Лекция

Нормативно правовые документы и стандарты в области защиты информации и информационной безопасности

- ФЗ №149 «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»
- ФЗ №152 «О ПЕРСОНАЛЬНЫХ ДАННЫХ»
- ФЗ №258 «ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ»

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН №149-ФЗ, 27 июля 2006г.
ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:

1) **информация** - сведения (сообщения, данные) независимо от формы их представления;

2) **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) **информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) **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;

6) **доступ к информации** - возможность получения информации и ее использования;

7) **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Статья 5. Информация как объект правовых отношений

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;
2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Статья 9. Ограничение доступа к информации

1. 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.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

5. 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.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН №152-ФЗ, 27 июля 2006г.
О ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 1. Сфера действия настоящего Федерального закона

1. 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, не входящими в систему органов местного самоуправления муниципальными органами (далее - муниципальные органы), юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Статья 2. Цель настоящего Федерального закона

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

В целях настоящего Федерального закона используются следующие основные понятия:

1) **персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

2) **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;
3) **обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
4) **распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

5) **использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

6) **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

7) **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН №1-ФЗ, 1- января 2002г.
ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

(в ред. Федерального закона от 08.11.2007 N 258-ФЗ)

Глава I. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Цель и сфера применения настоящего Федерального закона

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.

2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях.
Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:
электронный документ - документ, в котором информация представлена в электронно-цифровой форме;

электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

сертификат средств электронной цифровой подписи
закрытый ключ электронной цифровой подписи
открытый ключ электронной цифровой подписи
сертификат ключа подписи
подтверждение подлинности электронной цифровой подписи в электронном документе
пользователь сертификата ключа подписи
корпоративная информационная система

Глава II. УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Статья 4. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи

1. 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.

2. Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

Глава III. УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ

Статья 8. Статус удостоверяющего центра

1. Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные настоящим Федеральным законом. При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, определяются Правительством Российской Федерации по представлению уполномоченного федерального органа исполнительной власти.

Статус удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, определяется ее владельцем или соглашением участников этой системы.

Стандарты в области информационной безопасности

ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р ИСО/МЭК 15408-1-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

Стандарты в области информационной безопасности (часть 2)

ГОСТ Р ИСО/МЭК 15408-3-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

Стандарты в области защиты информации

ГОСТ Р 52069.0-2003 Защита информации. Система стандартов. Основные положения.

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования

Р 50.1.056-2005 Техническая защита информации. Основные термины и определения

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ГОСТ Р ИСО/МЭК 27001—2006, 2008 – 02 – 01

1 Область применения

1.1 Общие положения

Настоящий стандарт предназначен для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими организациями). Настоящий стандарт устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности (СМИБ) среди общих бизнес-рисков организации. Кроме этого, стандарт устанавливает требования по внедрению мер управления информационной безопасностью и ее контроля, которые могут быть использованы организациями или их подразделениями в соответствии с установленными целями и задачами обеспечения информационной безопасности (ИБ).

Целью построения СМИБ является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

Примечание — Термин «бизнес», в настоящем стандарте понимаемый в широком смысле, обозначает всю ту деятельность, которая является основой для целей существования организации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующий стандарт: ИСО/МЭК 17799:2005 Информационная технология. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **активы** (asset): Все, что имеет ценность для организации. [ИСО/МЭК 13335-1:2004] [4]

3.2 **доступность** (availability): Свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта. [ИСО/МЭК 13335-1:2004] [4]

3.3 **конфиденциальность** (confidentiality): Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса. [ИСО/МЭК 13335-1:2004] [4]

3.4 **информационная безопасность;** ИБ (information security): Свойство информации сохранять конфиденциальность, целостность и доступность.

Примечание - Кроме того, данное понятие может включать в себя также и свойство сохранять аутентичность, подотчетность, неотказуемость и надежность. [ИСО/МЭК 17799:2005]

3.5 **событие информационной безопасности** (information security event): Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью. [ИСО/МЭК ТО 18044:2004] [5]

3.6 **инцидент информационной безопасности** (information security incident): Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечание - Инцидентами информационной безопасности являются: утрата услуг, оборудования или устройств; системные сбои или перегрузки; ошибки пользователей; несоблюдение политики или рекомендаций по ИБ; нарушение физических мер защиты; неконтролируемые изменения систем; сбои программного обеспечения и отказы технических средств; нарушение правил доступа. [ИСО/МЭК ТО 18044:2004] [5]

3.7 **система менеджмента информационной безопасности; СМИБ** (information security management system; ISMS): Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Примечание - Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы.

3.8 **целостность** (integrity): Свойство сохранять правильность и полноту активов. [ИСО/МЭК 13335-1:2004] [4]

3.9 **остаточный риск** (residual risk): Риск, остающийся после его обработки. [Руководство ИСО/МЭК 73:2002] [6]

3.10 **принятие риска** (risk acceptance): Решение по принятию риска. [Руководство ИСО/МЭК 73:2002] [6]

3.11 **анализ риска** (risk analysis): Систематическое использование информации для определения источников риска и количественной оценки риска. [Руководство ИСО/МЭК 73:2002] [6]

3.12 **оценка риска** (risk assessment): Общий процесс анализа риска и его оценивания. [Руководство ИСО/МЭК 73:2002] [6]

3.13 **оценивание риска** (risk evaluation): Процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости. [Руководство ИСО/МЭК 73:2002] [6]

3.14 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в отношении риска.

Примечание - Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникацию риска.

[Руководство ИСО/МЭК 73:2002] [6]

3.15 **обработка риска** (risk treatment): Процесс выбора и осуществления мер по модификации риска. [Руководство ИСО/МЭК 73:2002] [6]

Примечания

Меры по обработке риска могут включать в себя избежание, оптимизацию, перенос или сохранение риска.

В настоящем стандарте термин «мера управления» (control) использован как синоним термина «мера» (measure).

3.16 **положение о применимости** (statement of applicability): Документированное предписание, определяющее цели и меры управления, соответствующие и применимые к системе менеджмента информационной безопасности организации.

Примечание - Цели и меры управления основываются на результатах и выводах процессов оценки и обработки рисков, на требованиях законодательных или нормативных актов, на обязательствах по контракту и бизнес-требованиях организации по отношению к информационной безопасности.

4 Система менеджмента информационной безопасности

4.1 Общие требования

Организация должна разработать, внедрить, обеспечить функционирование, вести мониторинг, анализировать, поддерживать и непрерывно улучшать документированную СМИБ применительно ко всей деловой деятельности организации и рискам, с которыми она сталкивается. С учетом целей настоящего стандарта используемый процесс основан на применении модели PDCA, приведенной на рисунке 1.