Информационная безопасность

Лекция 2. Общие принципы

В. М. Куприянов, Национальный центр ИНИС МАГАТЭ, НИЯУ МИФИ

НЦ ИНИС МИФИ

Цели изучения курса

- Усвоение знаний по нормативно-правовым основам организации информационной безопасности, изучение стандартов и руководящих документов по защите информационных систем;
- Ознакомление с основными угрозами информационной безопасности;
- Изучение правил выявления угроз, анализ и определение требований к различным уровням обеспечения информационной безопасности;
- Формирование научного мировоззрения , навыков индивидуальной самостоятельной работы с учебным материалом.

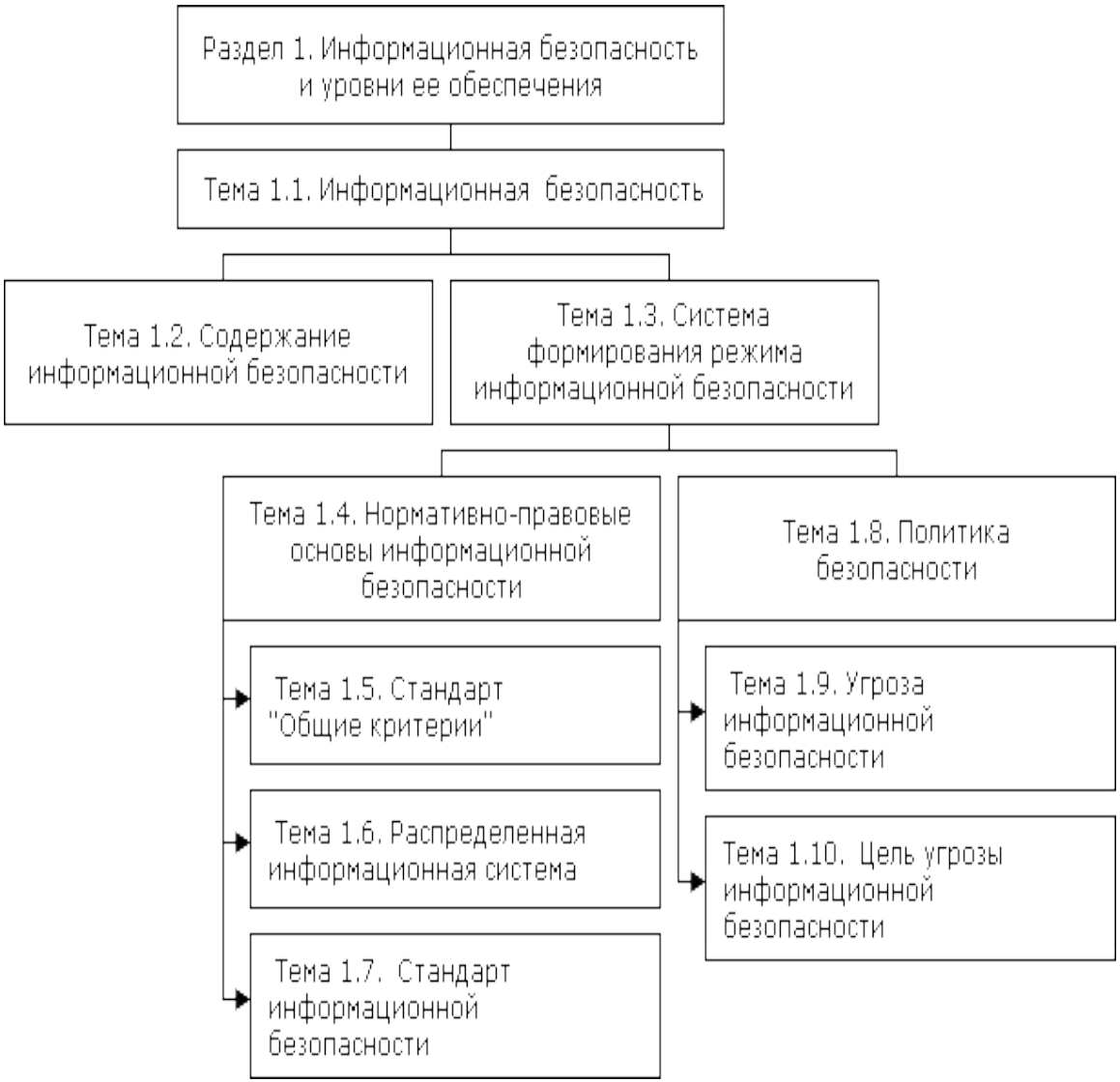
знать

- **различные подходы к определению понятия "информационная безопасность",**
- **составляющие понятия "информационная безопасность",**
- **определение целостности, конфиденциальности и доступности информации,**
- **задачи информационной безопасности,**
- **уровни формирования режима информационной безопасности,**
- **особенности законодательно-правового и административного уровней,**
- основное содержание оценочного стандарта ISO/IEC 15408,
- основное содержание стандартов по информационной безопасности распределенных систем,
- основные сервисы безопасности в вычислительных сетях,
- наиболее эффективные механизмы безопасности,
- цели и задачи административного уровня обеспечения информационной безопасности,
- содержание административного уровня,
- классы угроз информационной безопасности,
- причины и источники случайных воздействий на информационные системы,
- каналы несанкционированного доступа к информации,
- основные угрозы доступности, целостности и конфиденциальности информации;

уметь

- **объяснить, в чем заключается проблема информационной безопасности,**
- **объяснить, почему целостность, доступность и конфиденциальность являются главными составляющими информационной безопасности,**
- **использовать стандарты для оценки защищенности информационных систем,**
- выбирать механизмы безопасности для защиты распределенных вычислительных сетей,
- определять классы защищенных систем по совокупности мер защиты,
- выявлять и классифицировать угрозы информационной безопасности,
- анализировать угрозы информационной безопасности.

Структура Информационной безопасности



Цели изучения раздела

- усвоение знаний по нормативно-правовым основам организации информационной безопасности, изучение стандартов и руководящих документов по защите информационных систем;
- ознакомление с основными угрозами информационной безопасности;
- правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности;
- **формирование научного мировоззрения, навыков индивидуальной самостоятельной работы с учебным материалом.**
- **(что значит «Научное мировоззрение:**
- **- Проблемы информациологии)**

Академия информациологии

МЕЖДУНАРОДНАЯ АКАДЕМИЯ ИНФОРМАТИЗАЦИИ
общественная организация
В ГЕНЕРАЛЬНОМ КОНСУЛЬТАТИВНОМ СТАТУСЕ
С ЭКОНОМИЧЕСКИМ И СОЦИАЛЬНЫМ СОВЕТОМ ООН С 1995 Г.

РУС ENG

Главная | Академия | Мероприятия | Издания | Конкурсы | Проекты

НОВОСТИ

Вручение реликвии-амфоры Международной академии информатизации

7-й том "Элита информациологов мира"

Международная конференция "Некоторые аспекты развития мегаполиса"

все новости

Международная академия информатизации является общественной организацией, в которую в соответствии с её Уставом входят учёные, специалисты, государственные и общественные деятели, способствующие развитию информационных технологий и процессов всех отраслей хозяйства, информационно-производственной деятельности всех областей науки, информатизации общества, обеспечению информационноемких ресурсов, созданию единого мирового информационного пространства.

Информациология- церковь

- В день Торжества Православия автору этой заметки попалась в руки книга “Основы информациологии”, с околонаучным и околорелигиозным содержанием, несущим в себе определенный вызов для любого православного человека. Книга издана в издательстве “Высшая школа” в 2000 году, автор – некий И.И.Юзвишин, академик и председатель “Международной академии информатизации” (1), имеющей ни много, ни мало, а “Генеральной консультативный статус ООН и Всемирного информациологичесого парламента”. Труд г-на Юзвишина рекомендуется этой организацией как “учебник для высших и средних учебных заведений”, а также “для ученых, специалистов и служащих мирового сообщества”. Уже на титульной странице автор позволяет себе следующую выходку. Сначала цитируется Евангелие от Иоанна: “В начале было Слово и Слово было у Бога и слово было Бог…” (Ин.1,1), – а дальше идет цитата из самого г-на Юзвишина: “Бог – это Информация, и Информация – это Бог вездесущий…” Таким образом, Живой Бог, Бог-Любовь, сразу же подменяется на абстрактную “информацию” и далее во “вселенной” г-на Юзвишина более уже не присутствует. Становится понятно, с кем мы имеем дело.

Информациология (Юзвишин)

- **Информациология,** базируясь на **естественной и искусственной** инфор мации и на **информациогенно-вакуумной сущности** мироздания,**оказалась единственной генерализационной идеологией** жизнедеятельности, согласия, мира и научно-технического развития всего мирового сообщества. Именно поэтому Московский государственный университет радиотехники, электроники и автоматики (МИРЭА), Московский институт информациологии, Международная Академия Информатизации (МАИ) и другие учебные заведения, в которых читаются лекции и ведутся практические занятия по основам информациологии, придают большое значение **пропаганде идей информациологии,** просветительской и образовательской работе в области **информации, информациологи-ческой безопасности мирового сообщества, информациологических ресурсов и технологий, локальных, глобальных и космических информационных сетей, Интернет, СМИ и** т. д., в первую очередь среди ученых, преподавателей, аспирантов, студентов, специалистов, государственных и общественных деятелей.

Информациология

- Информациология дает следующее генерализационное (обобщенное) оп ределение информации: информация - это всеобщие самоотношения, самоотображения и их соотношения, представляющие универсальную генеративную информационногенную среду, являющуюся основой проявления и функционирования вакуумных и материальных сфер Вселенной. Благодаря информации появилась Вселенная - возникли галактики, планеты, Земля и жизнь на ней -постулация не требует доказательств.

Естественная информация окружающего нас мира явилась первопричиной зарождения живых существ, условием их развития и совершенствования; информация - основа отношений между людьми и природой; она является субстанцией соотношений и возникновения единого мирового информационно-сотового сообщества; информация, как универсальное (вездесущее) поле самоотношений, отображений и соотношений, - внутри нас, между нами и вне нас; **информация** - всеобщая **генеративная основа Вселенной.**

Информациология

- Информациология - это единая теория на единой фундаментальной информационной основе; это всеобщая методология и всеобщий информационный метаязык для ученых, специалистов, государственных и общественных деятелей.

Информациология завоевала широкое признание и оказывает активное воздействие на науку, политическую и экономическую жизнь общества; с информационных позиций она рассматривает весь спектр проблем физики, астрономии, химии, биологии, медицины, социологии, техники, бизнеса, политики, космоса. Широкое развитие получила информациология строительства, спорта, культуры;

- информациология рыночных отношений, политики, права; информациология района, города, региона, государства и т.д.
- Информациология - это совершенно новые супермикро- и макротехнологии во всех сферах деятельности, это научно-революционный прорыв в информационное будущее всего чело вечества и в трансцендентные миры.

Информациология обеспечила переход к духовному, биологическому и техническому развитию, которое в свою очередь создает основу небывалых возможностей для добра и зла. Поэтому информациология может быть использована определенной категорией людей в преступных и в других антигуманных целях. Она может быть использована ненадежными и опасноэксцентричными людьми как грозное оружие в информациологи-ческой войне, которая в последнее время усиленно развязывается отдельными СМИ. Поэтому информациология как ни одна из наук занимается разработкой фундаментальных основ информациологической безопасности и защиты населения в рамках распределенного информационно-сотового самоуправления каждого государства и всего мирового сообщества в целом

Информациология

- В третьем тысячелетии информация, как абсолютная истина познания явлений и процессов природы, станет глобальным ресурсом научно-технического эгресса, владея которым можно будет обойтись полностью или частично без *тонн* угля, цистерн нефти, вагонов железной руды, других материальных, трудо - финансовых ресурсов. Расшифровав информационно-кодовые структуры отношений, детерминирующих материализацию и дематериализацию в микро- и в сруктуктурах природы, люди научатся управлять процессами термоядерного синтеза, гравитации, электромагнитных и неэлектромагнитных явлений, авто-формгенезиса, автоинформгомеостаза, самообразования и самораспада в глубинных недрах Земли и в бесконечных просторах Вселенной. Получив информационный код Земли, Солнечной системы и Вселенной в целом, можно влиять не только на основные законы природы, но и управлять урожайностью культур, засухой, циклонами, другими природными явлениями и процессами, обеспечить эффктивный поиск внеземных информационно-космических цивилизаций, появится возможность оптимально решать социальные вопросы, проблемы государственного устройства, медицины, науки, культуры, спорта и т.д. Наступит эпоха транскосмических полетов и освоения галактик. С использованием информциологии успешно решаются вопросы государственной безопасности, осваиваются новейшие информационно-кодовые технологии, определяются эффектные информационные ресурсы и на их основе обеспечивается высокий уровень образования, здравоохранения и социально-экономического развития.

Законодательная база

- Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.
- Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества.
- С понятием "информационная безопасность" в различных контекстах связаны различные определения. Так, в **Законе РФ "Об участии в международном информационном обмене"** информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. Подобное же определение дается и в **Доктрине информационной безопасности Российской Федерации,** где указывается, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.
- Оба эти определения рассматривают информационная безопасность в национальных масштабах и поэтому имеют очень широкое понятие.

Различия в понятиях в России и США

- Так, например, в **"Концепции информационной безопасности сетей связи общего пользования Российской Федерации"** даны два определения этого понятия.

Информационная безопасность – это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы **информационной безопасности.**

Информационная безопасность – свойство сетей связи общего пользования сохранять неизменными характеристики **информационной безопасности** в условиях возможных воздействий нарушителя.

- Как определено стандартом МО MIL-STD-882, информационная **безопасность системы есть следствие** - "применения инженерных и управленческих принципов, критериев и методов для достижения приемлемого риска неудачи, благодаря ограничениям операционной эффективности, применимости, временных характеристик активности и управления стоимостью , на всех этапах жизненного цикла система ".

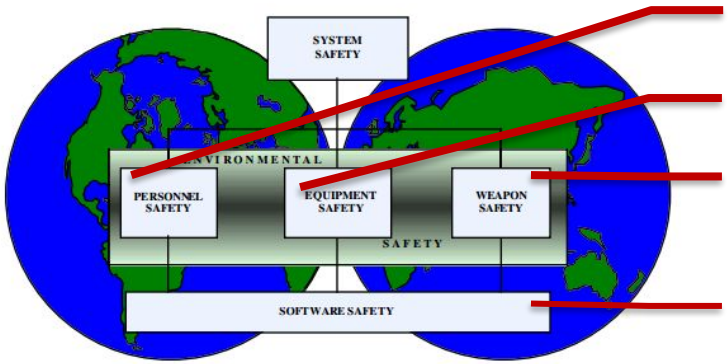


Figure 1.1 — System safety is a much broader concept than we may perceive.

Персональная безопасность

Промышленная безопасность

Военная безопасность

Безопасность программного обеспечения

Взаимодействие предметных областей

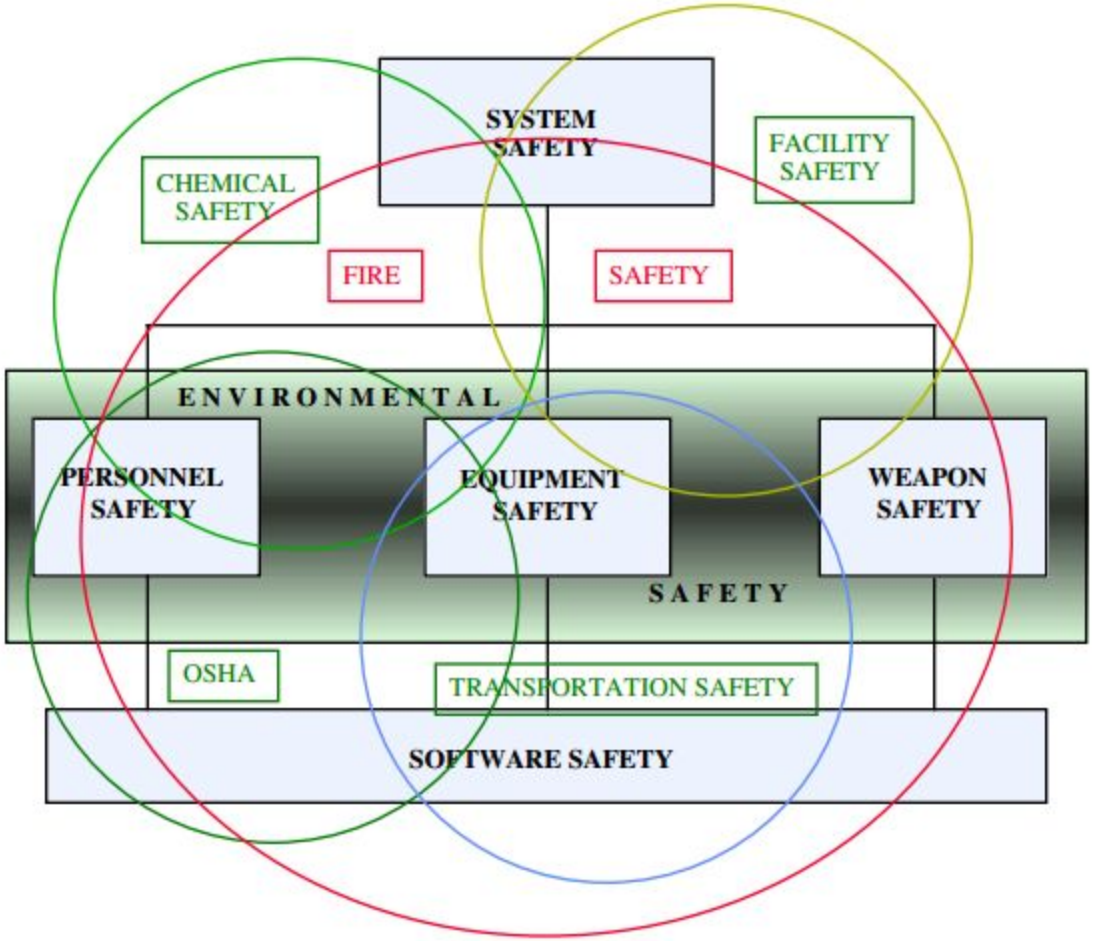


Figure 1.2 — All safety disciplines can be viewed as interrelated.

Определения системной безопасности MIL-STD-882:

Безопасность: Свобода от тех условий, которые могут привести к смерти, увечью, профессиональному заболеванию, повреждение или потере оборудования или имущества, или ущербу окружающей среде.

Система безопасности: Применение инженерных и управленческих принципов, критериев и методов достижения приемлемого риска неудачи, в рамках ограничений оперативной эффективности и полезности, затрата времени и средств, на всех этапах жизненного цикла системы

Техника безопасности: инженерная дисциплина, которая использует специализированные профессиональные знания и навыки применяемые на основе научно- технических принципов, критериев и методов для выявления и устранения опасности, в целях сокращения риска неудачи.

Критически важная безопасность : термин, применяемый к любым условиям, событиям, операциям, процессам или элементам, которые могут быть идентифицированы, и которыми можно управлять при реализации, и которые имеют важное значение для безопасности системы при ее эксплуатации и сопровождении (например, критически важные функции безопасности, критические безопасные пути, или важнейшие компоненты безопасности).

Безотказность: конструктивная особенность, позволяющая убедиться, что система остается в безопасности, или в случае отказа, то, что обеспечивается возврат системы к состоянию, которое не будет вызывать неверные действия.

Определения системной безопасности MIL-STD-882:

Опасные материалы: Любое вещество, которое угрожает безопасности, общественному здоровью и окружающей среде, требующие повышенного уровня управляющих усилий, вследствие своей химической, физической или биологической природы.

Оценка опасности для здоровья : применение биомедицинских знаний и принципов для выявления, устранения или регулирования опасностей для здоровья, связанных с системами, обеспечения и поддержки жизненного цикла материальных предметов.

Жизненный цикл: Все этапы жизни системы, включая проектирование, исследования, разработки, испытания и оценки, производства, развертывания, операций сопровождения и поддержки, утилизации.

Несчастный случай: незапланированное событие или ряд событий, приводящих к смерти, увечью, профессиональному заболеванию, повреждению или потерю оборудования или имущества, или ущерба окружающей среде.

.

Определения системной безопасности MIL-STD-882:

Риск несчастного случая: последствия возможности неудачи и ее последствий, с учетом потенциальной тяжести неудачи и вероятности возникновения.

Остаточный риск несчастного случая: остаточный риск неудачи, которая существует после всех мер которые были реализованы или исчерпаны, в соответствии с требованиями безопасности спецификаций и руководящих принципов.

Вероятность несчастного случая: совокупная вероятность возникновения отдельных событий или опасностей, которые могут создать определенную неудачу.

Уровни вероятности несчастного случая: произвольные классификации, которые обеспечивают качественную меру самой разумный вероятности возникновения неудачи в результате ошибки персонала, условий окружающей среды, конструкторских недостатков, процедурных недостатков системы, подсистемы, компонента или отказ или неисправность

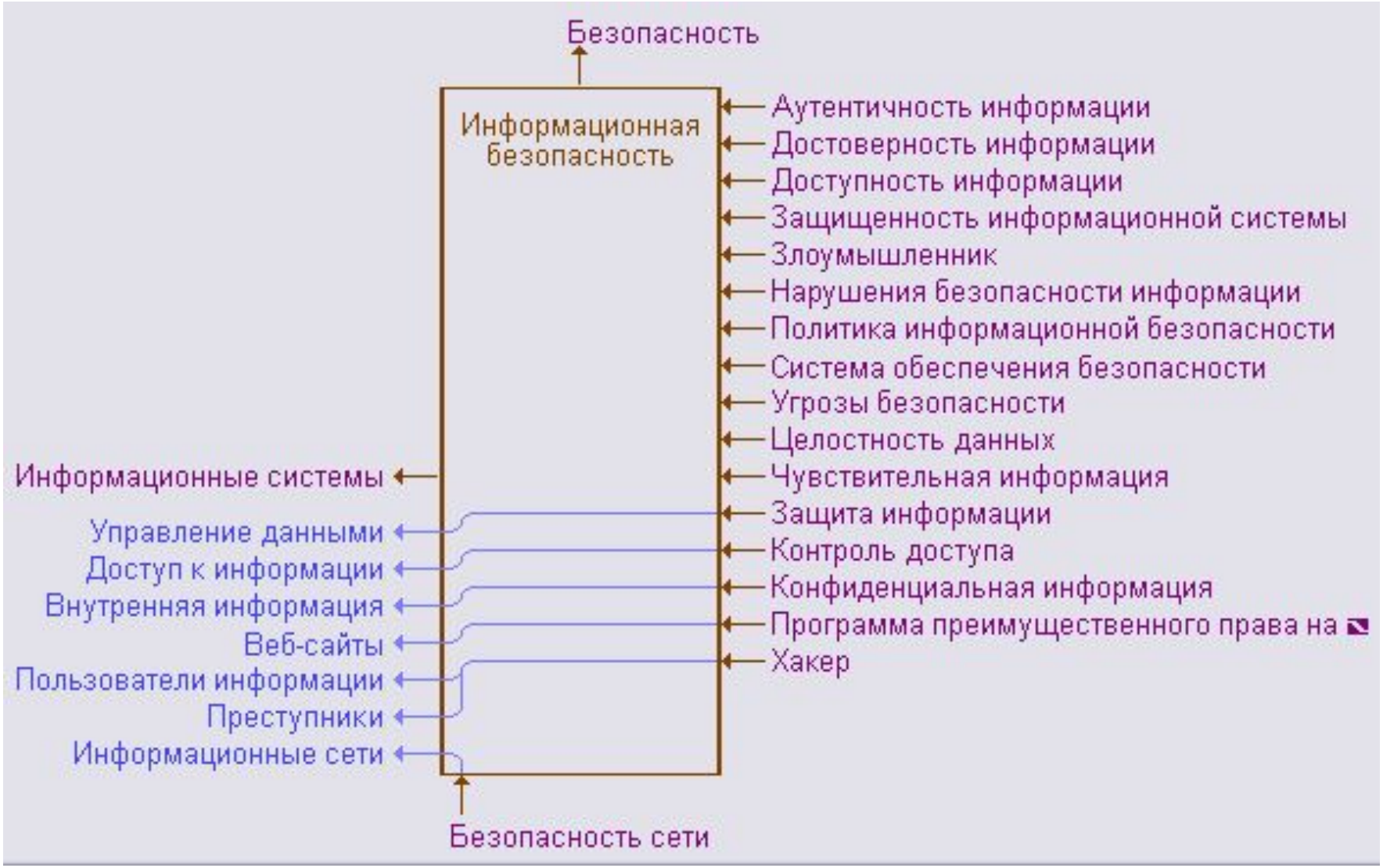
- **Информационная безопасность**
- **Безопасность информации**
- **Information security**
- Информационная безопасность - по законодательству РФ - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.
- Информационная безопасность имеет три основные составляющие:

-1- конфиденциальность - защита чувствительной информации от несанкционированного доступа;

-2- целостность - защита точности и полноты информации и программного обеспечения;

-3- доступность - обеспечение доступности информации и основных услуг для пользователя в нужное для него время.

Структура понятия «Информационная безопасность»



Базовые термины: информационная безопасность

- **Аутентичность информации**
- Аутентичность информации - избежание недостатка полноты или точности информации при ее санкционированных изменениях.
- **Безопасность**

Safety; Security

- Безопасность - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Различают:
  - социальную безопасность: правовую, интеллектуальную, духовно-культурную;
  - экономическую безопасность: финансовую, хозяйственную, технологическую; и
  - территориальную безопасность: экологическую, сырьевую, жизненную.
- Безопасность сети
- **Network security**
- Безопасность сети - меры, предохраняющие информационную сеть:
  - от несанкционированного доступа;
  - от случайного или преднамеренного вмешательства в нормальные действия; или
  - от попыток разрушения ее компонентов.
- Безопасность информационной сети включает защиту оборудования, программного обеспечения, данных и персонала.
-

Базовые термины: информационная безопасность

Достоверность информации

- Достоверность информации - в криптографии - общая точность и полнота информации. Достоверность информации обратно пропорциональна вероятности возникновения ошибок в информационной системе.

Доступность информации

- Доступность информации - избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Защита данных

Data protection

- Защита информации - совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера.

Защищенность информационной системы

- **Security**
- Защищенность информационной системы - способность системы противостоять несанкционированному доступу к конфиденциальной информации, ее искажению или разрушению. Различают два аспекта защищенности:
  -1- техническую защиту (свойство недоступности); и
  -2- социальную защищенность (свойство конфиденциальности).

Базовые термины: информационная безопасность

Контроль доступа

Access auditing

- Контроль доступа - процесс защиты данных и программ от их использования объектами, не имеющими на это права.
- В сетях для контроля доступа используются:
  - фильтрующие маршрутизаторы, реализующие алгоритмы анализа пакетов в части адресов отправления и назначения;
  - фильтры пакетов, запрещающие установление соединений, пересекающих границы защищаемой сети;
  - шлюзы прикладных программ, проверяющие права доступа к программам.

Конфиденциальная информация

- **Confidential information**
- Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством страны и уровнем доступа к информационному ресурсу. Конфиденциальная информация становится доступной или раскрытой только санкционированным лицам, объектам или процессам.

Базовые термины: информационная безопасность

Злоумышленник

Intruder

- Злоумышленник - субъект, оказывающий на информационный процесс воздействия с целью вызвать его отклонение от условий нормального протекания.
- В криптографии считается, что в распоряжении злоумышленника имеются все необходимые для выполнения его задачи технические средства, созданные на данный момент.

Конфиденциальная информация

- **Confidential information**
- Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством страны и уровнем доступа к информационному ресурсу. Конфиденциальная информация становится доступной или раскрытой только санкционированным лицам, объектам или процессам.

Базовые термины: информационная безопасность

Нарушение безопасности информации

Нарушение безопасности информации - событие, при котором компрометируется один или несколько аспектов безопасности информации (доступность, конфиденциальность, целостность и достоверность).

Политика информационной безопасности

- **Security policy**
- Политика информационной безопасности - совокупность правил, определяющих и ограничивающих виды деятельности объектов и участников, системы информационной безопасности.

Программа преимущественного права на защиту личной информации

- **Platform for privacy preferences initiative (P3P)**
- Программа преимущественного права на защиту личной информации - набор стандартов и технологических спецификаций для коммерческих веб-сайтов и браузеров. Программа обеспечивает пользователям возможность автоматического контроля информации, которую они оставляют на сайте.
-

Базовые термины: информационная безопасность

Система обеспечения безопасности

- **Security system**
- Система обеспечения безопасности - совокупность стандартных защитных мер: криптографическое кодирование, паролирование, присваивание идентификатора, электронная цифровая подпись и т.д.

Угроза безопасности

Threat

- Угроза безопасности - в широком смысле - потенциальное нарушение безопасности.
- Угроза безопасности - в системах обработки данных - потенциальное действие или событие, которое может привести к нарушению одного или более аспектов безопасности информационной системы.

Хакер

- **Hacker От англ.Hack - кромсать**
- Хакер - лицо, совершающее различного рода незаконные действия в сфере информатики:
  - несанкционированное проникновение в чужие компьютерные сети и получение из них информации;
  - незаконные снятие защиты с программных продуктов и их копирование;
  - создание и распространения компьютерных вирусов и т.п.
- Действия хакера образуют различные составы уголовных преступлений и гражданских правонарушений.
-

Базовые термины: информационная безопасность

- **Целостность данных**
- **Data integrity**
- Целостность данных - свойство, при выполнении которого данные сохраняют заранее определенный вид и качество.
- **Чувствительная информация**
- **Критическая информация**
- **Sensitive information**
- Чувствительная информация - информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к ощутимому убытку или (денежному) ущербу.