ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Парфёнов Василий

ОПРЕДЕЛЕНИЕ

Информационная безопасность государства — состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.

В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

ОПРЕДЕЛЕНИЕ

Информационная безопасность — это процесс обеспечения конфиденциальности, целостности и доступности информации.

1) Конфиденциальность: Обеспечение доступа к информации только авторизованным пользователям.
2) Целостность: Обеспечение достоверности и полноты информации и методов ее обработки.
3) Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

ПРОГРАММНО-ТЕХНИЧЕСКИЕ СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

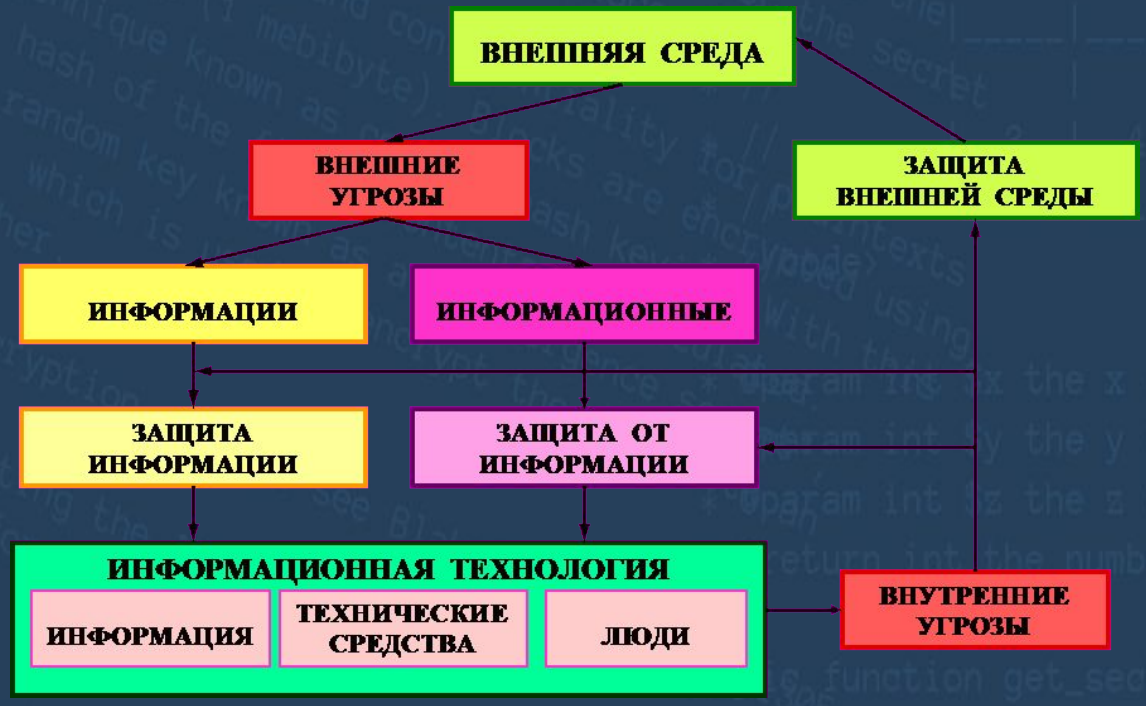
В литературе предлагается следующая классификация средств защиты информации.

Средства защиты от несанкционированного доступа (НСД):
Средства авторизации;
Мандатное управление доступом[11];
Избирательное управление доступом;
Управление доступом на основе ролей;
Журналирование (так же называется Аудит).
Системы анализа и моделирования информационных потоков (CASE-системы).
Системы мониторинга сетей:
Системы обнаружения и предотвращения вторжений (IDS/IPS).
Системы предотвращения утечек конфиденциальной информации (DLP-системы).
Анализаторы протоколов.
Антивирусные средства.
Межсетевые экраны.
Криптографические средства:
Шифрование;
Цифровая подпись.
Системы резервного копирования.
Системы бесперебойного питания:
Источники бесперебойного питания;
Резервирование нагрузки;
Генераторы напряжения.
Системы аутентификации:
Пароль;
Ключ доступа (физический или электронный);
Сертификат;
Биометрия.
Средства предотвращения взлома корпусов и краж оборудования.
Средства контроля доступа в помещения.
Инструментальные средства анализа систем защиты:
Антивирус.

ОРГАНИЗАЦИОННАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз. Организационная защита обеспечивает:

организацию охраны, режима, работу с кадрами, с документами;
использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.



ОРГАНИЗАЦИОННАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

К основным организационным мероприятиям можно отнести:

- организацию режима и охраны. Их цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц;
- организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учёт, исполнение, возврат, хранение и уничтожение;
- организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;
- организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
- организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учёта, хранения и уничтожения документов и технических носителей.
В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

ИСТОРИЧЕСКИЕ АСПЕКТЫ ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

I этап — до 1916 года — характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.

II этап — начиная с 1916 года — связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищённости радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

ИСТОРИЧЕСКИЕ АСПЕКТЫ ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

III этап — начиная с 1935 года — связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищённости радиолокационных средств от воздействия на их приёмные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.

IV этап — начиная с 1946 года — связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

ИСТОРИЧЕСКИЕ АСПЕКТЫ ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

V этап — начиная с 1965 года — обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

VI этап — начиная с 1973 года — связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьёзнее. Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.

ИСТОРИЧЕСКИЕ АСПЕКТЫ ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

VII этап — начиная с 1985 года — связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить, что очередной этап развития информационной безопасности, очевидно, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

СПАСИБО ЗА ВНИМАНИЕ!