Информационная безопасность. Основные понятия.

СибГУТИ

Понятие информационной безопасности

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

Информационная безопасность – 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.

Задачи обеспечения национальной безопасности РФ

– установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;

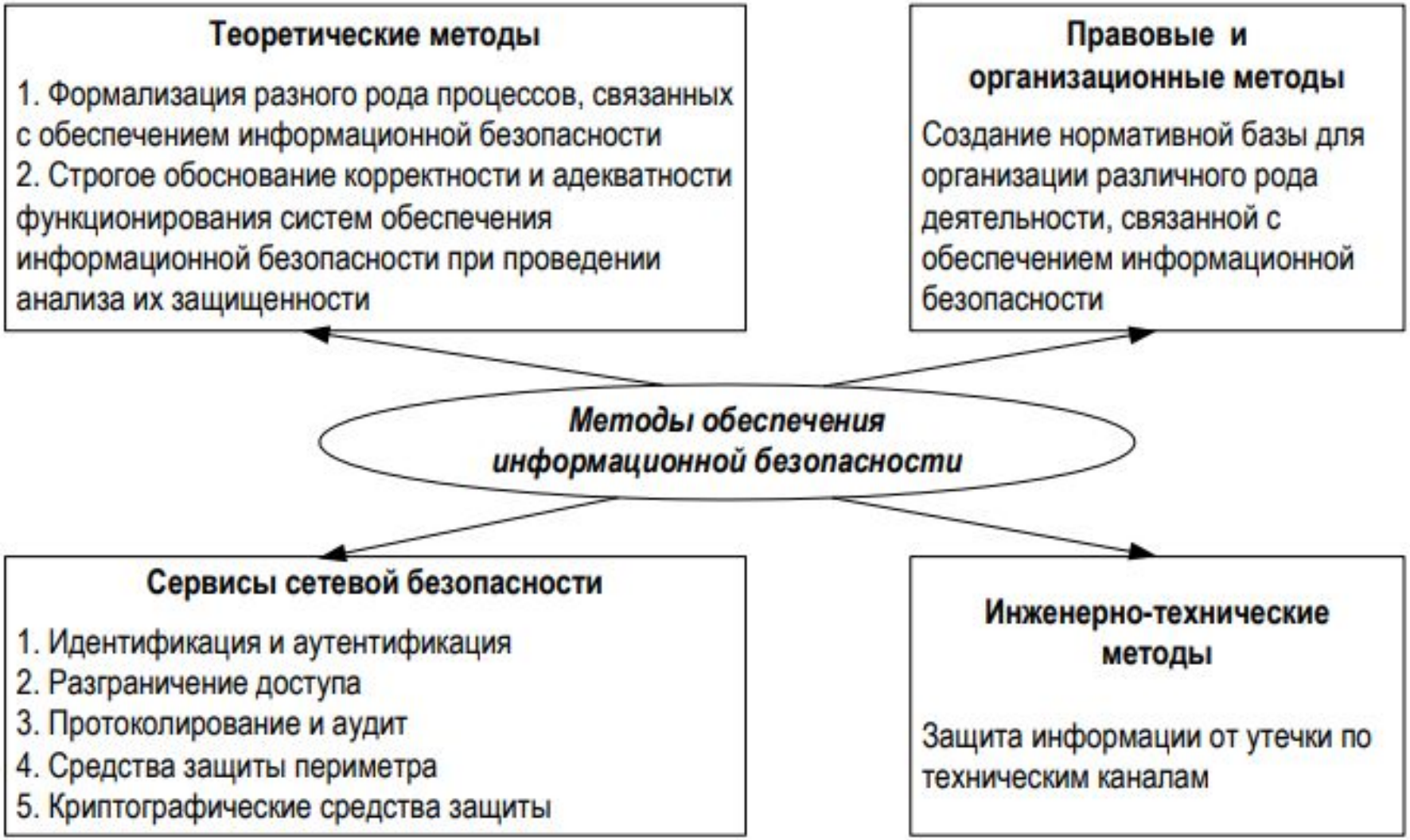
– совершенствование информационной инфраструктуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;

– разработка соответствующей нормативной базы и координация деятельности федеральных органов государственной власти, решающих задачи обеспечения информационной безопасности;

– развитие отечественной индустрии телекоммуникационных и ин- формационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;

– защита государственного информационного ресурса, и прежде всего в федеральных органах государственной власти и на предприятиях оборонного комплекса.

Методы обеспечения информационной безопасности



Основные определения

- БЕЗОПАСНОСТЬ ИНФОРМАЦИИ – состояние защищенности ин- формации, хранимой и обрабатываемой в автоматизированной системе, от негативного воздействия на нее с точки зрения нарушения ее физической и логической целостности (уничтожения, искажения) или несанкционированного использования.
- УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ – события или действия, которые могут вызвать нарушение функционирования автоматизирован- ной системы, связанное с уничтожением или несанкционированным использованием обрабатываемой в ней информации.
- УЯЗВИМОСТЬ ИНФОРМАЦИИ – возможность возникновения на каком-либо этапе жизненного цикла автоматизированной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
- ЗАЩИЩЕННОСТЬ ИНФОРМАЦИИ – поддержание на заданном уровне тех параметров находящейся в автоматизированной системе информации, которые характеризуют установленный

Основные определения

- ЗАЩИТА ИНФОРМАЦИИ – процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус ее защищенности.
- КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ – целенаправленное регулярное применение в автоматизированных системах средств и методов, а также осуществление мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся значимыми с точки зрения обеспечения безопасности информации.
- АВТОМАТИЗИРОВАННАЯ СИСТЕМА – организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации в процессе решения определенного круга прикладных задач.
- КАЧЕСТВО ИНФОРМАЦИИ – совокупность свойств, обуславливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением.

Административный уровень ИБ

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации (предприятия, фирмы).

Главная цель мер административного уровня – сформировать политику безопасности организации и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Политика безопасности – это совокупность документированных решений, принимаемых руководством организации и направленных на обеспечение информационной безопасности. Политика безопасности отражает подход организации к защите своих информационных

Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации:

Верхний уровень, к которому относятся решения, затрагивающие организацию в целом

Средний уровень, к которому относятся вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для разных видов систем обработки данных, используемых в организации

Нижний уровень, вопросы которого касаются отдельных информационных сервисов, отдельных систем и подсистем обработки данных, используемых в организации

Угрозы ИБ

Типовой объект защиты - автоматизированная система, коллектив людей и средства автоматизации их деятельности.

Состав автоматизированной системы:

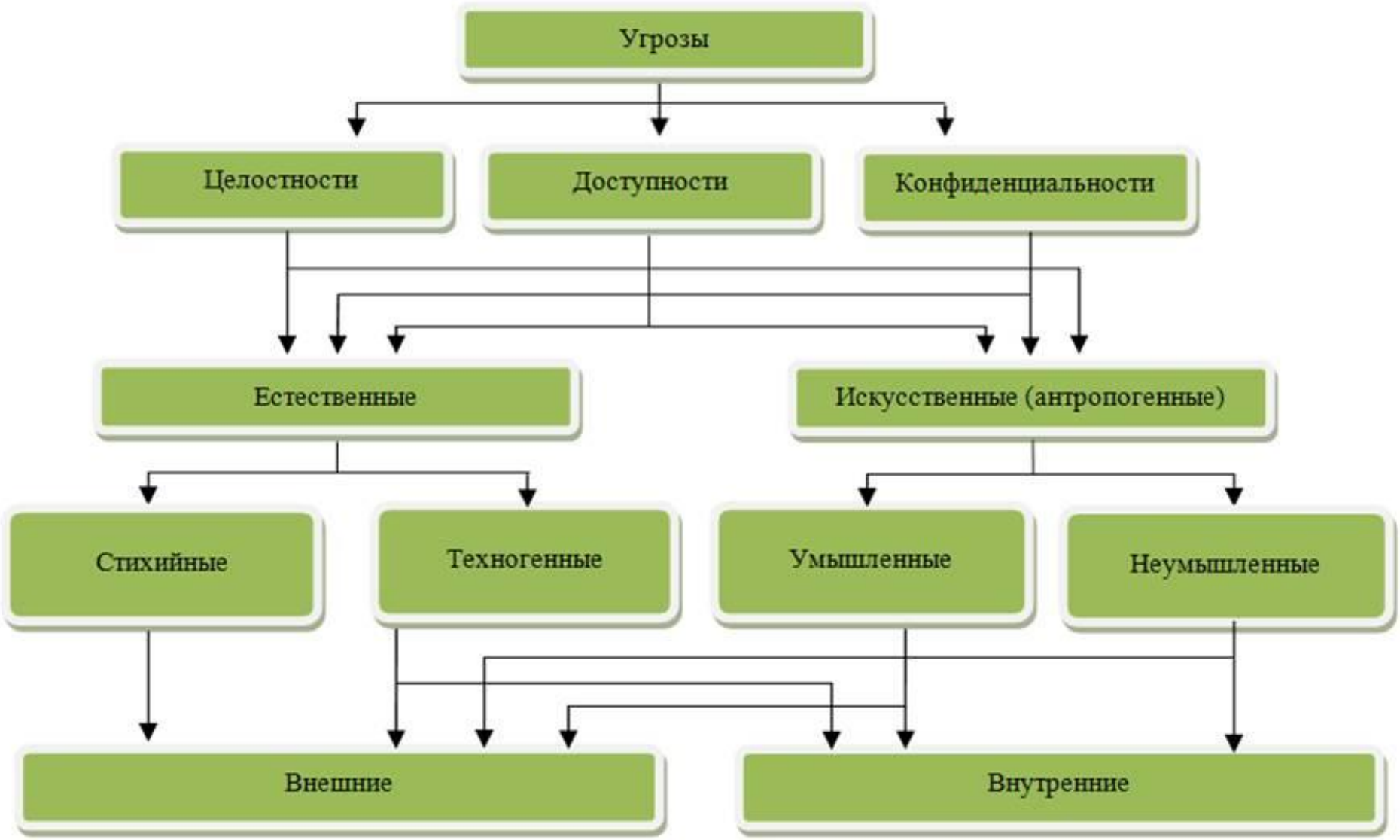
– автоматизированные рабочие места на базе автоматизированных компонентов;

– серверы (файловые, баз данных, DNS и т. д.);

– каналы передачи данных (как внутренние, так и внешние);

– отдельные и удаленные рабочие места, ЛВС, дополнительные каналы связи с удаленными пользователями.

Угрозы ИБ


Угрозы
Целостности
Доступности
Конфиденциальности
Естественные
Искусственные (антропогенные)
Стихийные
Техногенные
Умышленные
Неумышленные
Внешние
Внутренние

Угрозы ИБ

Источники угроз безопасности:

– угрозы, обусловленные действиями субъекта (антропогенные угрозы);

– угрозы, обусловленные техническими средствами (техногенные);

– угрозы, обусловленные стихийными источниками.

Группа угроз, обусловленных действиями субъекта, самая обширная и представляет наибольший интерес с точки зрения блокирования угроз. Субъекты в данном случае могут быть внутренними внешними.

Субъекты внешних угроз: криминальные структуры, недобросовестные партнеры, конкуренты, политические противники.

Субъекты внутренних угроз: персонал, лица с нарушенной психикой, внедренные агенты и т. д.

Виды угроз ИБ

Кража: Технических средств; носителей информации; информации (копирование, просмотр на дисплее); средств доступа (ключи, пароли и т. д.).

Подмена или модификация: ОС; СУБД; прикладных программ; информации (данных); паролей и правил доступа.

Уничтожение или разрушение: технических средств; носителей информации; ПО; информации; паролей и ключей.

Нарушение нормальной работы: скорости обработки информации; пропускной способности канала; уменьшения объемов свободной памяти; уменьшение объемов свободного дискового пространства; электропитания технических средств.

Ошибки: при инсталляции ПО; при написании прикладного ПО; при эксплуатации ПО; при эксплуатации технических средств.

Перехват информации: за счет побочных электромагнитных излучений (ПЭМИ); за счет наводок по посторонним проводникам; по акустическому каналу; при подключении к каналам передачи информации; за счет нарушения установленных правил доступа (взлом).

Методы защиты

Основными группами методов (способов) защиты информации являются: организационные методы, технические методы, программно-аппаратные.

Существуют четыре уровня защиты:

Предотвращение – только авторизованный персонал имеет доступ к информации и технологии;

Обнаружение – обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены;

Ограничение – уменьшается размер потерь, если преступление все- таки произошло несмотря на меры по его предотвращению и обнаружению;

Восстановление – обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

Принципы КСЗИ

К основным принципам относятся:

Принцип системного подхода к построению системы;

Принцип оптимальности (рациональности);

Принцип комплексности;

Принцип прозрачности (система защиты не должна мешать, не должна быть заметна);

Принцип модульности;

Принцип адаптивности (система защиты должна подстраиваться под изменения в компьютере);