Лекция 4. Юридические аспекты защиты информации

Цель лекции: Ознакомить студентов с юридическими аспектами защиты информации. Рассмотреть законодательные акты и нормативно-распорядительные документы. Ознакомить со стандартами защиты ИБ ISO/IEC 27000

План лекции:

1. Юридические аспекты защиты информации
2. Законодательные акты и нормативно-распорядительные документы
3. Стандарты защиты ИБ ISO/IEC 27000

Технико-математические аспекты правового обеспечения представляют совокупность технических средств, математических методов, моделей, алгоритмов и программ, обеспечивающих условия, необходимые для юридического разграничения прав и ответственности относительно регламентов обращения с защищаемой информацией.

При этом основными условиями являются:

1) фиксация на документе персональных идентификаторов («подписей») лиц, изготовивших документ и (или) несущих ответственность за него;

2) фиксация (при любой необходимости) на документе персональных идентификаторов (подписей) лиц, ознакомившихся с содержанием соответствующей информации;

3) фиксация фактов несанкционированного доступа с любой целью к конфиденциальной информации и средствам ее защиты;

4) невозможность незаметного (без оставления следов) изменения содержания информации даже лицами, имеющими к нему санкции на доступ;

5) применение криптографических методов и специальных средств защиты, что позволяет ограничить круг лиц, производящих обработку конфиденциальной информации.

Реализация рассмотренных технико-математических средств защиты информации также требует правового обеспечения. Решение этой задачи осуществляется в рамках существующего информационного законодательства.

В базовых законах определены понятия, объекты, цели и правовые основы защиты информации и информационных ресурсов. Нормативная база является необходимым условием обеспечения информационной безопасности.

Концепция информационной безопасности Республики Казахстан (далее - Концепция) разработана на основании Конституции Республики Казахстан и законов Республики Казахстан от 26 июня 1998 года " О

национальной безопасности Республики Казахстан", от 15 марта 1999 года " О государственных секретах ", от 13 июля 1999 года " О борьбе с терроризмом ", от 7 января 2003 года " Об электронном документе и электронной цифровой подписи", от 8 мая 2003 года "Об информатизации" и от 18 февраля 2005 года " О противодействии экстремизму ", Концепции развития конкурентоспособности информационного пространства Республики Казахстан на 2006 - 2009 годы, одобренной Указом Президента Республики Казахстан от 18 августа 2006 года N 163.

Концепция служит основой при определении, формировании, проведении и реализации единой государственной политики Республики Казахстан в области обеспечения информационной безопасности, ее положения будут учитываться при формировании государственной политики информатизации, защиты государственных информационных систем и государственных информационных ресурсов, создания и развития единого информационого пространства Казахстана.

Государственная политика обеспечения информационной безопасности Республики Казахстан (далее - Государственная политика) является открытой предусматривает информированность общества о деятельности государственных органов и общественных институтов в области информационной безопасности с учетом ограничений, предусмотренных действующим законодательством. Она основывается на обеспечении прав физических и юридических лиц на свободное создание, поиск, получение и распространение информации любым законным способом.

Состояние информационной безопасности Республики Казахстан

Происходящие в настоящее время процессы преобразования в политической жизни и экономике Казахстана оказывают непосредственное влияние на состояние его информационной безопасности. При этом возникают новые факторы, которые необходимо учитывать при оценке реального состояния информационной безопасности и определении ключевых проблем и направлений в этой области.
Указанные факторы можно разделить на:

- политические,
- экономические и
- организационно-технические.

Политическими факторами являются:

- изменение геополитической обстановки в различных регионах мира;
- информационная экспансия развитых стран мира, осуществляющих глобальный мониторинг мировых политических, экономических, военных,

экологических и других процессов, распространяющих информацию в целях получения односторонних преимуществ;

• становление новой казахстанской государственности на основе принципов демократии, законности, информационной открытости, совершенствования системы обеспечения безопасности страны;

• внутриполитические кризисы: конфликты ветвей власти, субъектов территориального государственного устройства, перевороты, покушения на охраняемые лица;

• деятельность внутриполитических блоков, союзов, альянсов, создание новых военно-политических объединений, влияющих на геополитическую расстановку сил в мире;

• стремление Казахстана к более тесному сотрудничеству с зарубежными странами в процессе проведения реформ;

• терроризм и экстремизм, обострение криминогенной обстановки, рост числа компьютерных преступлений, особенно, в кредитно-финансовой сфере.

Среди экономических факторов наиболее существенными являются:

• активная интеграция Казахстана в мировое экономическое пространство, появление множества отечественных и зарубежных коммерческих структур-производителей и потребителей информации, средств информатизации и защиты информации, включение информационной продукции в систему товарных отношений;

• расширяющаяся кооперация с зарубежными странами в интересах развития информационной инфраструктуры Казахстана;

• коммуникационная глобализация, оказывающая растущее воздействие на развитие экономических процессов во всем мире;

• отставание Казахстана в развитии и внедрении новейших информационных технологий, которые во все большей степени определяют уровень экономико-технологического развития в современном мире.

Из организационно-технических факторов определяющими являются:

• недостаточная нормативная правовая база в сфере информационных отношений, в том числе в области обеспечения информационной безопасности;

• слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг в Казахстане;

• широкое использование в сфере государственного управления, кредитно-финансовой и других сферах незащищенных от утечки информации и внешнего воздействия импортных технических и программных средств для хранения, обработки, передачи и защиты информации;

• рост объемов информации, передаваемой по открытым каналам связи и системам передачи данных.

Цели и задачи обеспечения информационной безопасности

Основными целями обеспечения информационной безопасности являются:

- создание и укрепление национальной системы защиты информации, в том числе в государственных информационных ресурсах;
- защита государственных информационных ресурсов, а также прав человека и интересов общества в информационной сфере;
- снижение или недопущение информационной зависимости Казахстана, информационной экспансии или блокады со стороны других государств, информационной изоляции Президента, Парламента, Правительства и других государственных органов и организаций.

Основными задачами по обеспечению информационной безопасности Республики Казахстан являются:

- совершенствование национального законодательства в области информационной безопасности;
- выявление, оценка, прогнозирование источников угроз информационной безопасности, определение параметров разведдоступности защищаемых объектов;
- разработка государственной политики обеспечения информационной безопасности, комплекса мероприятий и методов ее реализации;
- правовое регулирование и координация деятельности государственных органов и организаций в области обеспечения информацией безопасности;
- развитие системы обеспечения информационной безопасности, совершенствование ее организации, форм, методов и средств нейтрализации угроз информационной безопасности, ликвидации последствий ее нарушений;
- обеспечение активного участия Казахстана в процессах создания использования глобальных информационных сетей и систем;
- создание системы противодействия техническим разведкам путем разработки и совершенствования нормативной правовой и методологической базы по противодействию техническим разведкам.

ЗАКОНОДАТЕЛЬСТВО

- Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК. Об информатизации

- Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 О Концепции информационной безопасности Республики Казахстан до 2016 года
- Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407. Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")

КОНЦЕПЦИЯ кибербезопасности ("Киберщит Казахстана")

Концепция кибербезопасности ("Киберщит Казахстана") (далее – Концепция) разработана в соответствии с Посланием Президента Республики Казахстан "Третья модернизация Казахстана: Глобальная конкурентоспособность" с учетом подходов Стратегии "Казахстан-2050" по вхождению Казахстана в число 30-ти самых развитых государств мира.

Концепция основана на оценке текущей ситуации в сфере информатизации государственных органов, автоматизации государственных услуг, перспектив развития "цифровой" экономики и технологической модернизации производственных процессов в промышленности, расширения сферы оказания информационно-коммуникационных услуг.

Концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий.

Концепция призвана обеспечить единство подходов к мониторингу обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения.

Стандарты защиты ИБ ISO/IEC 27000

ISO/IEC 27000 — серия международных стандартов, включающая стандарты по информационной безопасности опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC).

Серия содержит лучшие практики и рекомендации в области информационной безопасности для создания, развития и поддержания Системы Менеджмента Информационной Безопасности.

Рисунок 1. Основные стандарты ИСО для построения СУИБ

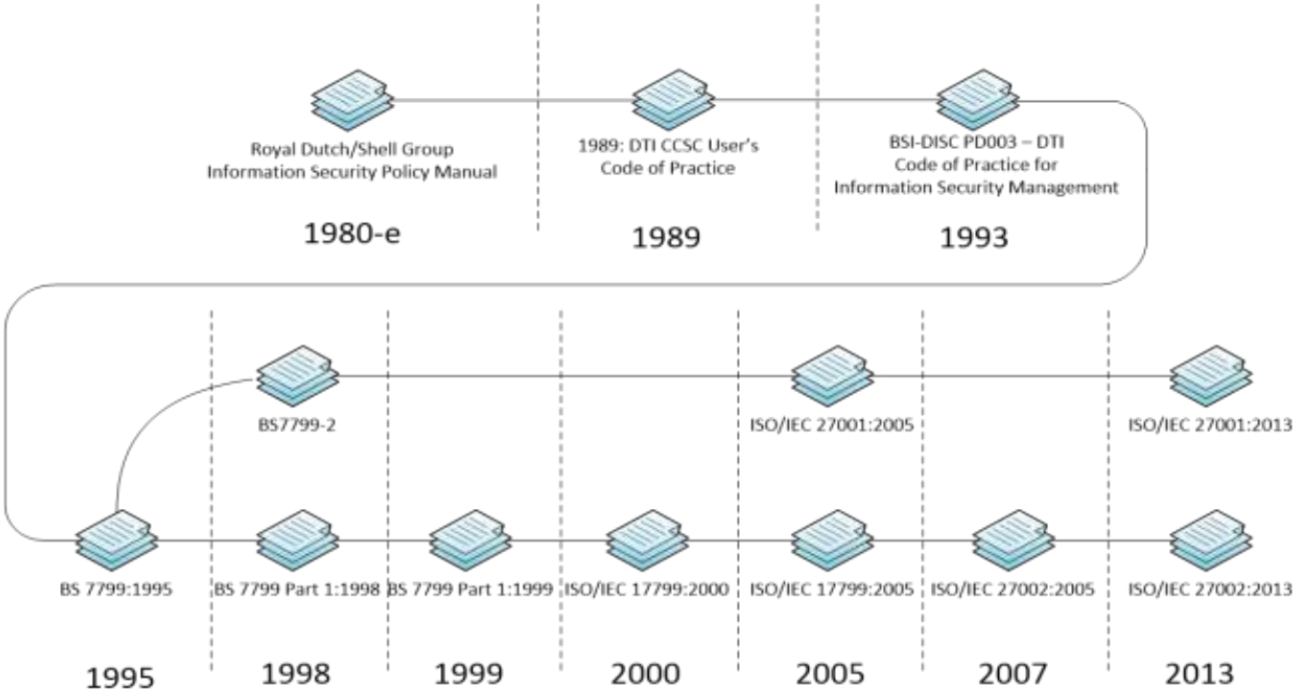

Рисунок 2 Хронология развития стандарта ISO/IEC 27001

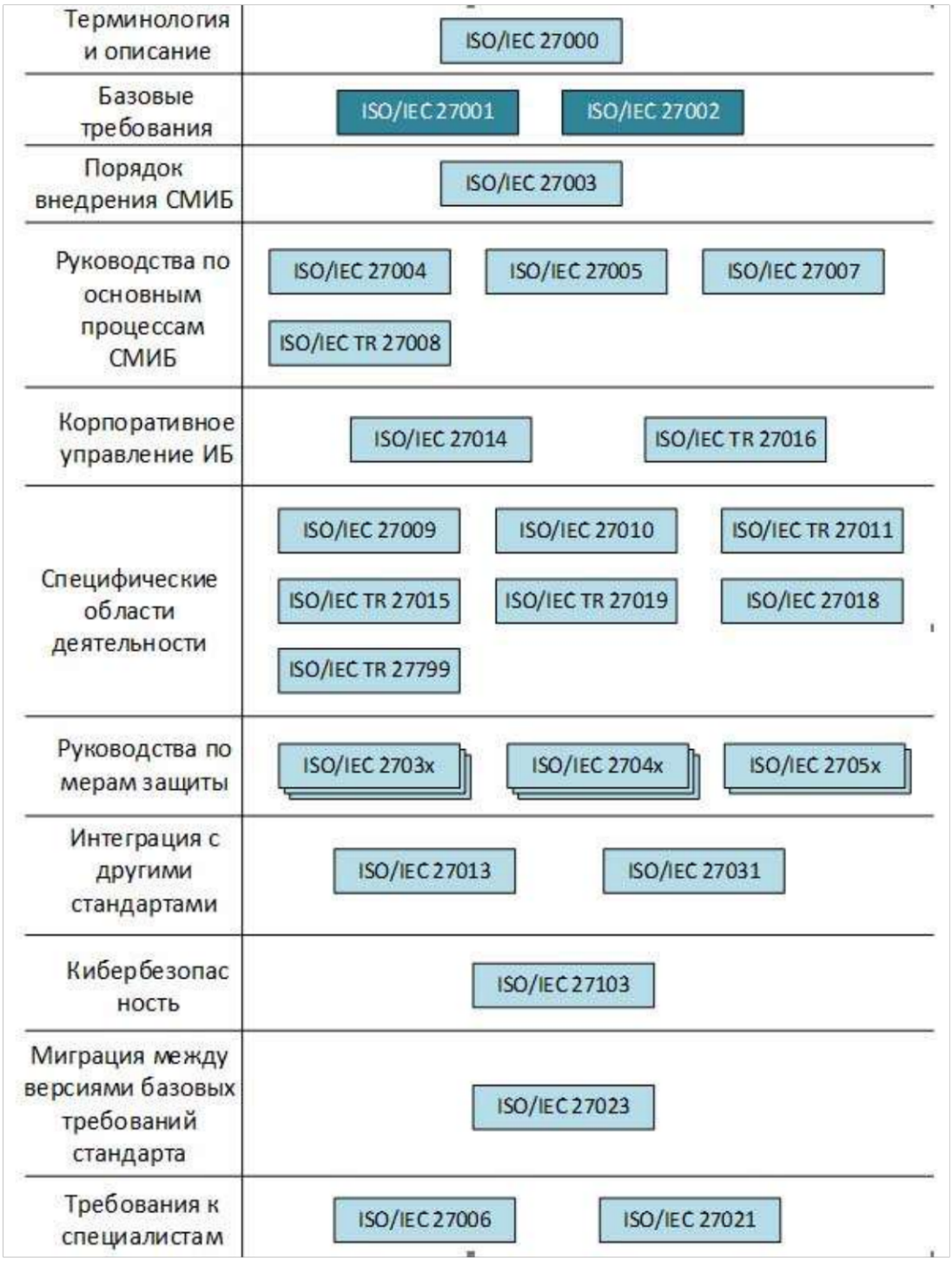

Рисунок 3 Группировка стандартов серии 27xxx

Принятые стандарты:

- Серия стандартов ИСО 27000 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности…» (далее — «СМИБ»): ГОСТ Р ИСО/МЭК 27000-2012 — «СМИБ. Общий обзор и терминология»

- ГОСТ Р ИСО/МЭК 27001-2006 — «СМИБ.Требования» (Опубликован в 2005)
- ГОСТ Р ИСО/МЭК 27002-2012 — «СМИБ. Свод норм и правил менеджмента информационной безопасности»
- ГОСТ Р ИСО/МЭК 27003-2012 —"СМИБ. Руководство по реализации системы менеджмента информационной безопасности" (Опубликован в январе 2010)
- ГОСТ Р ИСО/МЭК 27004-2011— «СМИБ. Измерения» (Опубликован в январе 2010)
- ГОСТ Р ИСО/МЭК 27005-2010 — «СМИБ. Менеджмент риска информационной безопасности» На основе BS7799-3 (опубликовано в 2008)
- ГОСТ Р ИСО/МЭК 27006-2020 — «СМИБ. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности» (дата введения: 01.07.2021)
- ГОСТ Р ИСО/МЭК 27007-2014 — «СМИБ. Руководства по аудиту систем менеджмента информационной безопасности»

Базовые стандарты ISO/IEC 27001 и ISO/IEC 27002 со временем были дополнены следующими документами:

• стандартом ISO/IEC 27000, описывающим терминологию и общий подход всей серии стандартов;

• стандартом ISO/IEC 27003 с указаниями по порядку внедрения СМИБ;

• стандартами по отдельным процессам СМИБ: измерению эффективности, риск-менеджменту, аудиту;

• стандартами по направлениям стратегического управления ИБ и экономике СМИБ;

• стандартами по особенностям СМИБ в специфических областях деятельности: телекоммуникационных услугах, финансовых операциях, обработке персональных данных в облачных сервисах, топливно-энергетическом комплексе, сообществах информационного обмена, организациях здравоохранения;

• детальными требованиями к мерам защиты информации, в том числе по управлению инцидентами, сетевой безопасности;

• руководствами по интеграции СМИБ с системами ИТ-менеджмента (ISO 20000) и системами обеспечения непрерывности деятельности (в том числе ISO 22301);

• руководством по обеспечению кибербезопасности в соответствии с общим подходом и практиками СМИБ;

- стандартами ISO/IEC 27006 и ISO/IEC 27021, описывающим требования к экспертам и аудиторам СМИБ.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.
2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.
3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.
4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582
5. Организационная безопасность на предприятии: бумажная и практическая безопасность. inforsec.ru. Дата обращения: 13 сентября 2021.
6.Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК. Об информатизации https://adilet.zan.kz/rus/docs/Z1500000418
7.Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 О Концепции информационной безопасности Республики Казахстан до 2016 года https://adilet.zan.kz/rus/docs/U1100000174
8.Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407. Об утверждении Концепции кибербезопасности ("Киберщит Казахстана") https://adilet.zan.kz/rus/docs/P1700000407