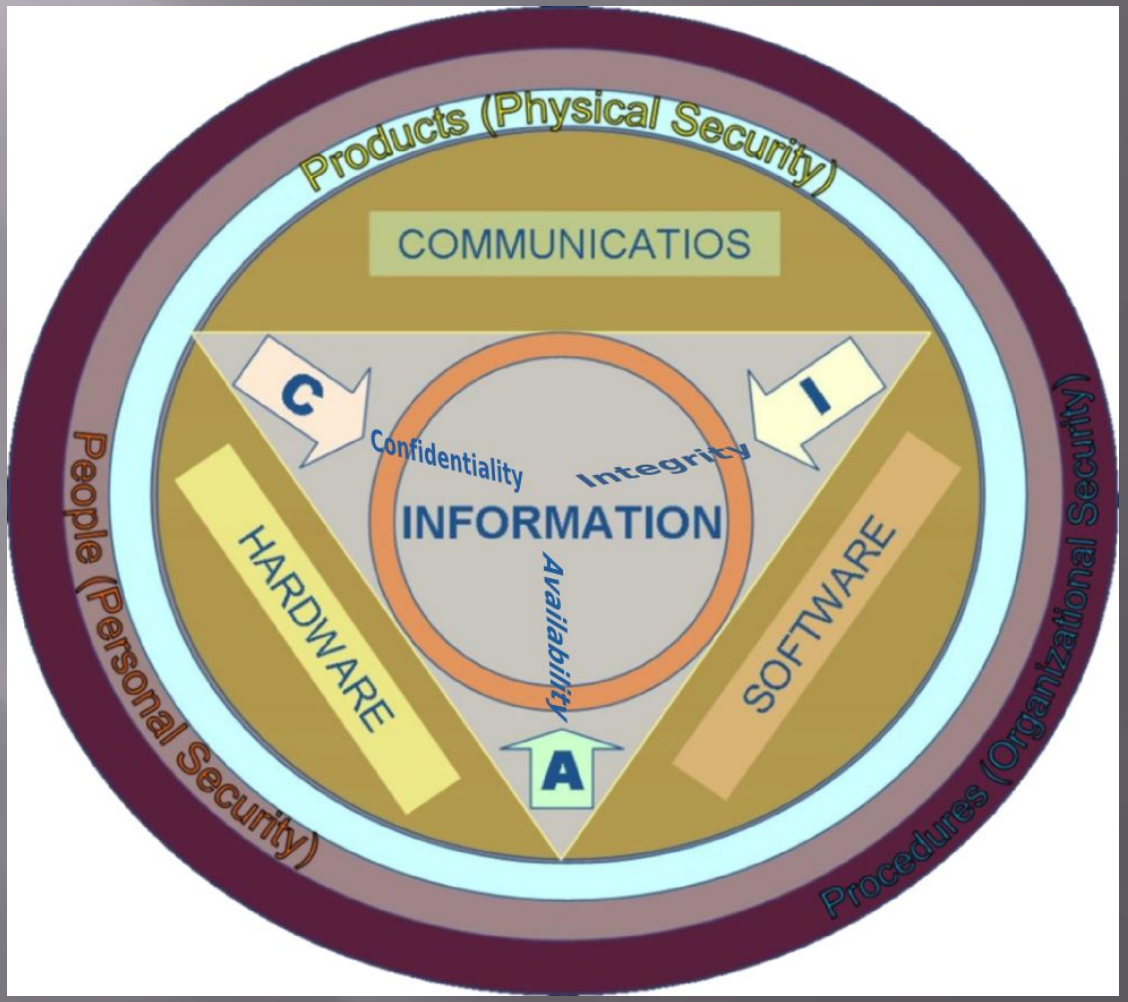
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выполнила: Краснова Ю.
Проверила: Силиверстова И. В.

Информационная безопасность может рассматриваться как:

- состояние (качество) определённого объекта (в качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства и т. п.)[1];
- деятельность, направленная на обеспечение защищённого состояния объекта (в этом значении чаще используется термин «защита информации»).[2]
- Кортеж защиты информации — это последовательность действий для достижения определённой цели.
- Информационная безопасность государства[3] — состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества виформационной сфере.
- В современном социуме информационная сфера имеет две составляющие[4]: информационно-техническую (искусственно созданный человеком мир техники, технологийи 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.

Информационная безопасность



Стандартизированные определения

Информационная безопасность[2] — это процесс обеспечения конфиденциальности, целостности и доступности информации.

Конфиденциальность: Обеспечение доступа к информации только авторизованным пользователям.

Целостность: Обеспечение достоверности и полноты информации и методов ее обработки.

Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Информационная безопасность (англ. *information security*)[5] — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.

Безопасность информации (данных) (англ. *information (data) security*)[6][1] — состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Безопасность информации (при применении информационных технологий) (англ. *IT security*)[6] — состояние защищённости информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

Безопасность автоматизированной информационной системы[6] — состояние защищённости автоматизированной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчётность и подлинность её ресурсов.

Информационная безопасность — защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Поддерживающая инфраструктура — системы электро-, тепло-, водо-, газоснабжения, системы кондиционирования и т. д., а также обслуживающий персонал. Неприемлемый ущерб — ущерб, которым

Информационная безопасность

СУЩЕСТВЕННЫЕ ПРИЗНАКИ ПОНЯТИЯ

- В качестве стандартной модели безопасности часто приводят модель из трёх категорий:
- конфиденциальность (англ. *confidentiality*)[6] — состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право;
- целостность (англ. *integrity*)[7] — избежание несанкционированной модификации информации;
- доступность (англ. *availability*)[8] — избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.
- Выделяют и другие не всегда обязательные категории модели безопасности:
- неотказуемость или апеллируемость (англ. *non-repudiation*)[5] — способность удостоверять имевшее место действие или событие так, что эти события или действия не могли быть позже отвергнуты;
- подотчётность (англ. *accountability*)[9] — обеспечение идентификации субъекта доступа и регистрации его действий;
- достоверность (англ. *reliability*)[5] — свойство соответствия предусмотренному поведению или результату;
- аутентичность или подлинность (англ. *authenticity*)[5] — свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ ТЕРМИНОВ

- В ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты» приводится следующая рекомендация использования терминов «безопасность» и «безопасный»:Для термина «информационная безопасность» следует придерживаться тех же рекомендаций. Желательно использовать более точные характеристики объектов, разделяемые как признаки понятия «информационная безопасность». Например, точнее будет использовать аргумент «для предотвращения угроз на доступность объекта» (или «для сохранения целостности данных») вместо аргумента «исходя из требований информационной безопасности».

Объём (реализация) понятия «информационная безопасность»

- Системный подход к описанию информационной безопасности предлагает выделить следующие составляющие информационной безопасности[10]:
- Законодательная, нормативно-правовая и научная база.
- Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
- Организационно-технические и режимные меры и методы (Политика информационной безопасности).
- Программно-технические способы и средства обеспечения информационной безопасности.
- Ниже в данном разделе подробно будет рассмотрена каждая из составляющих информационной безопасности.
- Целью реализации информационной безопасности какого-либо объекта является построение Системы обеспечения информационной безопасности данного объекта (СОИБ). Для построения и эффективной эксплуатации СОИБ необходимо[2]:
- выявить требования защиты информации, специфические для данного объекта защиты;
- учесть требования национального и международного Законодательства;
- использовать наработанные практики (стандарты, методологии) построения подобных СОИБ;
- определить подразделения, ответственные за реализацию и поддержку СОИБ;
- распределить между подразделениями области ответственности в осуществлении требований СОИБ;
- на базе управления рисками информационной безопасности определить общие положения, технические и организационные требования, составляющие Политику информационной безопасности объекта защиты;
- реализовать требования Политики информационной безопасности, внедрив соответствующие программно-технические способы и средства защиты информации;
- реализовать Систему менеджмента (управления) информационной безопасности (СМИБ);
- используя СМИБ организовать регулярный контроль эффективности СОИБ и при необходимости пересмотр и корректировку СОИБ и СМИБ.
- Как видно из последнего этапа работ, процесс реализации СОИБ непрерывный и циклично (после каждого пересмотра) возвращается к первому этапу, повторяя последовательно все остальные. Так СОИБ корректируется для эффективного выполнения своих задач защиты

Нормативные документы в области информационной безопасности

- В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся[11]:
- 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.
- Подробнее списки и содержание указанных нормативных документов в области информационной безопасности обсуждаются в разделе Информационное право.
- К нормативно-методическим документам можно отнести
- Методические документы государственных органов России:
  - Доктрина информационной безопасности РФ;
  - Руководящие документы ФСТЭК (Гостехкомиссии России);
  - Приказы ФСБ;
- 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 России);
- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Федеральная служба охраны Российской Федерации (ФСО России);
- Служба внешней разведки Российской Федерации (СВР России);
- Министерство обороны Российской Федерации (Минобороны 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);
- Кадровая служба;
- Служба информационной безопасности.

Организационно-технические и режимные меры и методы

Политика безопасности (информации в организации) (англ. *Organizational security policy*)[1] — совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Политика безопасности информационно-телекоммуникационных технологий (англ. *ICT security policy*)[5] — правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и её информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию.

Для построения Политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы[10]:

Защита объектов информационной системы;

Защита процессов, процедур и программ обработки информации;

Защита каналов связи (акустические, инфракрасные, проводные, радиоканалы и др.);

Подавление побочных электромагнитных излучений;

Управление системой защиты.

При этом по каждому из перечисленных выше направлений Политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

Определение информационных и технических ресурсов, подлежащих защите;

Выявление полного множества потенциально возможных угроз и каналов утечки информации;

Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

Определение требований к системе защиты;

Осуществление выбора средств защиты информации и их характеристик;

Внедрение и организация использования выбранных мер, способов и средств защиты;

Осуществление контроля целостности и управление системой защиты

Программно-технические способы и средства обеспечения информационной безопасности

- В литературе предлагается следующая классификация средств защиты информации.[10]
- Средства защиты от несанкционированного доступа (НСД):
  - Средства авторизации;
  - Мандатное управление доступом[12];
  - 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:
  - Мониторинговый программный продукт.

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.

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

Объективно категория «информационная безопасность» возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесён ущерб путём воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между всеми элементами социума.

Учитывая влияние на трансформацию идей информационной безопасности, в развитии средств информационных коммуникаций можно выделить несколько этапов[4]:

I этап — до 1816 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 1816 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).

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.

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.

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.