# СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

# РОССИЙСКОЕ И ЗАРУБЕЖНОЕ ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ИБ

- Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года. В соответствии со статьей 24 Конституции, 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.
- 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.

- 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.
- Отметим, что право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности, актуальности и целостности, представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

- Перечислим некоторые основополагающие законы и нормативные акты Российской Федерации в области информационной безопасности в их первой редакции:
- 1. Закон РФ "О государственной тайне" от 21.7.93 г. № 5485-1.
- 2. Закон РФ "О коммерческой тайне" (версия 28.12.94 г.).
- 3. Закон РФ "Об информации, информатизации и защите информации" от 25.1.95 г.
- 4. Закон РФ "О персональных данных" (версия 20.02.95 г.).
- 5. Закон РФ Российской Федерации "О федеральных органах правительственной связи и информации" от 19.2.93 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 15.9.93 г. № 912-51).
- 7. Положение о Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России). Распоряжение Президента Российской Федерации от 28.12.92 г. № 829-рпс.

- 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";
- · статья 273 "Создание, использование и распространение вредоносных программ для ЭВМ";
- · статья 274 "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети".

- Первая из указанных статей подразумевает посягательства на конфиденциальность, вторая определяет действия с вредоносным ПО, третья — с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации. В свете бурного развития локальных, региональных, национальных и всемирной сетей включение в сферу действия УК РФ вопросов доступности информационных сервисов является очень своевременным.
- 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.

- Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе "О государственной тайне". В нем государственная тайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

- Закон "Об информации, информатизации и защите информации"
- Основополагающим среди российских законов, посвященных вопросам информационной безопасности, 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 под номером 149-ФЗ от 27 июля 2006 г.). В нём даются основные определения и намечаются направления развития законодательства в данной области.

- Приведём примеры некоторых определений:
- · информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- · документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- · информационные процессы — процессы сбора, обработки, накопления, хранения, поиска и распространения информации;
- · информационная система — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;
- · информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- · информация о гражданах (персональные данные) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
- · конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;
- · пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

- 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.

- В качестве основного инструмента защиты информации закон предлагает мощные универсальные средства — лицензирование и сертификацию (статья 19):
- 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.

- Следующим законом, имеющим важное значение в сфере информационной безопасности, является Закон РФ "О лицензировании отдельных видов деятельности" от 8 августа 2001 года, № 128-ФЗ (Принят Государственной Думой 13 июля 2001 года).

Статья 17 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии:

- · распространение шифровальных (криптографических) средств;
- · техническое обслуживание шифровальных (криптографических) средств;
- · предоставление услуг в области шифрования информации;
- · разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- · выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;
- · выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- · разработка и (или) производство средств защиты конфиденциальной информации;
- · техническая защита конфиденциальной информации;
- · разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

- Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации (ФАПСИ) и Государственная техническая комиссия при Президенте РФ (Гостехкомиссия РФ). ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. Эти же организации возглавляют работы по сертификации средств соответствующей направленности. Кроме того, ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ.

- 10 января 2002 года Президентом РФ был подписан чрезвычайно важный закон "Об электронной цифровой подписи", № 1-ФЗ (принят Государственной Думой 13 декабря 2001 года), развивающий и конкретизирующий приведенные выше положения закона "Об информации...". Его роль поясняется в статье 1.
- 1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

Согласно Закону, электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.
- закон определяет сведения, которые должен содержать сертификат ключа подписи:
- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима запись об этом вносится удостоверяющим центром в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

# ОБЗОР МЕЖДУНАРОДНЫХ И НАЦИОНАЛЬНЫХ СТАНДАРТОВ И СПЕЦИФИКАЦИЙ В ОБЛАСТИ ИБ: «ОРАНЖЕВАЯ КНИГА», ИСО 15408 И ДР.

- Стандарты и спецификации двух видов:
- оценочных стандартов, направленных на классификацию информационных систем и средств защиты по требованиям безопасности;
- технических спецификаций, регламентирующих различные аспекты *реализации* средств защиты.

- 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. 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, с помощью соответствующих средств, доступом к информации так, что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию".

- Очевидно, однако, что абсолютно *безопасных систем* не существует, это абстракция. Есть смысл оценивать лишь *степень доверия*, которое можно 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".

- *Степень доверия* оценивается по двум основным критериям.
- ***Политика безопасности*** - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать 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.

- 2. ***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 ее компонентов.
- *Уровень гарантированности* показывает, насколько корректны механизмы, отвечающие за *реализацию политики безопасности*. Это пассивный аспект защиты.
- Важным средством обеспечения безопасности является механизм *подотчетности* (протоколирования).
- *Доверенная система* должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть *анализом регистрационной информации*.
- 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*. Качество вычислительной базы определяется исключительно ее *реализацией* и корректностью исходных данных, которые вводит системный администратор.
- Вообще говоря, компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.
- 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.

- *Монитор обращений* должен обладать тремя качествами:
- *Изолированность*. Необходимо предупредить возможность отслеживания работы монитора.
- *Полнота*. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.
- *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. Помимо перечисленных выше свойств *монитора обращений*, ядро должно гарантировать собственную неизменность.

- Границу *доверенной вычислительной базы* называют ***периметром безопасности***. Как уже указывалось, компоненты, лежащие 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 находится внутри владений, считается доверенным, а то, что вне, - нет.

**Механизмы безопасности**

- Согласно "Оранжевой книге", политика безопасности должна обязательно включать в себя следующие элементы:
- произвольное управление доступом ;
- безопасность повторного использования объектов ;
- метки безопасности ;
- принудительное управление доступом.

- 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 предоставлять другим субъектам или отбирать у них права доступа к объекту.
- Безопасность повторного использования объектов - важное 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.

- 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.
- Согласно "Оранжевой книге", 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.

- Если понимать политику безопасности узко, то есть как правила разграничения доступа, то механизм подотчетности является дополнением подобной политики. Цель подотчетности - в каждый момент времени знать, кто работает в системе и что делает. Средства подотчетности делятся на три категории:
- идентификация и аутентификация ;
- предоставление доверенного пути ;
- анализ регистрационной информации.

- Обычный способ идентификации - ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности ( аутентификации ) пользователя - пароль.
- Доверенный путь 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 (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы

- Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. "Оранжевая книга" предусматривает наличие средств выборочного протоколирования, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.
- Переходя к пассивным аспектам защиты, укажем, что в "Оранжевой книге" рассматривается два вида гарантированности - операционная и технологическая. Операционная гарантированность относится к архитектурным и реализационным аспектам системы, в то время как технологическая - к методам построения и сопровождения.

- Операционная гарантированность включает в себя проверку следующих элементов:
- архитектура системы;
- целостность системы;
- проверка тайных каналов передачи информации ;
- доверенное администрирование;
- доверенное восстановление после сбоев.

- Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности .
- Технологическая гарантированность охватывает весь жизненный цикл ИС, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные "закладки".

- Классы безопасности
- "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. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, ее политика безопасности и уровень гарантированности должны удовлетворять заданным требованиям, из которых мы упомянем лишь важнейшие.

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

- уровень С - произвольное управление доступом ;
- уровень В - принудительное управление доступом ;
- уровень А - верифицируемая безопасность.

- Конечно, в адрес "Критериев ..." можно высказать целый ряд серьезных замечаний (таких, например, как полное игнорирование проблем, возникающих в распределенных системах). Тем не менее, следует подчеркнуть, что публикация "Оранжевой книги" без всякого преувеличения стала эпохальным событием в области информационной безопасности. Появился общепризнанный понятийный базис, без которого даже обсуждение проблем ИБ было бы затруднительным.
- Отметим, что огромный идейный потенциал "Оранжевой книги" пока во многом остается невостребованным. Прежде всего это касается концепции технологической гарантированности, охватывающей весь жизненный цикл системы - от выработки спецификаций до фазы эксплуатации. При современной технологии программирования результирующая система не содержит информации, присутствующей в исходных спецификациях, теряется информация о семантике программ. Важность данного обстоятельства мы планируем продемонстрировать далее, в лекции об управлении доступом.