**1. Государственное регулирование в сфере защиты информации**

Правовое обеспечение включает в себя:

1. Нормотворческую деятельность по созданию законодательства, регулирующего общественные отношения в области защиты информации.

2. Исполнительную и правоприменительную деятельность по исполнению законодательства в области информации, информатизации, защиты информации органами государственной власти и управления организациями (юридическими лицами), гражданами.

Нормотворческая деятельность:

1. Оценка состояния действующего законодательства и разработка программы его совершенствования.

2. Создание организационно‑правовых механизмов обеспечения защиты информации.

3. Формирование правового статуса всех субъектов в системе защиты информации и определение их ответственности за обеспечение информационной безопасности.

4. Разработку организационно‑правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях с учетом всех категорий информации.

5. Разработку законодательных и других нормативных актов, регулирующих порядок ликвидации последствий воздействий угроз, восстановление права и ресурсов, реализации компенсационных мер.

Исполнительная и правоприменительная деятельность:

1. Разработка процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией.

2. Разработка составов правонарушений с учетом специфики уголовной, гражданской, административной и дисциплинарной ответственности.

Деятельность по правовому обеспечению информационной безопасности строится на трех фундаментальных положениях:

1. Соблюдение законности (предполагает наличие законов и иных нормативных документов, их применение и исполнение субъектами права в области информационной безопасности).

2. Обеспечение баланса интересов отдельных субъектов и государства (предусматривает приоритет государственных интересов как общих интересов всех субъектов). Ориентация на свободы, права и интересы граждан не принижает роль государства в обеспечении национальной безопасности в целом и в области информационной безопасности в частности).

3. Неотвратимость наказания (выполняет роль важнейшего профилактического инструмента в решении вопросов правового обеспечения).

Нормативно-правовая база в области защиты информации основывается на общегосударственных документах и ведомственных документах.

Общегосударственные документы:

1) Законы, кодексы;

2) Указы Президента Республики Беларусь;

3) Постановления Совета Министров.

Ведомственные документы:

1) межведомственные;

2) внутриведомственные.

Основные правовые акты, регламентирующие защиту информации в Республике Беларусь:

Концепция национальной безопасности Республики Беларусь (9 ноября 2010 г.) представляет собой совокупность официальных взглядов на сущность и содержание деятельности Республики Беларусь по обеспечению баланса интересов личности, общества, государства и их защите от внутренних и внешних угроз и обеспечивает единство подходов к формированию и реализации государственной политики обеспечения национальной безопасности, а также методологическую основу совершенствования актов законодательства в различных сферах национальной безопасности, разработки документов стратегического планирования.

Закон Республики Беларусь «Об информации, информатизации и защите информации» (9 октября 2008 г.) является основой для регулирования общественных отношений, возникающих при:

– поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией;

– создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов;

– организации и обеспечении защиты информации.

Постановление Совета Министров Республики Беларусь «О некоторых вопросах защиты информации» (26 мая 2009 г.) регламентирует порядок:

– защиты информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено;

– аттестации систем защиты информации;

– проведения государственной экспертизы средств защиты информации.

Постановление Совета Министров Республики Беларусь «Об утверждении положения о лицензировании деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи» (20 октября 2003 г.) устанавливает порядок выдачи специальных разрешений (лицензий) на осуществление деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи.

Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи» (28 декабря 2009 г.) определяет правовые основы применения электронных документов, определяет основные требования, предъявляемые к электронным документам, а также правовые условия 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.

В последнее время в разных странах появилось новое поколение стандартов в области защиты информации, посвященных практическим вопросам управления информационной безопасности компании. Это прежде всего международные и национальные стандарты управления информационной безопасностью ISO 15408, ISO 17799 (BS7799), BSI; стандарты аудита информационных систем и информационной безопасности COBIT, SAC, COSO, SAS 78/94 и некоторые другие, аналогичные им.

В соответствие с международными и национальными стандартами ISO 15408, ISO 17799 (BS7799), BSI; COBIT, SAC, COSO, SAS 78/94 обеспечение информационной безопасности в любой компании предполагает следующее. Во-первых, определение целей обеспечения информационной безопасности компьютерных систем. Во-вторых, создание эффективной системы управления информационной безопасностью. В третьих, расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям. В четвертых, применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния. В пятых, использование методик управления безопасностью с обоснованной системой метрик и мер обеспечения информационной безопасности, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Рассмотрим наиболее известные международные стандарты в области защиты информации.

**Международный стандарт ISO 15408**

Следуя по пути интеграции, в 1990 г. Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (ТЕС) составили специализированную систему мировой стандартизации, a ISO начала создавать международные стандарты по критериям оценки безопасности информационных технологий для общего использования, названные Common Criteria for Information Technology Security Evaluation или просто Common Criteria. В их разработке участвовали: Национальный институт стандартов и технологии и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Нидерланды), Органы исполнения программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция).

В дальнейшем "Общие критерии" неоднократно редактировались. В результате 8 июня 1999 года был утвержден Международный стандарт ISO/IEC 15408 под названием "Общие критерии оценки безопасности информационных технологий" (ОК).

Общие критерии обобщили содержание и опыт использования Оранжевой книги, развили европейские и канадские критерии, и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США. В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства ОК — полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития.

Использование методик данного стандарта позволяет определить для компании те критерии, которые могут быть использованы в качестве основы для выработки оценок защитных свойств продуктов и систем информационной технологии. Кроме того, эти методики позволяют проводить наиболее полное сравнение результатов оценки защитных свойств корпоративных информационных систем с помощью общего перечня (набора) требований для функций защиты продуктов и систем, а также методов точных измерений, которые проводятся во время получения оценок защиты. Основываясь на этих требованиях, в процессе выработки оценки уровня защиты устанавливается уровень доверия.

Результаты оценок защиты позволяют определить для компании достаточность защиты корпоративной информационной системы.

Вместе с тем в ОК главное внимание уделено защите от несанкционированного доступа (НСД). Модификации или потери доступа к информации в результате случайных или преднамеренных действий и ряд других аспектов информационной безопасности остался не рассмотренным. Например, оценка административных мер безопасности, оценка безопасности от побочных электромагнитных излучений, методики оценки различных средств и мер безопасности, критерии для оценки криптографических методов защиты информации.

Поэтому необходимо дополнять данный подход рядом своих собственных апробированных методик оценки важнейших элементов защиты. Дополненные таким образом ОК можно использовать как при задании требований к продуктам и системам информационных технологий, так и при оценке их безопасности на всех этапах жизненного цикла корпоративной информационной системы.

**Стандарты ISO/IEC 17799:2002 (BS 7799:2000)**

Версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;

- основные понятия и определения информационной безопасности;

- политика информационной безопасности компании;

- организация информационной безопасности на предприятии;

- классификация и управление корпоративными информационными ресурсами;

- Кадровый менеджмент и информационная безопасность;

- физическая безопасность;

- администрирование безопасности корпоративных информационных систем;

- управление доступом;

- требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения;

- управление бизнес-процессами компании с точки зрения информационной безопасности;

- внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799-2:2000 "Спецификации систем управления информационной безопасностью - Information security management – Part 2: Specification for information security management systems”, определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

Дополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов - British Standards Institution(BSI) http://www.bsi-global.com/, изданные в период 1995-2003 в виде следующей серии:

1. Введение в проблему управления информационной безопасности -Information security managment: an introduction.

2. Возможности сертификации на требования стандарта BS 7799 -Preparing for BS 7799 sertification.

3. Руководство BS 7799 по оценке и управлению рисками -Guide to BS 7799 risk assessment and risk management.

4. Готовы ли вы к аудиту на требования стандарта BS 7799-Are you ready for a BS 7799 audit?

5. Руководство для проведения аудита на требования стандарта – BS 7799Guide to BS 7799 auditing.

6. Практические рекомендации по управлению безопасностью информационных технологий -Code of practice for IT management.