ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Санкт – Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

Отделение: Информационных технологий и управления в телекоммуникациях
Специальность: 09.02.03 «Программирование в компьютерных системах»

МДК.03.03 ДОКУМЕНТИРОВАНИЕ И СЕРТИФИКАЦИЯ
Раздел ПМ 3. Разработка программной документации

Преподаватель **Рожков А.И.**

Санкт-Петербург 2020

СПб ГУТ)))

ТЕМА 3.1. Документирование и сертификация

Лекция. Стандарты и спецификации в области информационной безопасности

План занятия:

1. Российское и зарубежное законодательство в области ИБ
2. Обзор международных и национальных стандартов и спецификаций в области ИБ: «Оранжевая книга», ИСО 15408

1. Российское и зарубежное законодательство в области ИБ

При обеспечении информационной безопасности успех может быть эффективным только при применении комплексного подхода. **Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:**

- законодательного;
- административного (приказы, распоряжения, политики и другие организационные действия руководства организаций, связанных с защищаемыми информационными ресурсами);
- процедурного (меры безопасности, ориентированные на персонал);
- программно-технического;
- физического (комплексная защита помещений, оборудования и персонала).

Законодательный уровень является важнейшим для обеспечения информационной безопасности и различают на нем две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности ("мерами ограничительной направленности");
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но необходимо подчеркнуть аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту силами системных администраторов и сотрудников службы безопасности предприятия было бы неправильно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Зарубежное законодательство в области ИБ

Одним из важнейших законов в этом направлении является американский "Закон об информационной безопасности" (Computer Security Act of 1987, Public Law 100-235, January 8, 1988). Цель закона — реализация минимальных, но достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений спектра возможных действий.

В начале Закона называется конкретный исполнитель — Национальный институт стандартов и технологий, НИСТ (National Institute of Standardization — NIST), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и подлогов, выполняемых с помощью компьютеров. Документы, выпускаемые институтом, являются руководствами "симметричного действия", служащие как для регламентации действий специалистов, так и для повышения информированности общества.

Согласно Закону, все операторы федеральных информационных систем и баз данных, содержащих конфиденциальную информацию, должны сформировать планы обеспечения ИБ. Обязательным является и периодическое обучение всего персонала таких ИС. Институт, в свою очередь, обязан проводить исследования природы и масштаба уязвимых мест, вырабатывать экономически оправданные меры защиты. Результаты исследований применяются как в государственных системах, так и в частном секторе.

Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерство обороны, Министерство энергетики, Агентство национальной безопасности (АНБ) и т.д., чтобы избежать дублирования и несовместимости.

В 1997 году появился законопроект "О совершенствовании информационной безопасности" (Computer Security Enhancement Act of 1997, H.R. 1903), направленный на усиление роли НИСТ и упрощение операций с криптографическими средствами.

В законопроекте констатируется, что частные компании-разработчики готовы предоставить криптографические средства для обеспечения конфиденциальности, целостности и аутентичности данных и что разработка и использование шифровальных технологий должны происходить на основании требований рынка, а не распоряжений правительства. Кроме того, здесь отмечается, что за пределами США имеются сопоставимые и общедоступные криптографические технологии, и это следует учитывать при выработке экспортных ограничений, чтобы не снижать конкурентоспособность американских производителей аппаратного и программного обеспечения.

В 2001 году был одобрен Палатой представителей и передан в Сенат новый вариант рассмотренного законопроекта — Computer Security Enhancement Act of 2001 (H.R. 1259 RFS).

Программа безопасности, предусматривающая экономически оправданные защитные меры, синхронизированные с жизненным циклом информационных технологий и систем, **неоднократно входит в законодательные акты США и** согласно пункту 3534 ("Обязанности

федеральных ведомств") подглавы II ("Информационная безопасность") главы 35 ("Координация федеральной информационной политики") рубрики 44 ("Общественные издания и документы"), такая "Программа" **должна включать**:

- периодическую оценку рисков с рассмотрением внутренних и внешних угроз целостности, конфиденциальности и доступности систем, а также данных, ассоциированных с критически важными операциями и ресурсами;
- правила и процедуры, позволяющие, опираясь на проведенный анализ рисков, экономически оправданным образом уменьшить риски до приемлемого уровня;
- обучение персонала с целью информирования о существующих рисках и об обязанностях, выполнение которых необходимо для их (рисков) нейтрализации;
- периодический аудит и (пере)оценку эффективности правил и процедур;
- порядок и действия при внесении существенных изменений в систему;

- процедуры выявления нарушений информационной безопасности и реагирования на них; эти процедуры должны помочь уменьшить риски, избежать крупных потерь; организовать взаимодействие с правоохранительными органами.

В законодательстве Германии можно выделить "Закон о защите данных" (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)), который целиком посвящен защите персональных данных.

Законом устанавливается приоритет интересов национальной безопасности над сохранением тайны частной жизни. В остальном, права личности защищены весьма тщательно. Например, если сотрудник фирмы обрабатывает персональные данные в интересах частных компаний, он дает подписку о неразглашении, которая действует и после перехода на другую работу. Государственные учреждения, хранящие и обрабатывающие персональные данные, несут ответственность за нарушение тайны частной жизни "субъекта данных", как говорится в Законе.

Из законодательства Великобритании можно выделить семейство так называемых "добровольных стандартов" BS 7799, помогающих организациям на практике сформировать программы безопасности.

Российское законодательство в области ИБ

Основным законом Российской Федерации является Конституция. В соответствии с Конституцией, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Конституция гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, 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.

В сентябре 2000 года Президент Российской Федерации В.В.Путин утвердил "Доктрину информационной безопасности". Она закладывает основы информационной политики государства. С учетом существующих угроз для защиты национальных интересов России государство планирует активно развивать отечественную индустрию средств информации, коммуникации и связи с последующим выходом продукции на мировой рынок, обеспечивать гарантии безопасности для национальных информационных и телекоммуникационных систем и защиту государственных секретов с помощью соответствующих технических средств. Одновременно предусматривается повышать эффективность информационного обеспечения деятельности государства.

Принятие этого документа ставит в повестку дня и вопрос о необходимости совершенствования российского законодательства. К примеру, речь идет о принятии законов, касающихся пресечения компьютерной преступности.

Основополагающие законы и нормативные акты Российской Федерации в области информационной безопасности в их первой редакции:

1.Закон РФ "О государственной тайне" от 21.07.93 г. № 5485-1.

2.Закон РФ "О коммерческой тайне" (версия 18.04.2018 г.).

3.Закон РФ "Об информации, информатизации и защите информации" от 27.07.2006 г.

4.Закон РФ "О персональных данных" (версия 24.04.2020 г.).

5.Закон РФ "О федеральных органах правительственной связи и информации" от 19.02.93 г. № 4524-1.

6.Положение о государственной системе защиты информации в Российской Федерации от ИТР и от утечки по техническим каналам. (Постановление Правительства РФ от 15.09.93 г. № 912-51).

7.Положение о Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России). Утвержден Указом Президента РФ от 19 февраля 1999 г. № 212 в ред. Указов Президента РФ от 06.03.2002 N 257, от 05.10.2002 №1129

В настоящее время практически все эти законы и положения уточнены и дополнены соответствующими главами, параграфами и поправками, отражающими реалия текущей ситуации.

В Гражданском кодексе Российской Федерации фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, "информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности". Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

В Уголовном кодекс Российской Федерации глава 28 "Преступления в сфере компьютерной информации" содержит три соответствующие статьи:

- статья 272 "Неправомерный доступ к компьютерной информации" - подразумевает посягательства на конфиденциальность;

- статья 273 "Создание, использование и распространение вредоносных программ для ЭВМ" - определяет действия с вредоносным ПО;

- статья 274 "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети" - определяет действия с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации..

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Основополагающим среди российских законов, посвященных вопросам ИБ, следует считать закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года (принят Государственной Думой РФ 25 января 1995 года; актуальная версия закона от 03.04.2020). **В нём даются основные определения и намечаются направления развития законодательства в данной области:**

- **информация** — сведения (сообщения, данные) независимо от формы их представления;
- **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;
- **электронный документ** - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

- **информационная система** — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **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;
- **конфиденциальность информации** — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Закон выделяет следующие цели защиты информации:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;

- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Согласно закону "Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу". "Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, — уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";
- в отношении конфиденциальной документированной информации — собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;
- в отношении персональных данных — Федеральным законом".

Обратим внимание, что защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники.

В качестве основного инструмента защиты информации закон предлагает мощные универсальные средства — лицензирование и сертификацию:

1. Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".

2. Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

3. Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.

4. Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

2. Обзор международных и национальных стандартов и спецификаций в области ИБ: «Оранжевая книга», ИСО 15408

Существуют стандарты и спецификации двух существенно разных видов:

- **оценочные стандарты, направленные на классификацию информационных систем и средств защиты по требованиям безопасности -** выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. ;
- **технические спецификации, регламентирующие различные аспекты реализации средств защиты -** определяют, как строить ИС предписанной архитектуры.

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал **стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем".**

Данный труд, **называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года**. Уже его название заслуживает комментария. **Речь идет не о безопасных, а о доверенных системах, то есть системах, которым можно оказать определенную степень доверия.**

"Оранжевая книга" **поясняет понятие безопасной системы, которая "управляет, посредством соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию".**

Очевидно, однако, что абсолютно безопасных систем не существует, что это абстракция. Есть смысл оценивать лишь степень доверия, которое разумно оказать той или иной системе.

В "Оранжевой книге" **доверенная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".**

Обратим внимание, что в рассматриваемых Критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и (статической) целостности. Вопросы доступности "Оранжевая книга" не затрагивает.

Степень доверия оценивается по двум основным критериям:

- **Политика безопасности - набор законов, правил и норм поведения, специфицирующих, как организация обрабатывает, защищает и распространяет информацию.** В частности, правила определяют, в каких случаях пользователь может оперировать с конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. **Политика безопасности - это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.**

- **Уровень гарантированности - мера доверия, которая может быть оказана архитектуре и реализации ИС.** Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. **Это пассивный аспект защиты.**

Важным средством обеспечения безопасности является механизм подотчетности (протоколирования). Доверенная система должна фиксировать все события, касающиеся безопасности.

Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности. Доверенная вычислительная база - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности.

Основное назначение доверенной вычислительной базы - выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

От монитора обращений требуется выполнение трех свойств:

- **Изолированность.** Монитор должен быть защищен от отслеживания своей работы.
- **Полнота.** Монитор должен вызываться при каждом обращении, не должно быть способов его обхода.
- **Верифицируемость.** Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. Ядро безопасности - это основа, на которой строятся все защитные механизмы, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют периметром безопасности. Компоненты, лежащих вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что внутри владений, считается доверенным, а то, что вне, - нет.

Согласно "Оранжевой книге", политика безопасности должна включать в себя следующие элементы:

1. **произвольное управление доступом** - (называемое иногда **дискреционным**) - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту.;

2. **безопасность повторного использования объектов** - важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.;

3. **метки безопасности -** для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта - степень конфиденциальности содержащейся в нем информации. Метки безопасности состоят из двух частей - уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории - неупорядоченное. Назначение последних - описать предметную область, к которой относятся данные.

4. **принудительное управление доступом** - основано на сопоставлении меток безопасности субъекта и объекта. Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может писать в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий). Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

Механизм подотчетности является дополнением подобной политики. Цель подотчетности - в каждый момент времени знать, кто работает в системе и что он делает. Средства подотчетности делятся на три категории:

- **идентификация и аутентификация** - обычный способ идентификации - ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности (аутентификации) пользователя - пароль.;

- **предоставление доверенного пути** - связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие, потенциально опасные компоненты ИС. Цель предоставления доверенного пути - дать пользователю возможность убедиться в подлинности обслуживающей его системы;

- **анализ регистрационной информации** - анализ регистрационной информации (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы..

"Критерии ..." Министерства обороны США открыли путь к ранжированию информационных систем по степени доверия безопасности.

В "Оранжевой книге" определяется четыре уровня доверия - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Всего имеется шесть классов безопасности - C1, C2, B1, B2, B3, A1.

Такова классификация, введенная в "Оранжевой книге". Коротко ее можно сформулировать так:

- уровень C - произвольное управление доступом;
- уровень B - принудительное управление доступом;
- уровень A - верифицируемая безопасность.