть потенциальная защищенность, т. е. свойство предотвращать или существенно затруднять НСД к информации в дальнейшем при использовании СВТ в АС.

Документ имеет следующие главы:

- определение НСД;
- основные принципы защиты от НСД;
- модель нарушителя в АС;
- основные способы НСД;
- основные направления обеспечения защиты от НСД;
- основные характеристики технических средств защиты от НСД;
- классификация АС;
- организация работ по защите от НСД;

#### **4.3. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ**

Документ устанавливает классификацию автоматизированных систем (АС), подлежащих защите от НСД к информации, и требования по защите информации в АС различных классов. Руководящий документ разработан в дополнение ГОСТ 34.003-90, ГОСТ 34.601-90, РД 50-680-88, РД 50-34 680-90 и других документов. Документ может использоваться как нормативно-методический материал для заказчиков и разработчиков АС при формулировании и реализации требований по защите.

##### ***Классификация АС***

Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

Основными этапами классификации АС являются –

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД.

Необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;

- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС – коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

### ***Требования по защите информации от НСД для АС***

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогатель-

ных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем: управления доступом; регистрации и учета; криптографической; обеспечения целостности (табл. 1).

Т а б л и ц а 1

Требования к АС третьей группы		Классы	
Подсистемы и требования		ЗБ	ЗА
<b>1. Подсистема управления доступом</b>			
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:			
– в систему;		+	+
– к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;		–	–
– к программам;		–	–
– к томам, каталогам, файлам, записям, полям записей.		–	–
1.2. Управление потоками информации.		–	–
<b>2. Подсистема регистрации и учета</b>			
2.1. Регистрация и учет:			
– входа (выхода) субъектов доступа в (из) системы (узел сети);		+	+
– выдачи печатных (графических) выходных документов;		–	+
– запуска (завершения) программ и процессов (заданий, задач);		–	–
– доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;		–	–
– доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;		–	–
– изменения полномочий субъектов доступа;		–	–
– создаваемых защищаемых объектов доступа.		+	+
2.2. Учет носителей информации		–	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей		–	–
2.4. Сигнализация попыток нарушения защиты		–	–
<b>3. Криптографическая подсистема</b>			
3.1. Шифрование конфиденциальной информации		–	–
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах		–	–
3.3. Использование аттестованных (сертифицированных) криптографических средств		–	–
<b>4. Подсистема обеспечения целостности</b>			
4.1. Обеспечение целостности программных средств и обрабатываемой информации		+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации		+	+
4.3. Наличие администратора (службы) защиты информации в АС		–	–
4.4. Периодическое тестирование СЗИ НСД		+	+
4.5. Наличие средств восстановления СЗИ НСД		+	+
4.6. Использование сертифицированных средств защиты		–	+

Обозначения:

«–» – нет требований к данному классу;

«+» – есть требования к данному классу.

### ***Требования к классу защищенности 3Б***

*Подсистема управления доступом* – должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.

*Подсистема регистрации и учета* – должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы. Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

*Подсистема обеспечения целостности* – должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ; целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ. Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время. Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД. Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

### ***Требования к классу защищенности 3А***

*Подсистема управления доступом* – должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

*Подсистема регистрации и учета* – должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной си-

системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы; результат попытки входа: успешная или неуспешная (при НСД). Должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;
- спецификация устройства выдачи (логическое имя (номер) внешнего устройства).

Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку). Должно проводиться несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации. Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

*Подсистема обеспечения целостности* – должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ; целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ. Должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС. Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД. Должны быть в наличии средства восстановления СЗИ НСД, преду-

смагивающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности. Должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД (табл. 2).

Т а б л и ц а 2

**Требования к АС второй группы**

Подсистемы и требования	Классы	
	2Б	2А
<b>1. Подсистема управления доступом</b>		
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:		
– в систему;	+	+
– к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	–	+
– к программам;	–	+
– к томам, каталогам, файлам, записям, полям записей;	–	+
1.2. Управление потоками информации	–	+
<b>2. Подсистема регистрации и учета</b>		
2.1. Регистрация и учет:		
– входа (выхода) субъектов доступа в (из) систему (узел сети);	+	+
– выдачи печатных (графических) выходных документов;	–	+
– запуска (завершения) программ и процессов (заданий, задач);	–	+
– доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;	–	+
– доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	–	+
– изменения полномочий субъектов доступа;	–	–
– создаваемых защищаемых объектов доступа.	–	+
2.2. Учет носителей информации	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	–	+
2.4. Сигнализация попыток нарушения защиты	–	–
<b>3. Криптографическая подсистема</b>		
3.1. Шифрование конфиденциальной информации	–	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	–	–
3.3. Использование аттестованных (сертифицированных) криптографических средств	+	+
<b>4. Подсистема обеспечения целостности</b>		
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+
4.3. Наличие администратора (службы) защиты информации в АС	–	+
4.4. Периодическое тестирование СЗИ НСД	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+
4.6. Использование сертифицированных средств защиты	–	+

Обозначения:

«–» – нет требований к данному классу;

«+» – есть требования к данному классу.

### ***Требования к классу защищенности 2Б***

*Подсистема управления доступом* – должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

*Подсистема регистрации и учета* – должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная (при НСД).

Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (карточку).

*Подсистема обеспечения целостности* – должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации.

Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД.

Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

### ***Требования к классу защищенности 2А***

*Подсистема управления доступом* – должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов. Должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по их логическим адресам (номерам).

Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности, записываемой на них информации.

*Подсистема регистрации и учета* – должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная (при НСД);
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа.

Должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ.

Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный – несанкционированный).

Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная,
- идентификатор субъекта доступа;
- спецификация защищаемого файла.

Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта (логическое имя (номер)).

Должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта. Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку); учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации.

Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

*Криптографическая подсистема* – должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные носители данных (дискеты, микрокассеты и т. п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию.

Доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом.

Должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

*Подсистема обеспечения целостности* – должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

Должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС.

Должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД.

Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД.

Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД (табл. 3).

Т а б л и ц а 3

**Требования к АС первой группы**

Подсистемы и требования	Классы				
	1Д	1Г	1В	1Б	1А
<b>1. Подсистема управления доступом</b>					
1.1 Идентификация, проверка подлинности и контроль доступа субъектов:					
– в систему;	+	+	+	+	+
– к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	–	+	+	+	+
– к программам;	–	+	+	+	+
– к томам, каталогам, файлам, записям, полям записей.	–	+	+	+	+
1.2. Управление потоками информации	–	–	+	+	+
<b>2. Подсистема регистрации и учета</b>					
2.1. Регистрация и учет:					
– входа (выхода) субъектов доступа в (из) систему (узел сети);	+	+	+	+	+
– выдачи печатных (графических) выходных документов;	–	+	+	+	+
– запуска (завершения) программ и процессов (заданий, задач);	–	+	+	+	+
– доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;	–	+	+	+	+
– доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	–	+	+	+	+
– изменения полномочий субъектов доступа;	–	–	+	+	+
– создаваемых защищаемых объектов доступа.	–	–	+	+	+
2.2. Учет носителей информации	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	–	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	–	–	+	+	+
<b>3. Криптографическая подсистема</b>					
3.1. Шифрование конфиденциальной информации	–	–	–	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	–	–	–	–	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	–	–	–	+	+
<b>4. Подсистема обеспечения целостности</b>					
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
4.3. Наличие администратора (службы защиты информации в АС	–	–	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	–	–	+	+	+

Обозначения:

«–» – нет требований к данному классу;

«+» – есть требования к данному классу.

### ***Требования к классу защищенности 1Д***

*Подсистема управления доступом* – должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

*Подсистема регистрации и учета* – должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная – не-санкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа.

Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнал (учетную карточку); учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

*Подсистема обеспечения целостности* – должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время.

Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД.

Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

### ***Требования к классу защищенности 1Г***

*Подсистема управления доступом* – должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам.

Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

*Подсистема регистрации и учета* – должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная – не-санкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке.

Должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи (логическое имя (номер) внешнего устройства);
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ.

Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный – несанкционированный).

Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла.

Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта (логическое имя (номер)).

Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку); учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

*Подсистема обеспечения целостности* – должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

Должна осуществляться физическая охрана СБТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время.

Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД.

Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

#### ***Требования к классу защищенности 1В***

*Подсистема управления доступом* – должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и (или) адресам.

Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности, записываемой на него информации.

*Подсистема регистрации и учета* – должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из систе-

мы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная – не-санкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке.

Должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

- дата и время выдачи (обращение к подсистеме вывода);
- спецификация устройства выдачи (логическое имя (номер) внешнего устройства);
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;
- объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный.

Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный – не-санкционированный).

Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
- вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т. п.).

Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта (логическое имя (номер));
- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т. п.).

Должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

- дата и время изменения полномочий;
- идентификатор субъекта доступа (администратора), осуществившего изменения.

Должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта.

Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал (учетную карточку); учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации.

Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации.

Должна осуществляться сигнализация попыток нарушения защиты.

*Подсистема обеспечения целостности* – должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации.

Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС.

Должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС.

Должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год.

Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

### ***Требования к классу защищенности 1Б***

*Подсистема управления доступом* – должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов.

Должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам).

Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности, записываемой на него информации.

*Подсистема регистрации и учета* – должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешный или неуспешный – не-санкционированный;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке.

Должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества

страниц и копий документа (при неполной выдаче документа – фактически выданного количества листов в графе «Брак»). В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи (логическое имя (номер) внешнего устройства);
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;
- объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи успешный (весь объем), неуспешный.

Должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный – несанкционированный).

Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
- вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т. п.).

Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта (логическое имя (номер));
- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т. п.).

Должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

- дата и время изменения полномочий;
- идентификатор субъекта доступа (администратора), осуществившего изменения;
- идентификатор субъекта, у которого проведено изменение полномочий и вид изменения (пароль, код, профиль и т. п.);
- спецификация объекта, у которого проведено изменение статуса защиты и вид изменения (код защиты, уровень конфиденциальности).

Должен осуществляться автоматический учет создаваемых защищаемых файлов, иницируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта.

Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки; учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации.

Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной за-

писью в любую освобождаемую область памяти, использованную для хранения защищаемой информации.

Должна осуществляться сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

*Криптографическая подсистема* – должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные портативные носители данных (дискеты, микрокассеты и т. п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию.

Доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом.

Должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

*Подсистема обеспечения целостности* – должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется по контрольным суммам всех компонент СЗИ как в процессе загрузки, так и динамически в процессе работы АС;

- целостность программной среды обеспечивается качеством приемки программных средств в АС, предназначенных для обработки защищенных файлов.

Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС.

Должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь

свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС.

Должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал.

Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также оперативное восстановление функций СЗИ НСД при сбоях.

Должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

#### ***Требования к классу защищенности 1А***

*Подсистема управления доступом* — должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия длиной не менее восьми буквенно-цифровых символов.

Должна осуществляться аппаратурная идентификация и проверка подлинности терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по уникальным встроенным устройствам.

Должна осуществляться идентификация и проверка подлинности программ, томов, каталогов, файлов, записей, полей записей по именам и контрольным суммам (паролям, ключам).

Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности, записываемой на него информации.

*Подсистема регистрации и учета* — должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы

или останов не проводится в моменты аппаратного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная – не-санкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке.

Должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа – фактически выданного количества листов в графе «Брак»). В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи (логическое имя (номер) внешнего устройства);
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;
- объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный.

Должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);

- результат запуска (успешный, неуспешный – несанкционированный);

- полная спецификация соответствующего файла «образа» программы (процесса, задания) – устройство (том, каталог), имя файла (расширение).

Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющей доступ к файлу, вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т. п.).

Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта (логическое имя (номер));

- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;

- вид запрашиваемой операции (чтение, запись, монтирование, захват и т. п.).

Должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

- дата и время изменения полномочий и статуса;
- идентификатор субъекта доступа (администратора), осуществившего изменения;

- идентификатор субъекта доступа, у которого изменены полномочия и вид изменений (пароль, код, профиль и т. п.);

– спецификация объекта, у которого изменен статус защиты, и вид изменения (код защиты, уровень конфиденциальности).

Должен осуществляться автоматический учет создаваемых защищаемых файлов, иницилируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта.

Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку); учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации.

Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, в которой содержалась защищаемая информация.

Должна осуществляться надежная сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

*Криптографическая подсистема* – должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на любые съемные носители данных (дискеты, микрокассеты и т. п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться автоматическая очистка областей внешней памяти, содержавших ранее незашифрованную информацию.

Должны использоваться разные криптографические ключи для шифрования информации, принадлежащей различным субъектам доступа (группам субъектов).

Доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;

Должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

*Подсистема обеспечения целостности* – должны быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется по имитовставкам алгоритма ГОСТ 28147-89 или по контрольным суммам другого аттестованного алгоритма всех компонент СЗИ как в процессе загрузки, так и динамически в процессе функционирования АС;

- целостность программной среды обеспечивается качеством приемки любых программных средств в АС.

Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС.

Должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС.

Должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал.

Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также автоматическое оперативное восстановление функций СЗИ НСД при сбоях.

Должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

При обработке или хранении в АС информации, не отнесенной к категории секретной, в рамках СЗИ НСД государственным, кол-

лективным, частным и совместным предприятиям, а также частным лицам рекомендуются следующие организационные мероприятия:

- выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;
- определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;
- установление и оформление правил разграничения доступа, т. е. совокупности правил, регламентирующих права доступа субъектов к объектам;
- ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;
- обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;
- выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;
- организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т. д.;
- разработка СЗИ НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;
- осуществление приемки СЗИ НСД в составе АС.

При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и от-

несенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:

- не ниже 4 класса – для класса защищенности АС 1В;
- не ниже 3 класса – для класса защищенности АС 1Б;
- не ниже 2 класса – для класса защищенности АС 1А.

#### **4.4. СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ**

Документ устанавливает классификацию средств вычислительной техники (СВТ) по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

<...>

1.5. Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

1.6. Применение в комплекте СВТ средств криптографической защиты информации по ГОСТ 28147-89 может быть использовано для повышения гарантий качества защиты.

### **Требования к показателям защищенности**

Перечень показателей по классам защищенности СВТ приведен в таблице.

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	–	–	+	=	=	=
Очистка памяти	–	+	+	+	=	=
Изоляция модулей	–	–	+	=	+	=
Маркировка документов	–	–	+	=	=	=
Защита ввода и вывода на отчуждаемый физический носитель информации	–	–	+	=	=	=
Сопоставление пользователя с устройством	–	–	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	–	+	+	+	+	+
Регистрация	–	+	+	+	=	=
Взаимодействие пользователя с КСЗ	–	–	–	+	=	=
Надежное восстановление	–	–	–	+	=	=
Целостность КСЗ	–	+	+	+	=	=
Контроль модификации	–	–	–	–	+	=
Контроль дистрибуции	–	–	–	–	+	=
Гарантии архитектуры	–	–	–	–	–	+
Тестирование	+	+	+	+	+	=
Руководство для пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения:

«–» – нет требований к данному классу;

«+» – новые или дополнительные требования,

«=» – требования совпадают с требованиями к СВТ предыдущего класса.

Приведенные в данном разделе наборы требований к показателям каждого класса являются минимально необходимыми.

<...>

Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса.

## 2.2. Требования к показателям защищенности шестого класса

### 2.2.1. Дискреционный принцип контроля доступа

КСЗ должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т. д.).

Для каждой пары (субъект – объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.), т. е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.

Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т. д.).

### 2.2.2. Идентификация и аутентификация

КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен подвергать проверке подлинность идентификации – осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации. КСЗ должен препятствовать доступу к защищаемым ресурсам не идентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

### 2.2.3. Тестирование

В СВТ шестого класса должны тестироваться:

- реализация дискреционных ПРД (перехват явных и скрытых запросов, правильное распознавание санкционированных и несанкционированных запросов на доступ, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);

- успешное осуществление идентификации и аутентификации, а также их средств защиты.

### 2.2.4. Руководство для пользователя

Документация на СВТ должна включать в себя краткое руководство для пользователя с описанием способов использования КСЗ и его интерфейса с пользователем.

#### 2.2.5. Руководство по КСЗ

Данный документ адресован администратору защиты и должен содержать:

- описание контролируемых функций;
- руководство по генерации КСЗ;
- описание старта СВТ и процедур проверки правильности старта.

#### 2.2.6. Тестовая документация

Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п. 2.2.3.) и результатов тестирования.

#### 2.2.7. Конструкторская (проектная) документация

Должна содержать общее описание принципов работы СВТ, общую схему КСЗ, описание интерфейсов КСЗ с пользователем и интерфейсов частей КСЗ между собой, описание механизмов идентификации и аутентификации.

### 2.3. Требования к показателям пятого класса защищенности

#### 2.3.1. Дискреционный принцип контроля доступа

Данные требования включают в себя аналогичные требования шестого класса (п. 2.2.1).

Дополнительно должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

#### 2.3.2. Очистка памяти

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации.

#### 2.3.3. Идентификация и аутентификация

Данные требования полностью совпадают с аналогичными требованиями шестого класса (п. 2.2.2).

#### 2.3.4. Гарантии проектирования

На начальном этапе проектирования СВТ должна быть построена модель защиты. Модель должна включать в себя ПРД к объектам и непротиворечивые правила изменения ПРД.

#### 2.3.5. Регистрация

КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т. д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для каждого из этих событий должна регистрироваться следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией.

#### 2.3.6. Целостность КСЗ

В СВТ пятого класса защищенности должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части КСЗ.

#### 2.3.7. Тестирование

В СВТ пятого класса защищенности должны тестироваться:

- реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);
- успешное осуществление идентификации и аутентификации, а также их средства защиты;
- очистка памяти в соответствии с п. 2.3.2;
- регистрация событий в соответствии с п. 2.3.5, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;
- работа механизма, осуществляющего контроль за целостностью КСЗ.

#### 2.3.8. Руководство пользователя

Данное требование совпадает с аналогичным требованием шестого класса (п. 2.2.4).

#### 2.3.9. Руководство по КСЗ

Данный документ адресован администратору защиты и должен содержать:

- описание контролируемых функций;
- руководство по генерации КСЗ;
- описания старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации.

#### 2.3.10. Тестовая документация

Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с требованиями п. 2.3.7), и результатов тестирования.

#### 2.3.11. Конструкторская и проектная документация.

Должна содержать:

- описание принципов работы СВТ;
- общую схему КСЗ;
- описание интерфейсов КСЗ с пользователем и интерфейсов модулей КСЗ;
- модель защиты;
- описание механизмов контроля целостности КСЗ, очистки памяти, идентификации и аутентификации.

### 2.4. Требования к показателям четвертого класса защищенности

#### 2.4.1. Дискреционный принцип контроля доступа

Данные требования включают аналогичные требования пятого класса (п. 2.3.1).

Дополнительно КСЗ должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т. е. от доступа, не допустимого с точки зрения заданного ПРД). Под «явными» здесь подразумеваются действия, осуществляемые с использованием системных средств – системных макрокоманд, инструкций языков высокого уровня и т. д., а под «скрытыми» – иные действия, в том числе с использованием собственных программ работы с устройствами.

Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.

#### 2.4.2. Мандатный принцип контроля доступа

Для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих

меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т. п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

- субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;

- субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

Реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

В СВТ должен быть реализован диспетчер доступа, т. е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

#### 2.4.3. Очистка памяти

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен затруднять субъекту доступ к остаточной информации. При перераспределении оперативной памяти КСЗ должен осуществлять ее очистку.

#### 2.4.4. Изоляция модулей

При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) – т. е. в оперативной памяти ЭВМ программы разных пользователей должны быть защищены друг от друга.

#### 2.4.5. Маркировка документов

При выводе защищаемой информации на документ в начале и конце проставляют штамп № 1 и заполняют его реквизиты в соответствии с Инструкцией № 0126-87 (п. 577).

#### 2.4.6. Защита ввода и вывода на отчуждаемый физический носитель информации

КСЗ должен различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»). При вводе с «помеченного» устройства (вывода на «помеченное» устройство) КСЗ должен обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с «помеченным» каналом связи.

Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем КСЗ.

#### 2.4.7. Сопоставление пользователя с устройством

КСЗ должен обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки).

Идентифицированный КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству.

#### 2.4.8. Идентификация и аутентификация

КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ, должен проверять подлинность идентификатора субъекта – осуществлять аутентификацию. КСЗ должен

располагать необходимыми данными для идентификации и аутентификации и препятствовать входу в СВТ не идентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.

КСЗ должен обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

#### 2.4.9. Гарантии проектирования

Проектирование КСЗ должно начинаться с построения модели защиты, содержащей:

- непротиворечивые ПРД;
- непротиворечивые правила изменения ПРД;
- правила работы с устройствами ввода и вывода информации и каналами связи.

#### 2.4.10. Регистрация

Данные требования включают аналогичные требования пятого класса защищенности (п. 2.3.5). Дополнительно должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т. п.).

#### 2.4.11. Целостность КСЗ

В СВТ четвертого класса защищенности должен осуществляться периодический контроль за целостностью КСЗ.

Программы КСЗ должны выполняться в отдельной части оперативной памяти.

#### 2.4.12. Тестирование

В четвертом классе защищенности должны тестироваться:

- реализация ПРД (перехват запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискреционными и мандатными правилами, верное сопоставление меток субъектов и объектов, запрос меток вновь вводимой информации, средства защиты механизма разграничения доступа, санкционированное изменение ПРД);
- невозможность присвоения субъектом себе новых прав;
- очистка оперативной и внешней памяти;
- работа механизма изоляции процессов в оперативной памяти;
- маркировка документов;
- защита ввода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;
- идентификация и аутентификация, а также их средства защиты;

- запрет на доступ несанкционированного пользователя;
- работа механизма, осуществляющего контроль за целостностью СВТ;
- регистрация событий, описанных в п. 2.4.10, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.

#### 2.4.13. Руководство для пользователя

Данное требование совпадает с аналогичным требованием шестого (п. 2.2.4) и пятого (п. 2.3.8) классов.

#### 2.4.14. Руководство по КСЗ

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.3.9).

#### 2.4.15. Тестовая документация

Должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п. 2.4.12) и результатов тестирования.

#### 2.4.16. Конструкторская (проектная) документация

Должна содержать:

- общее описание принципов работы СВТ;
- общую схему КСЗ;
- описание внешних интерфейсов КСЗ и интерфейсов модулей КСЗ;
- описание модели защиты;
- описание диспетчера доступа;
- описание механизма контроля целостности КСЗ;
- описание механизма очистки памяти;
- описание механизма изоляции программ в оперативной памяти;
- описание средств защиты ввода и вывода на отчуждаемый физический носитель информации и сопоставления пользователя с устройством;
- описание механизма идентификации и аутентификации;
- описание средств регистрации.

### 2.5. Требования к показателям третьего класса защищенности

#### 2.5.1. Дискреционный принцип контроля доступа

Данные требования полностью совпадают с требованиями пятого (п. 2.3.1) и четвертого классов (п. 2.4.1) классов.

#### 2.5.2. Мандатный принцип контроля доступа

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.2).

#### 2.5.3. Очистка памяти

Для СВТ третьего класса защищенности КСЗ должен осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путем записи маскирующей информации в память при ее освобождении (перераспределении).

#### 2.5.4. Изоляция модулей

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.4).

#### 2.5.5. Маркировка документов

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.5).

2.5.6. Защита ввода и вывода на отчуждаемый физический носитель информации

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.6).

#### 2.5.7. Сопоставление пользователя с устройством

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.7).

#### 2.5.8. Идентификация и аутентификация

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.8).

#### 2.5.9. Гарантии проектирования

На начальном этапе проектирования КСЗ должна строиться модель защиты, задающая принцип разграничения доступа и механизм управления доступом. Эта модель должна содержать:

- непротиворечивые правила изменения ПРД;
- правила работы с устройствами ввода и вывода;
- формальную модель механизма управления доступом.

Должна предлагаться высокоуровневая спецификация части КСЗ, реализующего механизм управления доступом и его интерфейсов. Эта спецификация должна быть верифицирована на соответствие заданных принципов разграничения доступа.

#### 2.5.10. Регистрация

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.10).

#### 2.5.11. Взаимодействие пользователя с КСЗ

Для обеспечения возможности изучения, анализа, верификации и модификации КСЗ должен быть хорошо структурирован, его структура должна быть модульной и четко определенной. Интерфейс пользователя и КСЗ должен быть определен (вход в систему, запросы пользователей и КСЗ и т. п.). Должна быть обеспечена надежность такого интерфейса. Каждый интерфейс пользователя и КСЗ должен быть логически изолирован от других таких же интерфейсов.

#### 2.5.12. Надежное восстановление

Процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств КСЗ.

#### 2.5.13. Целостность КСЗ

Необходимо осуществлять периодический контроль за целостностью КСЗ.

Программы должны выполняться в отдельной части оперативной памяти. Это требование должно подвергаться верификации.

#### 2.5.14. Тестирование

СВТ должны подвергаться такому же тестированию, что и СВТ четвертого класса (п. 2.4.12).

Дополнительно должны тестироваться:

- очистка памяти (п. 2.5.3);
- работа механизма надежного восстановления.

#### 2.5.15. Руководство для пользователя

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.4.13).

#### 2.5.16. Руководство по КСЗ

Документ адресован администратору защиты и должен содержать:

- описание контролируемых функций;
- руководство по генерации КСЗ;
- описание старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации;
- руководство по средствам надежного восстановления.

#### 2.5.17. Тестовая документация

В документации должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (п. 2.5.14), а также результатов тестирования.

#### 2.5.18. Конструкторская (проектная) документация

Требуется такая же документация, что и для СВТ четвертого класса (п. 2.4.16). Дополнительно необходимы:

- высокоуровневая спецификация КСЗ и его интерфейсов;
- верификация соответствия высокоуровневой спецификации КСЗ модели защиты.

## 2.6. Требования к показателям второго класса защищенности

### 2.6.1. Дискреционный принцип контроля доступа

Данные требования включают аналогичные требования третьего класса (п. 2.5.1).

Дополнительно требуется, чтобы дискреционные правила разграничения доступа были эквивалентны мандатным правилам (т. е. всякий запрос на доступ должен быть одновременно санкционированным или несанкционированным одновременно и по дискреционным правилам, и по мандатным ПРД).

### 2.6.2. Мандатный принцип контроля доступа

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.2).

### 2.6.3. Очистка памяти

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.3).

### 2.6.4. Изоляция модулей

При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) – т. е. в оперативной памяти ЭВМ программы разных пользователей должны быть изолированы друг от друга. Гарантии изоляции должны быть основаны на архитектуре СВТ.

### 2.6.5. Маркировка документов

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 2.5.5).

2.6.6. Защита ввода и вывода на отчуждаемый физический носитель информации.

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.6).

### 2.6.7. Сопоставление пользователя с устройством

Данные требования полностью совпадают с аналогичным требованием четвертого (п. 2.4.7) и третьего (п. 2.5.7) классов.

### 2.6.8. Идентификация и аутентификация.

Требование полностью совпадает с аналогичным требованием четвертого (п. 2.4.8) и третьего (п. 2.5.8) классов.

#### 2.6.9. Гарантии проектирования

Данные требования включает аналогичные требования третьего класса (п. 2.5.9).

Дополнительно требуется, чтобы высокоуровневые спецификации КСЗ были отображены последовательно в спецификации одного или нескольких нижних уровней, вплоть до реализации высокоуровневой спецификации КСЗ на языке программирования высокого уровня.

При этом методами верификации должно осуществляться доказательство соответствия каждого такого отображения спецификациям высокого (верхнего для данного отображения) уровня. Этот процесс может включать в себя как одно отображение (высокоуровневая спецификация – язык программирования), так и последовательность отображений в промежуточные спецификации с понижением уровня, вплоть до языка программирования. В результате верификации соответствия каждого уровня предыдущему должно достигаться соответствие реализации высокоуровневой спецификации КСЗ модели защиты, изображенной на чертеже (см. рисунок).

#### 2.6.10. Регистрация

Данные требования полностью совпадают с аналогичным требованием четвертого (п. 2.4.10) и третьего (п. 2.5.10) классов.

#### 2.6.11. Взаимодействие пользователя с КСЗ

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.11).

#### 2.6.12. Надежное восстановление

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.12).

#### 2.6.13. Целостность КСЗ

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 2.5.13).

#### 2.6.14. Контроль модификации

При проектировании, построении и сопровождении СВТ должно быть предусмотрено управление конфигурацией СВТ, т. е. контроль изменений в формальной модели, спецификациях (разных уровней), документации, исходном тексте, версии в объектном коде. Должно обеспечиваться соответствие между документацией и тек-

стами программ. Должна осуществляться сравниваемость генерируемых версий. Оригиналы программ должны быть защищены.

#### 2.6.15. Контроль дистрибуции

Должен осуществляться контроль точности копирования в СВТ при изготовлении копий с образца. Изготавливаемая копия должна гарантированно повторять образец.

#### 2.6.16. Тестирование

СВТ второго класса должны тестироваться так же, как и СВТ третьего класса (п. 2.5.14).

Дополнительно должен тестироваться контроль дистрибуции.

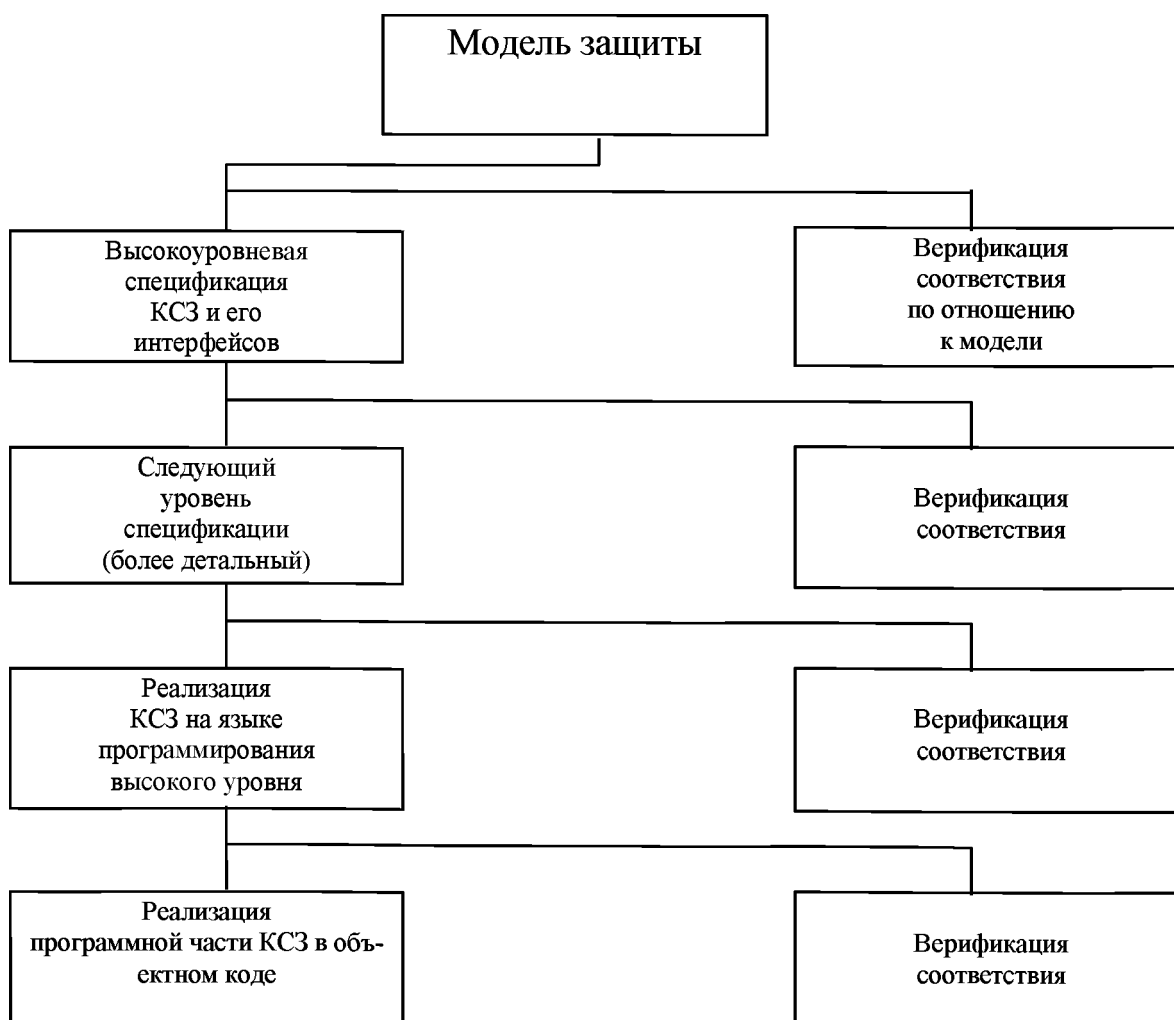


Рис. Схема модели защиты

#### 2.6.17. Руководство для пользователя

Данные требования полностью совпадают с аналогичным требованием четвертого (п. 2.4.13) и третьего (п. 2.5.15) классов.

#### 2.6.18. Руководство по КСЗ

Данные требования включают аналогичные требования третьего класса (п. 2.5.16).

Дополнительно должны быть представлены руководства по надежному восстановлению, по работе со средствами контроля модификации и дистрибуции.

#### 2.6.19. Тестовая документация

Должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (п. 2.6.16), а также результатов тестирования.

#### 2.6.20. Конструкторская (проектная) документация

Требуется такая же документация, что и для СВТ третьего класса (п. 2.5.18).

Дополнительно должны быть описаны гарантии процесса проектирования и эквивалентность дискреционных (п. 2.6.1) и мандатных (п. 2.6.2) ПРД.

### 2.7. Требования к показателям первого класса защищенности

#### 2.7.1. Дискреционный принцип контроля доступа

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.1).

#### 2.7.2. Мандатный принцип контроля доступа

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.2).

#### 2.7.3. Очистка памяти

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.3).

#### 2.7.4. Изоляция модулей

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.4).

#### 2.7.5. Маркировка документов

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.5).

2.7.6. Защита ввода и вывода на отчуждаемый физический носитель информации

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.6).

#### 2.7.7. Сопоставление пользователя с устройством

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.7).

#### 2.7.8. Идентификация и аутентификация

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.8).

#### 2.7.9. Гарантии проектирования

Данные требования включают с аналогичные требования второго класса (п. 2.6.9).

Дополнительно требуется верификация соответствия объектного кода тексту КСЗ на языке высокого уровня.

#### 2.7.10. Регистрация

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.10).

#### 2.7.11. Взаимодействие пользователя с КСЗ

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.11).

#### 2.7.12. Надежное восстановление

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.12).

#### 2.7.13. Целостность КСЗ

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.13).

#### 2.7.14. Контроль модификации

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.14).

#### 2.7.15. Контроль дистрибуции

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.15).

#### 2.7.16. Гарантии архитектуры

КСЗ должен обладать механизмом, гарантирующим перехват диспетчером доступа всех обращений субъектов к объектам.

#### 2.7.17. Тестирование

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.16).

#### 2.7.18. Руководство пользователя

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.17).

#### 2.7.19. Руководство по КСЗ

Данные требования полностью совпадают с аналогичным требованием второго класса (п. 2.6.18).

#### 2.7.20. Тестовая документация

Данные требования полностью совпадают с аналогичными требованиями второго класса (п. 2.6.19).

#### 2.7.21. Конструкторская (проектная) документация

Требуется такая же документация, что и для СВТ второго класса (п. 2.6.20).

Дополнительно разрабатывается описание гарантий процесса проектирования (п. 2.7.9).

### 3. Оценка класса защищенности СВТ (сертификация СВТ)

Оценка класса защищенности СВТ проводится в соответствии с Положением о сертификации средств и систем вычислительной техники и связи по требованиям защиты информации, Временным положением по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники и другими документами.

## **4.5. ВРЕМЕННОЕ ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ РАЗРАБОТКИ, ИЗГОТОВЛЕНИЯ И ЭКСПЛУАТАЦИИ ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ И СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ**

Положение устанавливает единый на территории Российской Федерации порядок исследований и разработок в области:

- защиты информации, обрабатываемой автоматизированными системами различного уровня и назначения, от НСД;
- создания средств вычислительной техники общего и специального назначения, защищенных от утечки, искажения или уничтожения информации за счет НСД, в том числе программных и технических средств защиты информации от НСД;
- создания программных и технических средств защиты информации от НСД в составе систем защиты секретной информации в создаваемых АС.

Положение определяет:

- организационную структуру и порядок проведения работ по защите информации от НСД и взаимодействия при этом на государственном уровне;

- систему государственных нормативных актов, стандартов, руководящих документов и требований по этой проблеме;

- порядок разработки и приемки защищенных СВТ, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД;

- порядок приемки указанных средств и систем перед сдачей в эксплуатацию в составе АС, порядок их эксплуатации и контроля за работоспособностью этих средств и систем в процессе эксплуатации.

1. *Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации.* Документ устанавливает классификацию межсетевых экранов (МЭ) по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Руководящий документ разработан в дополнение к Руководящим документам Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификацию автоматизированных систем и требования по защите информации».

2. *Защита информации. Специальные защитные знаки. Классификация и общие требования.* Документ устанавливает классификацию по классам защиты специальных защитных знаков, предназначенных для контроля доступа к объектам защиты, а также для защиты документов от подделки. Документ является руководством для заказчиков специальных защитных знаков и испытательных лабораторий, проводящих сертификационные испытания в Системе сертификации средств защиты по требованиям безопасности информации.

3. *Защита от несанкционированного доступа к информации.* Настоящий документ устанавливает классификацию программного обеспечения (как отечественного, так и импортного производства) средств защиты информации, в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недеklarированных возможностей. Действие документа не распро-

страняется на программное обеспечение средств криптографической защиты информации.

**Кроме этого, Комиссией разработана группа документов, посвященных вопросам лицензирования и сертификации средств защиты информации.**

*4. Положение о государственном лицензировании деятельности в области защиты информации.* Документ устанавливает основные принципы, организационную структуру системы лицензирования деятельности предприятий в сфере оказания услуг в области защиты информации, а также правила осуществления лицензирования и надзора за деятельностью предприятий, получивших лицензию.

*5. Положение о сертификации средств защиты информации.* Положение устанавливает порядок сертификации средств защиты информации, составляющей государственную тайну, в Российской Федерации. В развитие этого положения разработан целый ряд дополнительных, таких как, Положение о сертификации средств защиты информации по требованиям безопасности информации, Положение по аттестации объектов информатики по требованиям безопасности информации, Положение об аккредитации испытательных лабораторий экспертных комитетов по сертификации средств защиты информации по требованиям безопасности информации и ряд др.

## Глава 5. ЗАЩИТА И ОБРАБОТКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

### 5.1. ВИДЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Согласно Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»:

- *информация* – сведения (сообщения, данные) независимо от формы их представления;
- *конфиденциальность информации* – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- *обладатель информации* – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- *документированная информация* – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация в зависимости от порядка ее предоставления или распространения подразделяется:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая, в соответствии с федеральными законами, подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

К общедоступной информации относятся:

- нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

- информация о состоянии окружающей среды;

- информация о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

- информация, накапливаемая в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

- иная информация, недопустимость ограничения доступа к которой установлена федеральными законами.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Для определения к какому виду относится информация, в законодательстве Российской Федерации имеется «Перечень сведений конфиденциального характера», утвержденный Указом Президента РФ от 13 июля 2015 г. № 357. В нем приводятся сведения конфиденциального характера, к которым относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распро-

странению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых, в соответствии с Федеральными законами от 20 апреля 1995 г. № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства», другими нормативными правовыми актами Российской Федерации, принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве».

К конфиденциальной информации относятся сведения, составляющие:

- государственную тайну;
- коммерческую тайну;
- служебная тайну;
- профессиональную тайну;

– персональные данные.

### ***Государственная тайна***

Отношения, возникающие в связи с отнесением информации к сведениям государственной тайны, регламентируются Законом Российской Федерации 1993 г. № 5485 «О государственной тайне».

В Законе используются следующие основные понятия:

– *государственная тайна* – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

– *носители сведений, составляющих государственную тайну*, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

– *допуск к государственной тайне* – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений;

– *доступ к сведениям, составляющим государственную тайну*, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

К государственной тайне могут быть отнесены следующие сведения:

1. В области экономики, науки и техники:

– о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, мобилизационных мощностях промышленности по изготовлению вооружения и военной техники, об объемах поставок и о запасах стратегических видов сырья и материалов, а также о размещении и фактических размерах государственных материальных резервов;

– об использовании инфраструктуры Российской Федерации в интересах обеспечения ее обороноспособности и безопасности;

– о силах и средствах гражданской обороны, дислокации, предназначении и степени защищенности объектов административного управления, обеспечения безопасности населения, о функцио-

нировании промышленности, транспорта и связи в целом по Российской Федерации;

- об объемах, планах (заданиях) государственного оборонного заказа, выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, связях предприятий по кооперации, разработчиках или изготовителях, указанных вооружения, военной техники и другой оборонной продукции;

- о научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность Российской Федерации;

- о государственных запасах драгоценных металлов и драгоценных камней Российской Федерации, ее финансах и бюджетной политике (кроме обобщенных показателей, характеризующих общее состояние экономики и финансов);

2. В области внешней политики и экономики:

- сведения о внешнеполитической и внешнеэкономической (торговой, кредитной и валютной) деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб ее интересам.

### ***Коммерческая тайна***

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг, и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну.

В Законе используются следующие основные понятия:

- *коммерческая тайна* – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

- *информация, составляющая коммерческую тайну*, – научно-техническая, технологическая, производственная, финансово-эконо-

мическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;

– *режим коммерческой тайны* – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности;

– *обладатель информации, составляющей коммерческую тайну*, – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

– *доступ к информации, составляющей коммерческую тайну*, – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, следующих мер:

1. Определение перечня информации, составляющей коммерческую тайну.

2. Ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

3. Учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана.

4. Регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.

5. Нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц – полное наименование и место нахождения,

для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан:

- ознакомить под расписку работника, доступ которого к этой информации необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

- ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и мерами ответственности за его нарушение;

- создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работник обязан:

- выполнять установленный работодателем режим коммерческой тайны;

- не разглашать эту информацию и не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

- возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

- передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну.

Работодатель вправе потребовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если эта информация разглашена в течение срока действия режима коммерческой тайны.

Причиненные работником или прекратившим трудовые отношения с работодателем лицом убытки не возмещаются, если разглашение информации, составляющей коммерческую тайну, произошло вследствие несоблюдения работодателем мер по обеспечению режима коммерческой тайны, действий третьих лиц или непреодолимой силы.

Трудовым договором с руководителем организации должны предусматриваться его обязанности по обеспечению охраны конфиденциальности, составляющей коммерческую тайну информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны конфиденциальности этой информации.

Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством.

Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

### ***Служебная тайна***

Федеральный закон «О служебной тайне» (проект № 124871-4) регулирует отношения, возникающие в связи с отнесением сведений к служебной тайне, их защитой и снятием ограничений на доступ к указанным сведениям в целях обеспечения прав, свобод и законных интересов граждан и организаций, осуществления установленных законодательством Российской Федерации полномочий федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

В Законе используются следующие основные понятия:

- *конфиденциальные сведения* – сведения, для которых установлен специальный режим сбора, хранения, обработки, распространения и использования, доступ к которым ограничен в соответствии с федеральным законом (за исключением сведений, составляющих государственную тайну);
- *носители сведений, составляющих служебную тайну*, – материальные объекты, в том числе физические поля, в которых соот-

ветствующие сведения находят свое отображение в виде символов, образов, сигналов;

– *отнесение сведений к служебной тайне* – введение в предусмотренном данным Федеральным законом порядке ограничений на распространение сведений, составляющих служебную тайну, и на доступ к ним;

– *режим служебной тайны* – совокупность правовых, организационных, технических и иных мер, принимаемых уполномоченными должностными лицами органов государственной власти и организаций, обеспечивающих ограничения на распространение сведений, составляющих служебную тайну, и на доступ к этим сведениям;

– *сведения, составляющие служебную тайну (служебная тайна)*, – конфиденциальные сведения, образующиеся в процессе управленческой деятельности органа или организации, распространение которых препятствует реализации органом или организацией предоставленных ему полномочий, либо иным образом отрицательно сказывается на их реализации, а также конфиденциальные сведения, полученные органом или организацией в соответствии с их компетенцией в установленном законодательством порядке;

Не подлежат отнесению к служебной тайне сведения:

– содержащиеся в законодательных и иных правовых актах, устанавливающих права, свободы, обязанности граждан и порядок их реализации, а также правовой статус органов государственной власти, органов местного самоуправления, организаций;

– о чрезвычайных ситуациях, происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

– в области экологии, метеорологии, демографии, эпидемиологии и санитарии, культуры, сельского хозяйства, о состоянии преступности и другие сведения, необходимые для обеспечения безопасности граждан и населения в целом;

– о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, организациям и учреждениям;

– о фактах нарушения прав и свобод человека и гражданина, нарушении законности должностными лицами органов государ-

ственной власти, органов местного самоуправления, организаций и учреждений;

- об использовании органами государственной власти, органами местного самоуправления бюджетных средств, иных государственных и местных ресурсов, о состоянии экономики и потребностях населения, если иное не предусмотрено федеральным законом;

- о размерах золотого запаса и государственных валютных резервах Российской Федерации;

- о деятельности органов государственной власти и органов местного самоуправления, накапливаемые в информационных системах органов и организаций и представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан, а также содержащиеся в официальных изданиях, поступающих в фонды библиотек и архивов;

- о состоянии здоровья лиц, занимающих государственные должности категории «А»;

- сведения о деятельности органов государственной власти, обязательные для размещения в информационных системах общего пользования в соответствии с законодательством Российской Федерации.

### ***Порядок отнесения сведений к служебной тайне***

Отнесение сведений к служебной тайне осуществляется на основании перечней сведений, разрабатываемых органами государственной власти и утверждаемых их руководителями.

Перечни сведений, отнесенных к служебной тайне, подлежат не реже чем один раз в пять лет обязательному пересмотру в целях проверки соответствия их содержания действительной потребности органов государственной власти в введении ограничений на доступ к отдельным категориям сведений.

Документы, содержащие сведения, составляющие служебную тайну, независимо от формы представления этих документов, должны включать помимо обязательных реквизитов, следующие:

- ограничительную пометку «для служебного пользования»;
- наименование органа государственной власти, установившего ограничения на распространение сведений;
- регистрационный номер документа в системе делопроизводства;

– дату снятия ограничений на распространение сведений, либо событие, при наступлении которого ограничения подлежат отмене (в случае, если срок сохранения режима служебной тайны составляет менее 5 лет);

– наименование должности лица, подписавшего документа, его собственноручную подпись или электронную цифровую подпись, используемую в соответствии с законодательством Российской Федерации.

Граждане Российской Федерации допускаются к сведениям, составляющим служебную тайну, по решению руководителя органа или организации, в распоряжении которых они находятся, в объемах, вызванных необходимостью. Каждый факт ознакомления гражданина с конкретными сведениями, составляющими служебную тайну, подлежит учету.

### ***Профессиональная тайна***

Профессиональная тайна – это защищаемая законом информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

### ***Основные виды профессиональной тайны***

1. *Врачебная тайна.* Врачебная тайна – это социально-этическое, медицинское и правовое понятие, которое запрещает разглашение данных о человеке третьим лицам.

Согласно Федеральному закону от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», врачебной тайной являются сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении.

Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением некоторых случаев, установленных в законе.

2. *Тайна связи.* В Федеральном законе от 7 июля 2003 г. № 126-ФЗ «О связи» говорится, что на территории Российской Фе-

дерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

3. *Адвокатская тайна.* Согласно Федеральному закону от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации», адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.

4. *Тайна усыновления.* Норма об охране тайны усыновления, закрепленная в Семейном кодексе Российской Федерации (СК), основана на требованиях Конституции РФ о праве граждан на личную и семейную тайну. Согласно СК, тайна усыновления охраняется законом. Разглашение сведений об усыновлении может причинить моральные (нравственные) страдания ребенку, усыновителям, воспрепятствовать созданию нормальной семейной обстановки и затруднить процесс воспитания ребенка.

5. *Тайна страхования.* В Гражданском кодексе Российской Федерации говорится, что страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными статьей 139 или статьей 150.

6. *Тайна исповеди.* Согласно Федеральному закону от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и религиозных объединениях», тайна исповеди – сведения, доверенные священнослужителю гражданином на исповеди. Тайна исповеди охраняется законом. Священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали известны ему из исповеди.

### ***Персональные данные***

Отношения, связанные с обработкой персональных данных, осуществляемой государственными органами, муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких

средств, регулирует Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Целью Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

*Персональные данные* – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением некоторых случаев, предусмотренных законом.

## **5.2. ПОРЯДОК ОБРАЩЕНИЯ С КОНФИДЕНЦИАЛЬНЫМИ ДОКУМЕНТАМИ**

Конфиденциальная информация фиксируется на различных носителях. Документы и электронные носители, содержащие конфиденциальную информацию подлежат обязательному учету. Для этого документам присваивается одна из пометок ограничения распространения:

- конфиденциально – «К»;
- строго конфиденциально – «СК»;
- для служебного пользования – «ДСП».

### ***Оформление документов***

Необходимость проставления пометки ограничения на документах, содержащих конфиденциальные сведения, определяется исполнителем документа на стадии подготовки документа. Подтверждение соответствия грифа на документах производится руководителем подразделения или руководством организации, подписывающим или утверждающим документ.

На электронных носителях информации такая пометка проставляется в любом удобном месте на элементе конструкции носителя информации.

Руководитель структурного подразделения, где находятся документы, содержащие конфиденциальные сведения, несет персональную ответственность за организацию работы с ними, за обеспечение доступа к ним сотрудников согласно списку, а также лиц, имеющим разрешение на работу с этими документами.

### ***Учет документов***

Обработка входящей и исходящей корреспонденции, содержащей конфиденциальные сведения, а также учет внутренних документов в организации осуществляется назначенным для этой цели сотрудником (уполномоченным).

Входящая конфиденциальная корреспонденция вскрывается уполномоченным сотрудником. Работа с входящими конфиденциальными документами включает следующие этапы:

- прием;
- регистрацию;
- доклад руководству о полученных документах;
- рассмотрение руководством и принятие решения;
- направление на исполнение;
- исполнение;
- помещения документа в дело;
- принятие решения о дальнейшем использовании;
- дальнейшее использование;
- передача в архив;
- уничтожение.

При получении проверяется:

- целостность их упаковки;
- количество листов;
- количество экземпляров;
- наличие приложений (если они указаны в сопроводительном письме).

В случае обнаружения нарушения целостности конверта или отсутствия некоторых документов – составляется акт в двух экземплярах. Один экземпляр акта отправляется в адрес отправителя, а другой – хранится в организации.

Документы должны быть зарегистрированы (учтены). Регистрация документов заключается в присвоении учетного номера и

проставлении его на документе с указанием даты регистрации. Учетный номер документу присваивается в организации.

После регистрации документы передаются руководству для принятия решения. Руководитель после рассмотрения документа определяет исполнителя и дает указания по исполнению документа. Эти указания оформляются на самом документе в виде резолюции.

С резолюцией руководителя конфиденциальный документ передается исполнителю.

При приеме конфиденциального документа на электронном носителе проверяется наличие и подлинность электронной цифровой подписи (ЭЦП) корреспондента.

При отсутствии ЭЦП на входящем конфиденциальном документе уполномоченный сотрудник обязан проставить в нем свою ЭЦП для гарантии неизменности документа.

При обнаружении недостатчи вложения составляется акт, в котором перечисляются все вложения, оказавшиеся в наличии, а также недостающие, их тематика, наличие или отсутствие повреждений на конверте, другие необходимые, по мнению составителей акта, сведения, а для конфиденциальных документов в электронном виде – объем и тематика полученного документа, факт нарушения ЭЦП.

По завершении работы с документом на нем проставляется отметка о его исполнении и направлении в дело. После чего документ подшивается в дело.

Решение о дальнейшем использовании конфиденциального документа определяется его значением и практической ценностью. В зависимости от этого конфиденциальные документы могут:

- использоваться в дальнейшем;
- передаваться в архив на хранение;
- уничтожаться.

Работа с конфиденциальными исходящими документами включает следующие этапы:

- разработка проекта документа;
- согласование документа;
- подписание документа;
- регистрация документа;
- отправка документа.

Проект исходящего конфиденциального документа разрабатывается исполнителем документа затем передается на подпись руководству организации. После подписания документа он регистрируется в журнале регистрации исходящих конфиденциальных доку-

ментов. Рассылка конфиденциальных документов осуществляется согласно подписанных руководством списков с указанием учетных номеров отправленных документов.

Конфиденциальная информация в электронном виде может приниматься и передаваться только с использованием защищенных каналов связи на рабочих местах, специально предназначенных для этих целей.

Исходящие конфиденциальные документы в электронном виде скрепляются ЭЦП исполнителя и помещаются в электронное сообщение.

### ***Порядок работы с конфиденциальными внутренними документами***

Работа с конфиденциальными внутренними документами включает следующие этапы:

- разработка проекта документа;
- согласование;
- подписание документа;
- регистрация документа;
- направление на исполнение;
- исполнение;
- помещение документа в дело;
- принятие решения о дальнейшем использовании;
- дальнейшее использование;
- передача в архив;
- уничтожение.

Отправка документов, содержащих конфиденциальную информацию, средствами факсимильной связи допускается только после получения на это разрешения руководства организации.

При передаче документов между структурными подразделениями их регистрация не производится.

### ***Печатание и копирование документов***

Печать конфиденциальных документов осуществляется исполнителями, либо лицами, имеющими право допуска к работе с конфиденциальной информацией. При печати документов должна быть исключена возможность просмотра информации посторонними лицами.

Черновики и варианты документов, уничтожаются лично исполнителем, который несет персональную ответственность за их

уничтожение. Уничтожение осуществляется способами, исключающими возможность прочтения.

Документы, поступившие из сторонних организаций, копируются с согласия этих организаций.

Входящие документы копируются (тиражируются) с обязательной отметкой в журнале регистрации о количестве размноженных экземпляров. В журнале также отмечается, кому направлен каждый экземпляр размноженного документа.

Количество копий документа определяется исполнителем документа.

Ответственность за несанкционированное копирование документов возлагается на руководителя структурного подразделения.

#### ***Порядок комплектования документов в дела***

Исполненные конфиденциальные документы подшиваются в дела. На обложке дела, в которое помещены документы, проставляется ограничительная пометка.

Делами, в которые подшиты документы, могут пользоваться только сотрудники, которым это необходимо для выполнения своих функциональных обязанностей. На отдельном листе, хранящемся в деле, указывается список сотрудников, которым разрешено ознакомление с документами, подшитыми в дело.

#### ***Хранение документов***

Конфиденциальная информация хранится в форме печатных документов и в электронном виде.

Средства обработки и хранения конфиденциальной информации должны быть расположены так, чтобы уменьшить возможность подглядывания. Запрещается оставлять на рабочем месте документы без присмотра. Документы, не используемые в данный момент, следует убирать в особенности при уходе из помещения.

Конфиденциальные документы в электронном виде должны храниться только на компьютерах, оснащенных специальными средствами защиты.

Хранение документов, дел и электронных носителей осуществляется в сейфах, расположенных в надежно запираемых служебных помещениях.

#### ***Снятие грифа ограниченного распространения***

Снятие грифа с конфиденциального документа производится руководителем подразделения или руководством организации, подписавшим (утвердившим) документ, при условии, что сведения, со-

держась в нем, утратили конфиденциальность, а также при корректировке «Перечня сведений конфиденциальной информации».

Снятие грифа с информации, владельцем которой на договорных началах является сторонняя организация, разрешается только с ее письменного согласия.

О снятии грифа делается отметка на самом документе, в учетных экземплярах и в учетном журнале.

### ***Уничтожение документов***

Уничтожение документов и дел осуществляется по акту путем, исключающим возможность восстановления текста. Уничтожение информации на электронных носителях производится путем ее стирания с использованием специальных средств.

Акты на уничтожение регистрируются и комплектуются в отдельное дело.

После уничтожения документов в журналах регистрации делается отметка об уничтожении со ссылкой на соответствующий акт.

### ***Порядок отправки документов***

Оформленные и зарегистрированные документы передаются на отправку. Отправляемые документы должны быть упакованы в отдельные от другой документации конверты.

К конвертам с документами составляется опись вложения в двух экземплярах, один из которых вместе с документами направляется получателю, другой – подшивается в дело.

Доставка документов в другие организации осуществляется специальными службами доставки (фельдсвязь, спецсвязь, заказными или ценными почтовыми отправлениями). При необходимости документы с пометкой ограниченного распространения могут доставляться курьером.

### ***Ответственность***

Сотрудник, получивший конфиденциальный документ, обязан принимать меры для обеспечения его сохранности и не разглашать содержащиеся в нем сведения если этого не требуется для выполнения им своих служебных обязанностей.

Разглашение сведений или утрата документов конфиденциального характера является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, а также договорными обязательствами между организацией и сотрудником.

## СОКРАЩЕНИЯ

- ГОСТ Р** – государственные стандарты РФ.  
**ГОСТ** – государственные и межгосударственные стандарты.  
**ОСТ** – отраслевые стандарты.  
**СТП** – стандарты предприятий.  
**ФЗ** – Федеральный закон.  
**ИТ** – информационные технологии.  
**ИБ** – информационная безопасность.  
**СУИБ** – система управления информационной безопасностью.  
**ПО** – программное обеспечение.  
**ISO** – Международная организация по стандартизации.  
**ИЕС** – Международная электротехническая комиссия.  
**СМИБ** – система менеджмента информационной безопасности.  
**ФГУ «ГНИИИ ПТЗИ ФСТЭК России»** – федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю».  
**ФСТЭК** – Федеральная служба по техническому и экспортному контролю.  
**ЗИ** – защита информации.  
**ТЗИ** – техническая защита информации.  
**НСД** – несанкционированный доступ.  
**НСВ** – несанкционированное воздействие.  
**ПНВ** – преднамеренное воздействие.  
**НПНВ** – непреднамеренное воздействие.  
**27 ЦНИИ МО РФ** – 27 Центральный научно-исследовательский институт Министерства обороны Российской Федерации.  
**НКЦ «ЦНИИКА-СПИН»** – Научно-консультационный центр по созданию и применению информационных технологий.  
**ПС** – программные средства.  
**КВ** – компьютерные вирусы.  
**ПЭВМ** – персональная электронно-вычислительная машина (персональный компьютер).  
**ЭВМ** – электронно-вычислительная машина.  
**ОИ** – объект информатизации.  
**ООО «ЦБИ»** – общество с ограниченной ответственностью «Центр безопасности информации».

**ФГУ «4 ЦНИИ Минобороны России»** – Федеральное государственное учреждение «4 Центральный научно-исследовательский институт Министерства обороны России».

**ФГУП «ЦНИИАТОМИНФОРМ»** – Федеральное государственное унитарное предприятие «Центральный научно-исследовательский институт управления, экономики и информации Росатома».

**ОО** – объект оценки.

**ПЗ** – профиль защиты.

**ЗБ** – задание по безопасности.

**ОУД** – оценочный уровень доверия.

**ПБО** – политика безопасности объекта оценки.

**ФБО** – функции безопасности объекта оценки.

**ОДФ ФБО** – область действия функций безопасности объекта оценки.

**ПФБ** – политика функции безопасности.

**ИФБО** – интерфейс функции безопасности объекта оценки.

**ОДФ** – область действия функции безопасности объекта оценки.

**СФБ** – стойкость функции безопасности.

**ФБ** – функция безопасности.

**ПБО** – политика безопасности объекта оценки.

**ФГУ «ГНИИИ ПТЗИ ФСТЭК России»** – федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю».

**ФГУ «ГНИИИ ПТЗИ ФСТЭК России»** – Федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю».

**ООО НПФ «Кристалл»** – общество с ограниченной ответственностью научно-производственная фирма «Кристалл».

**СМИБ** – система менеджмента информационной безопасности.

**ОЭСР** – организация экономического сотрудничества и развития.

**Ростехрегулирование** – федеральное агентство по техническому регулированию и метрологии.

**МТУ** – межрегиональные территориальные управления.

## КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Кто осуществляет руководство российской национальной стандартизацией?
2. Что включают в состав технического комитета по стандартизации для разработки проекта стандарта?
3. Назовите одну из ключевых задач стандартизации (не перепутайте с целями).
4. Назовите одну из целей стандартизации (не перепутайте с задачами).
5. Какова категория стандарта, который обязателен к применению предприятиями и организациями, деятельность которых попадает под положения соответствующих норм?
6. Перечислите стандарты, применимые одновременно в нескольких странах, которые объединены по культурным или географическим признакам.
7. Какие стандарты действуют в отношении конкретного сегмента экономики?
8. С помощью каких стандартов устанавливаются требования в отношении методов (или же процессов) на участках производства?
9. Назовите государственный стандарт РФ.
10. Назовите межгосударственный стандарт.
11. Назовите корпоративный стандарт.
12. Назовите отраслевой стандарт.
13. ГОСТ Р – какой стандарт имеет такое сокращение?
14. Как расшифровывается ГОСТ?
15. Как расшифровывается ОСТ?
16. Как расшифровать СТП?
17. Какая схема организации национального фонда источников права в сфере стандартизации принята в России?
18. В классификации источников норм в стандартизации на каком уровне располагается техническое законодательство?
19. В классификации источников норм в стандартизации на каком уровне располагаются документы, в которых содержатся нормы, регулирующие производственные объекты и процессы?
20. В классификации источников норм в стандартизации на каком уровне располагаются источники, содержащие в себе отраслевые стандарты, и те, которые создаются научно-техническими обществами?

21. В классификации источников норм в стандартизации на каком уровне располагаются источники, включающие стандарты предприятий, а также дополняющие и сопровождающие их нормы?

22. Требования к стандарту. Каковы возможность его применения к постоянно развивающимся информационным технологиям и время его «устаревания»?

23. Стандарт BS 7799. Опишите его.

24. Какой стандарт называется «Информационная технология. Практический кодекс по менеджменту информационной безопасности»?

25. Какой стандарт называется «Управление информационной безопасностью. Практические правила»?

26. Какой стандарт называется «Руководство по управлению рисками информационной безопасности»?

27. Какой стандарт называется «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности»?

28. Какой стандарт называется «Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности – Определения и основные принципы»?

29. Как называется стандарт BS 7799-1?

30. Как называется стандарт BS 7799-2?

31. Как называется стандарт BS 7799-3?

32. Как называется стандарт ISO/IEC 17799?

33. Как называется стандарт ISO/IEC 27000?

34. Какой стандарт называется «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования»?

35. Какой стандарт называется «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности»?

36. Как называется стандарт ISO/IEC 27001?

37. Как называется стандарт ISO/IEC 27002?

38. Какой стандарт называется «Защита информации. Основные термины и определения»?

39. Какой стандарт называется «Информационные технологии. Основные термины и определения в области технической защиты информации»?

40. Какой стандарт называется «Защита информации. Испытание программных средств на наличие компьютерных вирусов»?

41. Какой стандарт называется «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»?

42. Какой стандарт называется «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»?

43. Как называется стандарт ГОСТ Р 50922-2006?

44. Как называется стандарт Р 50.1.053-2005?

45. Как называется стандарт ГОСТ Р 51188-1998?

46. Как называется стандарт ГОСТ Р 51275-2006?

47. Как называется стандарт ГОСТ Р ИСО/МЭК 15408-2008?

48. Какой стандарт называется «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Введение и общая модель»?

49. Какой стандарт называется «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Функциональные компоненты безопасности»?

50. Какой стандарт называется «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Требования доверия к безопасности»?

51. Какой стандарт называется «Информационная технология. Практические правила управления информационной безопасностью»?

52. Какой стандарт называется «Методы и средства обеспечения безопасности системы менеджмента информационной безопасности»?

53. Как называется стандарт ГОСТ Р ИСО/МЭК 27001-2006?

54. Как называется стандарт ГОСТ Р ИСО/МЭК 17799-2005?

55. Как называется стандарт ГОСТ Р ИСО/МЭК 15408-3-2008?

56. Как называется стандарт ГОСТ Р ИСО/МЭК 15408-2-2013?

57. Как называется стандарт ГОСТ Р ИСО/МЭК 15408-1-2008?

58. Руководящие документы Гостехкомиссии России. Дайте название документа.

59. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа. Термины и определения». Какие вопросы рассматриваются в документе?

60. Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных си-

стем от несанкционированного доступа (НСД) к информации». Какие вопросы рассматриваются в документе?

61. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Какие вопросы рассматриваются в документе?

62. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Какие вопросы рассматриваются в документе?

63. Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Какие вопросы рассматриваются в документе?

64. Федеральный закон «Об информации, информационных технологиях и защите информации». Кратко опишите его.

65. Закон Российской Федерации «О государственной тайне». Дайте его характеристику.

66. Дайте понятие Федеральному закону «О коммерческой тайне».

67. Прокомментируйте Федеральный закон «О служебной тайне».

68. Опишите Федеральный закон «О персональных данных».

69. Дайте название закона 2006 г. № 152.

70. Дайте название закона 2006 г. № 149.

71. Дайте название закона проект № 124871-4.

72. Дайте название закона 2004 г. № 98.

73. Дайте название закона 1993 г. № 5485.

74. Дайте название закона 2006 г. № 149.

## СПИСОК ЛИТЕРАТУРЫ

1. Британский стандарт BS 7799-1:2005 «Информационная технология. Практический кодекс по менеджменту информационной безопасности».
2. Британский стандарт BS 7799-2:2005 «Управление информационной безопасностью. Практические правила».
3. Британский стандарт BS 7799-3:2006 «Руководство по управлению рисками информационной безопасности».
4. Международный стандарт ISO/IEC 17799:2005 «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности».
5. Международный стандарт ISO/IEC 27001:2013. «Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности – Требования». Вторая редакция (01.10.2013).
6. Международный стандарт ISO/IEC 27002:2013. «Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью». Вторая редакция (01.10.2013).
7. Национальный стандарт Российской Федерации ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».
8. Национальный стандарт Российской Федерации Р 50.1.053-2005. «Информационные технологии. Основные термины и определения в области технической защиты информации».
9. Национальный стандарт Российской Федерации ГОСТ Р 51188-1998. «Защита информации. Испытание программных средств на наличие компьютерных вирусов».
10. Национальный стандарт Российской Федерации ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
11. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ГОСТ Р ИСО/МЭК 15408-1-2008. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».
12. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ГОСТ Р ИСО/МЭК 15408-2-2013. «Информационная технология. Методы и средства обеспечения безопасности. Крите-

рии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности».

13. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ГОСТ Р ИСО/МЭК 15408-3-2008. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности».

14. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-2008. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

15. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью».

16. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ГОСТ Р ИСО/МЭК 27001-2006. «Методы и средства обеспечения безопасности системы менеджмента информационной безопасности».

17. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа. Термины и определения» (введен 30 марта 1992 г.).

18. Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа (НСД) к информации» (введен 30 марта 1992 г.).

19. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (введен 30 марта 1992 г.).

20. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (введен 30 марта 1992 г.).

21. Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники» (введен 30 марта 1992 г.).

22. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г.

23. Гражданский Кодекс Российской Федерации. От 30 ноября 1994 г. № 51-ФЗ.

24. Семейный Кодекс Российской Федерации. От 29 декабря 1995 г. № 223-ФЗ.

25. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».

26. Указ Президента РФ от 13 июля 2015 г. № 357 «Перечень сведений конфиденциального характера».

27. Федеральный закон от 20 апреля 1995 г. № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов».

28. Федеральный закон от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства».

29. Федеральный закон от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве».

30. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне».

31. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

32. Федеральный закон «О служебной тайне» (проект № 124871-4).

33. Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

34. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

35. Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации».

36. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

37. Федеральный закон от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и религиозных объединениях».

Учебное издание

СЫЧЕВ Юрий Николаевич

СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.  
ЗАЩИТА И ОБРАБОТКА КОНФИДЕНЦИАЛЬНЫХ  
ДОКУМЕНТОВ

Учебное пособие

Редактор *Ю. А. Еремина*

Оформление обложки *К. Г. Жигалов*

Подписано в печать 11.01.17. Формат 60х84 1/16.

Усл. печ. л. 13,0. Уч.-изд. л. 12,92.

Тираж 100 экз. Заказ

ФГБОУ ВО «РЭУ им. Г. В. Плеханова».

117997, Москва, Стремянный пер., 36.

Напечатано в ФГБОУ ВО «РЭУ им. Г. В. Плеханова».

117997, Москва, Стремянный пер., 36.

Для заметок