Основы информационной безопасности

Лекция 5.

Законодательный уровень информационной безопасности

Что такое законодательный уровень информационной безопасности и почему он важен

В деле обеспечения информационной безопасности успех может принести только комплексный подход. Мы уже указывали, что для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

Что такое законодательный уровень информационной безопасности и почему он важен

- законодательного;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

Что такое законодательный уровень информационной безопасности и почему он важен

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Что такое законодательный уровень информационной безопасности и почему он важен

Мы будем различать на законодательном 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 (назовем их 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).

Что такое законодательный уровень информационной безопасности и почему он важен

На практике обе группы мер важны в равной степени, но нам хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Что такое законодательный уровень информационной безопасности и почему он важен

Самое важное (и, вероятно, самое трудное) на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Обзор белорусского законодательства в области информационной безопасности

Основным законом Республики Беларусь является Конституция

(с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г. и 17 октября 2004 г.)

Обзор белорусского законодательства в области информационной безопасности

Статья 34. Гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни, состоянии окружающей среды.

Государственные органы, общественные объединения, должностные лица обязаны предоставить гражданину Республики Беларусь возможность ознакомиться с материалами, затрагивающими его права и законные интересы.

Пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав.

Обзор белорусского законодательства в области информационной безопасности

Статья 28. Каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство.

Обзор белорусского законодательства в области информационной безопасности

В **Гражданском кодексе РБ** фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно ему 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.

Обзор белорусского законодательства в области информационной безопасности

Весьма продвинутым в плане информационной безопасности является **Уголовный кодекс РБ**

В зависимости от тяжести последствий:

Статья 349. Несанкционированный доступ к компьютерной информации (до 7 лет)

Статья 350. Модификация компьютерной информации (до 7 лет)

Статья 351. Компьютерный саботаж (до 10 лет)

Статья 352. Неправомерное завладение компьютерной информацией (до 2 лет)

Обзор белорусского законодательства в области информационной безопасности

Статья 354. Разработка, использование либо распространение вредоносных программ (до 10 лет)

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети (до 7 лет)

Основной закон

Основополагающим среди белорусских законов, посвященных вопросам информационной безопасности, следует считать

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ

10 ноября 2008 г. № 455-З

Об информации, информатизации и защите информации

Основной закон

В нем даются основные определения, намечаются направления, в которых должно развиваться законодательство в данной области, регулируются отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Основной закон

Процитируем основные определения:

- информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи;
- информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

Основной закон

- информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации;
- информационная услуга – деятельность по осуществлению поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также защиты информации;
- информационные отношения – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий;

Основной закон

- информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах;
- обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору;
- оператор информационной системы – субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством ее информационные услуги;

Основной закон

Статья 4. Принципы правового регулирования информационных отношений

Правовое регулирование информационных отношений осуществляется на основе следующих принципов:

- свободы поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией;
- установления ограничений распространения и (или) предоставления информации только законодательными актами Республики Беларусь;

Основной закон

- своевременности предоставления, объективности, полноты и достоверности информации;
- защиты информации о частной жизни физического лица и персональных данных;
- обеспечения безопасности личности, общества и государства при пользовании информацией и применении информационных технологий;
- обязательности применения определенных информационных технологий для создания и эксплуатации информационных систем и информационных сетей в случаях, установленных законодательством Республики Беларусь.

Основной закон

Отметим, что в этих принципах явным образом фигурируют **целостность** (достоверность) и **доступность** (**своевременность предоставления**) информации.

Основной закон

Глава 7 целиком посвящена вопросам защиты информации. Процитируем ее полностью.

Основной закон

Статья 27. Цели защиты информации

Целями защиты информации являются:

- обеспечение национальной безопасности, суверенитета Республики Беларусь;
- сохранение информации о частной жизни физических лиц и неразглашение персональных данных, содержащихся в информационных системах;
- обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;
- недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий.

Основной закон

Статья 28. Основные требования по защите информации

- Защите подлежит информация, неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу.
- Требования по защите общедоступной информации могут устанавливаться только в целях недопущения ее уничтожения, модификации (изменения), блокирования правомерного доступа к ней.
- Требования по защите информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено, определяются законодательством Республики Беларусь.

Основной закон

Статья 29. Меры по защите информации

- К правовым мерам по защите информации относятся заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.
- К организационным мерам по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.
- К техническим (программно-техническим) мерам по защите информации относятся меры по использованию средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации.

Основной закон

ГЛАВА 8
ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ

Статья 33. Права и обязанности обладателя информации

Статья 34. Права и обязанности пользователя информации

Статья 35. Права и обязанности пользователя информационной системы и (или) информационной сети

Статья 36. Права и обязанности собственника информационных ресурсов

Статья 37. Права и обязанности собственника программно-технических средств, информационных систем и информационных сетей

Лицензирование

Мы продолжим наш обзор:
УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ 1 сентября 2010 г. № 450

О лицензировании отдельных видов деятельности

Начнем с основных определений.

Лицензирование

лицензия – специальное разрешение на осуществление вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом соискателю лицензии;

Лицензирование

лицензирование – комплекс реализуемых государством мер, связанных с выдачей лицензий, их дубликатов, внесением в лицензии изменений и (или) дополнений, приостановлением, возобновлением, продлением срока действия лицензий, прекращением их действия, аннулированием лицензий, контролем за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий;

Лицензирование

ГЛАВА 21

ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИМИ МЕТОДАМИ, ВКЛЮЧАЯ ПРИМЕНЕНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Лицензирование

Лицензируемая деятельность включает составляющие работы и услуги:

- 13.1. разработка, производство, реализация, монтаж, наладка, сервисное обслуживание (либо выборка из указанного перечня работ) технических средств обработки информации в защищенном исполнении, программных средств обработки информации в защищенном исполнении, технических, программных, программно-аппаратных средств защиты информации и контроля ее защищенности, средств криптографической защиты информации (либо выборка из указанного перечня средств)

Лицензирование

- 13.2. проведение испытаний, специальные исследования (либо выборка из указанного перечня работ) технических средств обработки информации, программных средств обработки информации, технических, программных, программно-аппаратных средств защиты информации и контроля ее защищенности, средств криптографической защиты информации (либо выборка из указанного перечня средств) по требованиям безопасности информации
- 13.3. проектирование, создание (либо выборка из указанного перечня работ) систем защиты информации на объектах информатизации

Лицензирование

- 13.4. проектирование, создание (либо выборка из указанного перечня работ) систем защиты информации информационных систем
- 13.5. аттестация объектов информатизации
- 13.6. аттестация систем защиты информации информационных систем
- 13.7. проведение работ по выявлению специальных технических средств, предназначенных для негласного получения информации

Лицензирование

- 13.8. удостоверение формы внешнего представления электронного документа на бумажном носителе
- 13.9. оказание услуг по распространению открытых ключей проверки подписи

Электронная цифровая подпись

Еще один важный закон:

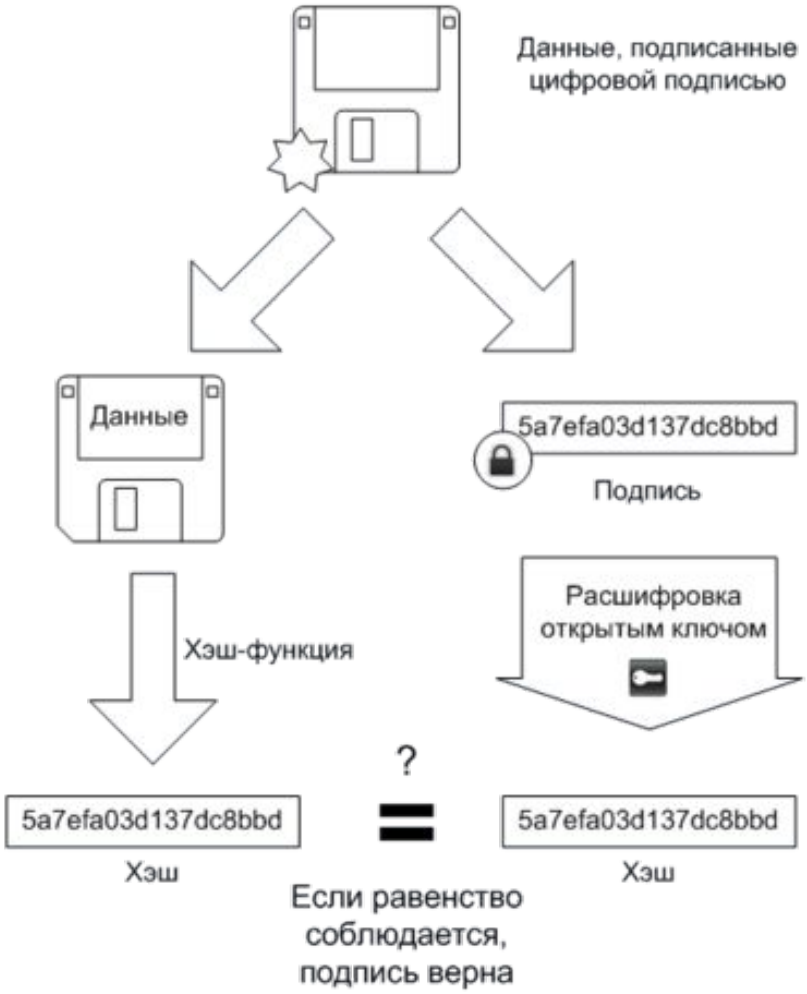
ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ

28 декабря 2009 г. № 113-З

Об электронном документе и электронной цифровой подписи

Подписывание

Проверка



Электронная цифровая подпись

Настоящий Закон направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе.

Для целей настоящего Закона используются следующие термины и их определения:

Электронная цифровая подпись

электронная цифровая подпись – последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности;

электронный документ – документ в электронном виде с реквизитами, позволяющими установить его целостность и подлинность.

Электронная цифровая подпись

сертификат открытого ключа – электронный документ, изданный поставщиком услуг и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа определенным организации или физическому лицу, и иную информацию, предусмотренную настоящим Законом и иными актами законодательства Республики Беларусь;

Электронная цифровая подпись

средство электронной цифровой подписи – программное, программно-техническое или техническое средство, с помощью которого реализуются одна или несколько из следующих функций: выработка электронной цифровой подписи, проверка электронной цифровой подписи, выработка личного ключа или открытого ключа;

Электронная цифровая подпись

личный ключ электронной цифровой подписи (далее – личный ключ) – последовательность символов, принадлежащая определенным организации или физическому лицу и используемая при выработке электронной цифровой подписи;

Стандартизация в области ИБ

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ О ТЕХНИЧЕСКОМ НОРМИРОВАНИИ И СТАНДАРТИЗАЦИИ

Статья 15. Виды технических нормативных правовых актов

К техническим нормативным правовым актам в области технического нормирования и стандартизации относятся:

- технические регламенты;
- технические кодексы;
- стандарты, в том числе государственные стандарты, стандарты организаций;
- технические условия.

Стандартизация в области ИБ

- **Технические регламенты** разрабатываются в целях защиты жизни, здоровья и наследственности человека, имущества и охраны окружающей среды, а также предупреждения действий, вводящих в заблуждение потребителей продукции и услуг относительно их назначения, качества или безопасности. Разработка технических регламентов в иных целях не допускается.
- Технический регламент применяется одинаковым образом и в равной мере независимо от страны и (или) места происхождения продукции.
- Требования утвержденного технического регламента являются обязательными для соблюдения всеми субъектами технического нормирования и стандартизации.
- Технический регламент не может быть введен в действие, если отсутствуют методики контроля, измерений и испытаний технических требований, установленных в техническом регламенте.

Стандартизация в области ИБ

Технические кодексы разрабатываются с целью реализации требований технических регламентов, повышения качества процессов разработки (проектирования), производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации продукции или оказания услуг.

- Разработка и утверждение технических кодексов осуществляются республиканскими органами государственного управления.
- Требования технических кодексов к процессам разработки (проектирования), производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации продукции или оказанию услуг основываются на результатах установившейся практики.
- Технические кодексы вводятся в действие после их государственной регистрации.

Стандартизация в области ИБ

Государственные стандарты

- основываются на современных достижениях науки, техники, международных и межгосударственных (региональных) стандартах, правилах, нормах и рекомендациях по стандартизации, прогрессивных стандартах других государств, за исключением случаев, когда такие документы могут быть непригодными или неэффективными для обеспечения:
- национальной безопасности;
- защиты жизни, здоровья и наследственности человека;
- охраны окружающей среды, рационального использования природных ресурсов и энергосбережения;
- предупреждения действий, вводящих в заблуждение потребителей продукции и услуг относительно их назначения, качества или безопасности.

Стандартизация в области ИБ

Государственные стандарты в зависимости от объекта стандартизации содержат:

- требования к продукции, процессам ее разработки, производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации или оказанию услуг;
- требования к правилам приемки и методикам контроля продукции;
- требования к технической и информационной совместимости;
- правила оформления технической документации;
- общие правила обеспечения качества продукции (услуг), сохранения и рационального использования ресурсов;
- требования к энергоэффективности и снижению энерго- и материалоемкости продукции, процессов ее производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации или оказания услуг;
- термины и определения, условные обозначения, метрологические и другие общие технические и организационно-методические правила и нормы.

Стандартизация в области ИБ

Технические кодексы установившейся практики

- ТКП 114–2008 (07040) "Банковские технологии. Оценка соответствия программных средств. Порядок оценки соответствия специальным требованиям"
- ТКП 115–2008 (07040) "Банковские технологии. Оценка соответствия программных средств. Порядок оценки соответствия общим требованиям"
- ТКП 133-2008 (07040) Банковские технологии. Порядок создания электронных платежных документов, используемых в Республиканской централизованной системе обмена межбанковской корреспонденцией в форме электронных документов. Часть 1. Сообщение МТ 104
- ТКП 135-2008 (07040) Банковские технологии. Порядок применения СТБ ИСО/МЭК 14764-2003 в процессе оценки сопровождения программных средств

Стандартизация в области ИБ

Стандарты Республики Беларусь

- СТБ 1176.1-99 Информационная технология. Защита информации. Функция хэширования.
- СТБ 1176.2-99 Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи

Стандартизация в области ИБ

- ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
- ГОСТ 31078-2002 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

Стандартизация в области ИБ

- СТБ 34.101.1-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
- СТБ 34.101.2-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
- СТБ 34.101.3-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3: Гарантийные требования безопасности.

Стандартизация в области ИБ

- СТБ 34.101.8-2006 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования.
- СТБ 34.101.9-2004 Информационные технологии. Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы.
- СТБ 34.101.10-2004 Информационные технологии. Средства защиты информации от несанкционированного доступа в автоматизированных системах. Общие требования.
- СТБ 34.101.11-2009 Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в доверенной зоне корпоративной сети.
- СТБ 34.101.12-2007 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Оценка качества.
- СТБ 34.101.13-2009 Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в демилитаризованной зоне корпоративной сети.