ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ХАКАСИЯ

«ХАКАССКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

Специальность 09.02.07

«Информационные системы и программирование»

ПРАКТИЧЕСКАЯ РАБОТА №4

тема: СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Руководитель:

\_\_\_\_\_\_\_\_\_\_\_\_ Н.И. Мороз

(подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(оценка, дата)

Выполнил:

Студент группы ИС(ПРО) – 31

\_\_\_\_\_\_\_\_\_\_\_\_ В.Е Байкалов

(подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(дата)

Абакан 2022 г.

Содержание

[вВедение 3](#_Toc97815185)

[Основная часть 4](#_Toc97815186)

[1 Российское и зарубежное законодательство в области ИБ 4](#_Toc97815187)

[2 Оранжевая книга 8](#_Toc97815189)

[3 Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий". Основные понятия. 9](#_Toc97815190)

# вВедение

Специалистам в области информационной безопасности (ИБ) сегодня почти невозможно обойтись без знаний соответствующих стандартов и спецификаций. На то имеется несколько причин.

Формальная состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и/или Руководящим документам Гостехкомиссии России) закреплена законодательно. Однако наиболее убедительны содержательные причины. Во-первых, стандарты и спецификации - одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях ИБ. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами. Во-вторых, и те, и другие являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов, причем в Internet-сообществе это средство действительно работает, и весьма эффективно.

# Основная часть

1. Российское и зарубежное законодательство в области ИБ

Таблица 1.1 – Правовые акты

|  |  |  |
| --- | --- | --- |
| **№** | **Правовые акты в области ИБ, дата принятия** | **Цель акта. Основные статьи , относящие к области ИБ** |
| 1 | Уголовный кодекс Российской Федерации (редакция от 18 февраля 2020 года). | статья 272. Неправомерный доступ к компьютерной информации;  статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;  статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.  статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. |
| 2 | Конституция, принятая 12 декабря 1993 года. | Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 - право на знание достоверной информации о состоянии окружающей среды.  Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации. |
| 3 | Гражданский кодекс РФ 21 октября 1994 **года** | Статья 1225 вводит перечень охраняемых результатов интеллектуальной деятельности и средств индивидуализации. Статьи 946 и 1123 посвящены тайне страхования и тайне завещания соответственно. Это подразумевает,как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности у тех, кто должен защищать вышеуказанную информацию. |
| 4 | Закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ | В статье 9 Закона содержатся следующие положения:  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.  Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.  Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.  Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.  Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.  Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.  Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.  Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.  Статья 16 целиком посвящена вопросам защиты информации. Процитируем ее полностью.  Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:  обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;  соблюдение конфиденциальности информации ограниченного доступа;  реализацию права на доступ к информации.  Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.  Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.  Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:  предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;  своевременное обнаружение фактов несанкционированного доступа к информации;  предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;  недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;  возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;  постоянный контроль за обеспечением уровня защищенности информации.  нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации  Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.  Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.  В процитированной статье Закона фигурируют все три основных аспекта информационной безопасности: доступность, целостность и конфиденциальность. Кроме того, обязательным является отслеживание нарушений безопасности и постоянный контроль за обеспечением уровня защищенности информации. |
| 5 | Федеральный закон "О персональных данных" | В статье 1 определяется сфера действия рассматриваемого закона:  Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях.  В статье 5 Закона сформулированы следующие принципы обработки персональных данных:  Обработка персональных данных должна осуществляться на законной и справедливой основе.  Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.  Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.  Обработке подлежат только персональные данные, которые отвечают целям их обработки.  Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.  Статья 12 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Нас будут интересовать следующие виды:  разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);  деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);  разработка и производство средств защиты конфиденциальной информации;  деятельность по технической защите конфиденциальной информации; |

# Оранжевая книга

Стандарт содержит два основных вида требований безопасности:

* Функциональные.
* Требования доверия.

Функциональная безопасность является частью общей безопасности системы или часть оборудования, которая зависит от автоматической защиты, правильно работающей в ответ на ее входы или отказ предсказуемым образом (отказоустойчивый ). Система автоматической защиты должна быть спроектирована так, чтобы правильно обрабатывать вероятные человеческие ошибки, сбои оборудования и операционные / экологические нагрузки.

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности, всего 11 функциональных классов (в трёх группах), 66 семейств, 135 компонентов.

Требования гарантии безопасности (доверия) — требования, предъявляемые к технологии и процессу разработки и эксплуатации объекта оценки. Разделены на 10 классов, 44 семейства, 93 компонента, которые охватывают различные этапы жизненного цикла.

1. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий". Основные понятия.

ISO/IEC 15408 направлен на защиту информации от несанкционированного раскрытия, модификации или потери возможности ее использования. Категории защиты, относящиеся к этим трем типам нарушения безопасности, обычно называют конфиденциальностью, целостностью и доступностью соответственно.

Область применения:

ГОСТ Р ИСО/МЭК 15408 определяет критерии, за которыми исторически закрепилось название "Общие критерии" (OK). OK предназначены для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий (ИТ). Устанавливая общую базу критериев, OK делают результаты оценки безопасности ИТ значимыми для более широкой аудитории.

OK дают возможность сравнения результатов независимых оценок безопасности. Это достигается предоставлением общего набора требований к функциям безопасности продуктов и систем ИТ и к мерам доверия, применяемых 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 помогут потребителям решить, являются ли продукты или системы ИТ достаточно безопасными для их предполагаемого применения и приемлемы ли прогнозируемые риски при их использовании.

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

OK направлены на защиту информации от несанкционированного раскрытия, модификации или потери возможности ее использования. Категории защиты, относящиеся к этим трем типам нарушения безопасности, обычно называют конфиденциальностью, целостностью и доступностью соответственно. OK могут быть также применены к тем аспектам безопасности ИТ, которые выходят за пределы этих трех понятий. OK сосредоточены на угрозах информации, возникающих в результате действий человека, как злоумышленных, так и иных, но возможно также применение OK и для некоторых угроз, не связанных с человеческим фактором. Кроме того, OK могут быть применены и в других областях ИТ, но не декларируется их правомочность вне строго ограниченной сферы безопасности ИТ.

OK применимы 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.

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

OK не содержат критериев оценки безопасности, касающихся административных мер безопасности, непосредственно не относящихся к мерам безопасности ИТ. Известно, однако, что безопасность ОО в значительной степени может быть достигнута административными мерами, такими как организационные меры, управление персоналом, физическая защита и процедурный контроль. 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 ОК применимы и в этой области. В частности, рассмотрены некоторые аспекты физической защиты ОО.

В ОК не рассматривается ни методология оценки, ни административно-правовая структура, в рамках которой критерии могут применяться органами оценки. Тем не менее, ожидается, что ОК будут использоваться для целей оценки в контексте такой структуры и такой методологии.

Процедуры использования результатов оценки при аттестации продуктов и систем ИТ находятся вне области действия ОК. 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 на тех аспектах среды эксплуатации, которые могут непосредственно влиять на безопасное использование элементов ИТ. Результаты процесса оценки 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.

Критерии для оценки специфических качеств криптографических алгоритмов не входят в ОК. Если требуется независимая оценка математических свойств криптографии, встроенной в ОО, то в системе оценки, в рамках которой применяются ОК, необходимо предусмотреть проведение таких оценок.

Главные достоинства ГОСТ Р ИСО/МЭК 15408:

* полнота требований к И Б;
* гибкость в применении;
* открытость для последующего развития с учетом новейших достижений науки и техники.

**Таблица 1.1 – Правовые акты**

|  |  |  |
| --- | --- | --- |
| **№** | **Название элемента** | **Содержание элемента** |
| 1 | Область применения | Данная часть ИСО/МЭК 15408 определяет требования доверия ИСО/МЭК 15408 и включает оценочные уровни доверия (ОУД), определяющие шкалу для измерения доверия для ОО-компонентов, составные пакеты доверия (СоПД), определяющие шкалу для измерения доверия для составных ОО, отдельные компоненты доверия, из которых составлены уровни и пакеты доверия, а также критерии для оценки ПЗ и ЗБ. |
| 2 | Нормативные ссылки | Указанные в данном разделе документы являются необходимыми для применения настоящего стандарта. Для датированных ссылок используют только указанное издание. Для недатированных ссылок - последнее издание со всеми изменениями и дополнениями.  ИСО/МЭК 15408-1, Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель.  ИСО/МЭК 15408-2, Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные компоненты безопасности. |
| 3 | Термины, определения | В настоящем стандарте применяются термины, определения, обозначения и сокращения, приведенные в ИСО/МЭК 15408-1. |
| 4 | Краткий обзор | Описание разделов, содержащихся в стандарте |
| 5 | Парадигма доверия ИСО/МЭК 15408 | Цель данного раздела состоит в изложении основных принципов и подходов к установлению доверия к безопасности. Данный раздел позволит понять логику построения требований доверия в ИСО/МЭК 15408-3. |
| 6. | Требования доверия к безопасности | Требования доверия к безопасности для: классов, семейств и компонентов, ОУД, СоПД |
| 7 | Оценочные уровни доверия | Оценочные уровни доверия (ОУД) образуют возрастающую шкалу, которая позволяет соотнести получаемый уровень доверия со стоимостью и возможностью достижения этой степени доверия. В подходе ИСО/МЭК 15408 определяются отдельные понятия для доверия к ОО после завершения оценки и по поддержанию доверия во время эксплуатации ОО. |
| 8 | Составные пакеты доверия | Составные пакеты доверия (СоПД) образуют возрастающую шкалу, которая позволяет соотнести уровень полученного доверия с затратами и возможностью достижения этой степени доверия для составных ОО.  Важно отметить, что лишь небольшая часть семейств и компонентов доверия из ИСО/МЭК 15408-3 включена в составные пакеты доверия. Это связано с тем, что они основываются на результатах оценки ранее оцененных сущностей (базовых компонентов и зависимых компонентов) и в этой связи нельзя говорить, что они не обеспечивают значимое и требуемое доверие. |
| 9 | Оценка профиля защиты | Оценка ПЗ требуется для демонстрации того, что ПЗ является полным, непротиворечивым и правильным, а в случае, если ПЗ основывается на одном или нескольких других ПЗ или пакетах доверия, что этот ПЗ является корректной реализацией этих ПЗ и пакетов доверия. Эти свойства необходимы для того, чтобы ПЗ можно было использовать в качестве основы для разработки ЗБ или другого ПЗ. |
| 10 | Оценка задания по безопасности | Оценка ЗБ требуется для демонстрации того, что ЗБ является правильным и внутренне непротиворечивым, и если ЗБ основано на одном или более ПЗ или пакетах доверия, что ЗБ является корректной реализацией этих ПЗ и пакетов. Эти свойства необходимы для того, чтобы можно было использовать ЗБ в качестве основы при оценке ОО. |
| 11 | Разработка | Требования класса "Разработка" предоставляют информацию об объекте оценки. Сведения, полученные путем изучения этой информации, служат основой для проведения анализа уязвимостей и тестирования ОО в соответствии с описанием, представленным в классах AVA "Анализ уязвимостей" и ATE "Тестирование". |
| 12 | Руководства | Класс "Руководства" предоставляет требования к документации руководств для всех пользовательских ролей. Для безопасной подготовки и безопасного функционирования ОО необходимо описать все существенные аспекты, относящиеся к безопасному применению ОО. В данном классе также рассматриваются случаи непреднамеренных неточностей конфигурации или ошибок эксплуатации ОО. |
| 13 | Поддержка жизненного цикла | Поддержка жизненного цикла является аспектом установления организационного порядка и управления в процессе совершенствования ОО во время его разработки и сопровождения. Уверенность в соответствии ОО требованиям безопасности к ОО будет больше, если анализ безопасности и формирование свидетельств выполняются на регулярной основе как неотъемлемая часть деятельности по разработке и сопровождению. |
| 14 | Тестирование | Класс "Тестирование" включает в себя четыре семейства: ATE\_COV "Покрытие", ATE\_DPT "Глубина", ATE\_FUN "Функциональное тестирование" и ATE\_IND "Независимое тестирование" (например, функциональное тестирование, выполняемое оценщиками). Тестирование позволяет получить доверие к тому, что ФБО функционирует в описанном (в функциональной спецификации, проекте ОО, представлении реализации) режиме. |
| 15 | Оценка уязвимости | Класс AVA "Оценка уязвимостей" учитывает возможность наличия пригодных для использования уязвимостей, вносимых при разработке или при эксплуатации ОО. |
| 16 | Композиция | Класс ACO: "Композиция" включает пять семейств. Эти семейства определяют требования доверия, разработанные для обеспечения уверенности, что составной ОО будет функционировать в безопасном режиме, полагаясь на функциональные возможности безопасности, предоставляемые ранее оцененными программными, программно-аппаратными или аппаратными компонентами. |