**Лекция 3:**

**Основы законодательства в области обеспечения информационной безопасности**

### **Аннотация:**В лекции рассказывается о нормативной базе для защиты информации.

### **Правовое обеспечение информационной безопасности**

При обеспечении информационной безопасности успех может быть эффективным только при применении комплексного подхода. Выше было отмечено, что 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. Будем различать на этом уровне 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.

**Краткий обзор зарубежного законодательства в области информационной безопасности**

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. Помимо регламентации дополнительных функций НИСТ, Закон предписывает создать при Министерстве торговли США комиссию по информационной безопасности, которая должна:

* выявлять перспективные управленческие, техническо-технологические, программные и физические меры, способствующие повышению ИБ;
* выдавать рекомендации Национальному институту стандартов и технологий, доводить их до сведения всех заинтересованных ведомств.

С практической точки зрения важен раздел № 6 Закона, обязывающий все правительственные ведомства сформировать план обеспечения информационной безопасности, направленный на то, чтобы компенсировать риски и предотвратить возможный ущерб от утери, неправильного использования, несанкционированного доступа или модификации информации в федеральных системах. Копии планов направляются в НИСТ и в Агентство национальной безопасности (АНБ, National Safety Agency — NSA).

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.

Очень важен раздел 3, в котором закрепляется обязанность НИСТ готовить стандарты, руководства, средства и методы для инфраструктуры открытых ключей (ниже аналогичный закон РФ об ЭЦП) по запросам частного сектора. Эти нормативные документы позволяют сформировать негосударственную инфраструктуру, пригодную для взаимодействия с федеральными ИС. В разделе № 4 особое внимание обращается на необходимость анализа средств и методов оценки уязвимых мест других продуктов частного сектора в области ИБ. Законом поощряется разработка требований и правил безопасности, нейтральных по отношению к конкретным техническим решениям, использование в федеральных ИС коммерческих продуктов, участие в реализации шифровальных технологий, позволяющее в конечном итоге сформировать инфраструктуру, которую можно рассматривать как резервную для федеральных ИС.

Важно, что в соответствии с разделами № 10 и далее предусматривается выделение финансирования, называются точные сроки реализации программ партнёрства и проведения исследований инфраструктуры с открытыми ключами, национальной инфраструктуры цифровых подписей. В частности, предусматривается, что для удостоверяющих центров должны быть разработаны типовые правила и процедуры, порядок лицензирования, стандарты аудита. 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).

За четыре года (1997-2001 годы) на законодательном и других уровнях информационной безопасности США было сделано следующие важные разработки:

* смягчены экспортные ограничения на криптографические средства (январь 2000 г.);
* сформирована инфраструктура с открытыми ключами;
* разработано большое число стандартов (например, новый стандарт электронной цифровой подписи — FIPS 186-2, январь 2000 г.).

Программа безопасности, предусматривающая экономически оправданные защитные меры, синхронизированные с жизненным циклом информационных технологий и систем, неоднократно входит в законодательные акты США. Например, 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. В материальном выражении ответственность ограничена верхним пределом в 250 тысяч немецких марок.

Из законодательства Великобритании можно выделить семейство так называемых "добровольных стандартов" BS 7799, помогающих организациям на практике сформировать программы безопасности. Ниже положения этого системообразующего стандарта будут рассмотрены подробнее.

Закон вводит следующие основные понятия:

* электронный документ;
* электронная цифровая подпись;
* владелец сертификата ключа подписи;
* средства электронной цифровой подписи
* сертификат средств электронной цифровой подписи;
* закрытый ключ электронной цифровой подписи;
* сертификат ключа подписи;
* пользователь сертификата ключа подписи;
* информационная система общего пользования;
* корпоративная информационная система.

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.

В заключение раздела отметим, что в области информационной безопасности законы реально работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи очень важны руководящие документы Гостехкомиссии РФ, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно выделим утвержденный в июле 1997 года "Руководящий документ по межсетевым экранам", вводящий в официальную сферу использования один из самых современных классов защитных средств.

В современном мире глобальных сетей нормативно-правовая база должна быть согласована с международной практикой. Особое внимание следует обратить на то, что желательно привести российские стандарты и сертификационные нормативы в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности. Есть целый ряд оснований для того, чтобы это сделать. Одно из них — необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских компаний, второе (более существенное) — доминирование на современном этапе развития аппаратно-программных продуктов зарубежного производства.

На законодательном уровне должен быть решен вопрос об отношении к таким изделиям. Здесь необходимо выделить два аспекта: независимость в области информационных технологий и информационную безопасность. Использование зарубежных продуктов в некоторых критически важных системах (в первую очередь, оборонных), в принципе, может представлять угрозу национальной безопасности (в том числе информационной), поскольку нельзя исключить вероятности встраивания "закладных" элементов. В то же время, в подавляющем большинстве случаев потенциальные угрозы информационной безопасности носят исключительно внутренний характер. В таких условиях незаконность использования зарубежных разработок (ввиду сложностей с их сертификацией) при отсутствии отечественных аналогов затрудняет (или вообще делает невозможной) защиту информации без серьезных на то оснований.

Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно сложна, однако, как показывает опыт европейских стран, решить ее можно. Сложившаяся в Европе система сертификации по требованиям информационной безопасности позволила оценить операционные системы, системы управления базами данных и другие разработки американских компаний. Вхождение России в эту систему и участие российских специалистов в сертификационных испытаниях в состоянии снять имеющееся противоречие между независимостью в области информационных технологий и информационной безопасностью без какого-либо ущерба для национальной безопасности.