ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Санкт – Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

Отделение: Информационных технологий и управления в телекоммуникациях
Специальность: 09.02.03 «Программирование в компьютерных системах»

МДК.03.03 ДОКУМЕНТИРОВАНИЕ И СЕРТИФИКАЦИЯ
Раздел ПМ 3. Разработка программной документации

Преподаватель **Рожков А.И.**

Санкт-Петербург 2020

СПб ГУТ)))

ТЕМА 3.1. Документирование и сертификация

Лекция. Нормативно-правовые документы и стандарты в области защиты информации и информационной безопасности

План занятия:

1. Международные правовые и нормативные акты обеспечения информационной безопасности процессов переработки информации.
2. Отечественное организационное, правовое и нормативное обеспечение и регулирование в сфере информационной безопасности.

1. Международные правовые и нормативные акты обеспечения информационной безопасности процессов переработки информации.

Законодательные меры по защите процессов переработки информации заключаются в исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц - пользователей и обслуживающего технического персонала - за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также в ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

Цель законодательных мер - предупреждение и сдерживание потенциальных нарушителей.

Поскольку ИБ должна быть связующим звеном между политикой национальной безопасности и информационной политикой страны, то логично было бы проводить ее по единым принципам, выделяя их как общие и для информационной политики.

Таким образом государственная информационная политика должна опираться на следующие базовые принципы:

- открытость политики (все основные мероприятия информационной политики открыто обсуждаются обществом, государство учитывает общественное мнение);
- равенство интересов участников (политика в равной степени учитывает интересы всех участников информационной деятельности независимо от их положения в обществе, формы собственности и государственной принадлежности);
- системность (реализация процессов обеспечения ИБ через государственную систему);
- приоритетность отечественного производителя (при равных условиях приоритет отдается конкурентоспособному отечественному производителю информационно-коммуникационных средств, продуктов и услуг);

- социальная ориентация (основные мероприятия государственной информационной политики должны быть направлены на обеспечение социальных интересов граждан России);
- государственная поддержка (мероприятия информационной политики, направленные на информационное развитие социальной сферы, финансируются преимущественно государством);
- приоритетность права - законность (развитие и применение правовых и экономических методов имеет приоритет перед любыми формами административных решений проблем информационной сферы);
- сочетание централизованного управления силами и средствами обеспечения безопасности с передачей в соответствии с федеральным устройством России части полномочий в этой области органам государственной власти субъектов Российской Федерации и органам местного самоуправления;
- интеграция с международными системами обеспечения ИБ.

В международной практике обеспечения ИБ основными направлениями являются:

- нормирование компьютерной безопасности по критериям оценки защищенности надежных систем и информационных технологий;
- стандартизация процессов создания безопасных информационных систем.

Еще в 1983 г. Агентство компьютерной безопасности Министерства обороны США опубликовало отчет, названный TCSEC ("**Критерии оценки защищенности надежных систем**"), или "**Оранжевую книгу**" (по цвету переплета), в которой были определены семь уровней безопасности (A1 - гарантированная защита; B1, B2, B3 - полное управление доступом; C1, C2 - избирательное управление доступом, D - минимальная безопасность) для оценки защиты грифованных данных в многопользовательских компьютерных системах.

Для оценки компьютерных систем Министерства обороны США Национальный центр компьютерной безопасности МО США выпустил инструкции NCSC-TG-005 и NCSC-TG-011, известные как "**Красная книга**" (по цвету переплета).

В свою очередь, Агентство информационной безопасности ФРГ подготовило GREEN BOOK ("Зеленая книга"), в которой рассмотрены в комплексе требования к доступности, целостности и конфиденциальности информации как в государственном, так и в частном секторе.

В 1990 г. "Зеленая книга" была одобрена ФРГ, Великобританией, Францией и Голландией и направлена в Европейский Союз (ЕС), где на ее основе были подготовлены ITSEC ("Критерии оценки защищенности информационных технологий"), или "Белая книга", как европейский стандарт, определяющий критерии, требования и процедуры для создания безопасных информационных систем и имеющий две схемы оценки: по эффективности (от Е1 до Е6) и по функциональности (доступность, целостность системы, целостность данных, конфиденциальность информации и передачи данных).

В "Белой книге" названы основные компоненты безопасности по критериям ITSEC:

1) информационная безопасность;

2) безопасность системы;

3) безопасность продукта;

4) угроза безопасности;

5) набор функций безопасности;

6) гарантированность безопасности;

7) общая оценка безопасности;

8) классы безопасности.

Согласно европейским критериям ITSEC, ИБ включает в себя шесть основных элементов ее детализации:

1) цели безопасности и функции ИБ;

2) спецификация функций безопасности:

- идентификация и аутентификация (понимается не только традиционная проверка подлинности пользователя, но и функции для регистрации новых пользователей и удаления старых, а также функции для изменения и проверки аутентификационной информации, в том числе контроля целостности и функции для ограничения количества повторных попыток аутентификации);

- управление доступом (в том числе функции безопасности, которые обеспечивают временное ограничение доступа к совместно используемым объектам с целью поддержания целостности этих объектов; управление распространением прав доступа; контроль за получением информации путем логического вывода и агрегирования данных);
- подотчетность (протоколирование);
- аудит (независимый контроль);
- повторное использование объектов;
- точность информации (поддержка определенного соответствия между разными частями данных (точность связей) и обеспечение неизменности данных при передаче между процессами (точность коммуникации));

- надежность обслуживания (функции обеспечения, когда действия, критичные по времени, будут выполнены именно тогда, когда нужно; некритичные действия нельзя перенести в разряд критичных; авторизованные пользователи за разумное время получат запрашиваемые ресурсы; функции обнаружения и нейтрализации ошибок; функции планирования для обеспечения коммуникационной безопасности, т.е. безопасности данных, передаваемых по каналам связи);
- обмен данными;

3) конфиденциальность информации (защита от несанкционированного получения информации);

4) целостность информации (защита от несанкционированного изменения информации);

5) доступность информации (защита от несанкционированного или случайного удержания информации и ресурсов системы);

6) описание механизмов безопасности.

Для реализации функций идентификации и аутентификации могут использоваться такие механизмы, как специальный сервер KERBEROS (сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищенной среде, а передаваемые пакеты могут быть перехвачены и модифицированы. Протокол Kerberos решает проблему передачи пароля средствами криптографии с секретным ключом), а для защиты компьютерных сетей - фильтрующие маршрутизаторы, сетевые анализаторы протоколов (экраны) типа FireWall, пакеты фильтрующих программ и т.д.

Общая оценка безопасности системы по ITSEC состоит из двух компонентов: оценка уровня гарантированной эффективности механизмов (средств) безопасности и оценка уровня их гарантированной корректности. Безопасность системы в целом оценивается отдельно для систем и продуктов. Защищенность их не может быть выше мощности самого слабого из критически важных механизмов безопасности (средств защиты).

При проверке эффективности анализируется соответствие между задачами безопасности по конфиденциальности, целостности, доступности информации и реализованным набором функций безопасности - их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками слабых мест защиты. **Кроме того, в понятие "эффективность" включается и способность механизмов защиты противостоять прямым атакам, которая называется мощностью механизмов защиты.** По ITSEC декларируется три степени мощности: базовая, средняя и высокая. При проверке корректности анализируется правильность и надежность реализации функций безопасности. По ITSEC декларируется семь уровней корректности - от E0 до E6.

В "Европейских критериях" установлено 10 классов безопасности. F-DX предназначен для систем с повышенными требованиями одновременно по классам F-D1 и F-DC.

2. Отечественное организационное, правовое и нормативное обеспечение и регулирование в сфере информационной безопасности.

К основным задачам в сфере обеспечения и регулирования ИБ РФ относятся следующие:

- формирование и реализация единой государственной политики по обеспечению защиты национальных интересов от угроз в информационной сфере, реализация конституционных прав и свобод граждан на информационную деятельность;
- совершенствование законодательства Российской Федерации в сфере обеспечения ИБ;
- определение полномочий органов государственной власти Российской Федерации, субъектов Российской Федерации и органов местного самоуправления в сфере обеспечения ИБ;
- координация деятельности органов государственной власти по обеспечению ИБ;
- создание условий для успешного развития негосударственной компоненты в сфере обеспечения ИБ, осуществления эффективного гражданского контроля за деятельностью органов государственной власти;

- совершенствование и защита отечественной информационной инфраструктуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;
- развитие стандартизации информационных систем на базе общепризнанных международных стандартов и их внедрение во всех видах таких систем;
- развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти, на предприятиях оборонного комплекса;
- духовное возрождение России, обеспечение сохранности и защиты культурного и исторического наследия (в том числе музейных, архивных, библиотечных фондов, основных историко-культурных объектов);

- сохранение традиционных духовных ценностей при важнейшей роли Русской Православной церкви и церквей других конфессий;
- пропаганда средствами массовой информации элементов национальных культур народов России, духовно-нравственных, исторических традиций, норм общественной жизни и передового опыта подобной пропагандистской деятельности;
- повышение роли русского языка как государственного языка и языка межгосударственного общения народов России и государств членов Содружества Независимых государств (СНГ);
- создание оптимальных социально-экономических условий для осуществления важнейших видов творческой деятельности и функционирования учреждений культуры;
- противодействие угрозе развязывания противоборства в информационной сфере;
- организация международного сотрудничества по обеспечению ИБ при интеграции России в мировое информационное пространство.

Установление стандартов и нормативов в сфере обеспечения ИБ РФ является наиболее важной регулирующей функцией.

Комплексный характер защиты процессов переработки информации достигается за счет использования унифицированного алгоритмического обеспечения для средств криптографической защиты в соответствии с российскими государственными стандартами:

- ГОСТ 34.13-2018 "Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров "
- ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи";
- ГОСТ Р 34.11-2012 "Информационная технология. Криптографическая защита информации. Функция хэширования";
- ГОСТ Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования".

Немаловажное значения для формирования оптимальных схем государственного воздействия на информационные процессы имеет нормативно-правовое обеспечение данной сферы, включающее в себя в качестве одного из краеугольных камней систему лицензирования и сертификации информационных продуктов и услуг, информационных и телекоммуникационных систем, сетей связи и сопутствующих технологий.

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

- Акты федерального законодательства;
- Международные договоры РФ;
- Конституция РФ;
- Законы федерального уровня (включая федеральные конституционные законы, кодексы);
- Указы Президента РФ;
- Постановления правительства РФ;
- Нормативные правовые акты федеральных министерств и ведомств;
- Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

К нормативно-методическим документам можно отнести:

1. Методические документы государственных органов России:

   - Доктрина информационной безопасности РФ;
   - Руководящие документы ФСТЭК (Гостехкомиссии России);
   - Приказы ФСБ;

2. Стандарты информационной безопасности, из которых выделяют:

   - Международные стандарты;
   - Государственные (национальные) стандарты РФ;
   - Рекомендации по стандартизации;
   - Методические указания.

Органы (подразделения), обеспечивающие информационную безопасность.

В зависимости от приложения деятельности в области защиты информации (в рамках государственных органов власти или коммерческих организаций), сама деятельность организуется специальными государственными органами (подразделениями), либо отделами (службами) предприятия.

Государственные органы РФ, контролирующие деятельность в области защиты информации:

- Комитет Государственной думы по безопасности;
- Совет безопасности России;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК);
- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Министерство внутренних дел Российской Федерации (МВД России);

- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Службы, организующие защиту информации на уровне предприятия:

- Служба экономической безопасности;
- Служба безопасности персонала (Режимный отдел);
- Отдел кадров;
- Служба информационной безопасности.