Защита компьютерной информации

Михальцов П.А.

20 января 2020 г.

1 Защита информации в информационно вычислительных системах

1.1 Проблемы защиты компьютерной информации

Вопросы

1. Основное понятия об угрозах информационной безопасности
2. Актуальность проблемы обеспечения информационной безопасности. Задачи защиты информации
3. Задачи информационной безопасности

1.1.1 Основное понятия об угрозах информационной безопасности

Информационная безопасность — такое состояние системы, при которой она может противостоять против дестабилизирующий воздействию внешних и внутрений угроз, а также – её функционирования не создаёт информационных угроз для элементов самой системы и внешней среды

Обеспечение информационной безопасности проблемы может быть достигнуто лишь при взаимоувязанном решении трёх составляющих проблем:

- защита находящееся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации
- защита элементов системы от дестабилизирующий воздействия внешних и внутренних информационных угроз
- защита внешний среды от информационной угроз со стороны рассматриваемой системы

Под ***защитой информации*** понимать совокупность мероприятий и действий, направленнох на обеспечение её безопасности – конфендициальность и целосность – в процессе сбора, перердачи, обработки и хранения.

Безопасность информациии - это свойство (состояние) передаваемой накапливаемой, обрабатываемой и хранимой информации, характеризующие её степень защищенности от дистабилизирующиго воздействия внешней среды и внутренних угроз то есть её конфендициальность, сигнальная скрытность(энергетическая и структурная) и целостность – устойчивость к разрушающим, имитирующими и искажающим воздействиям и помехам.

Под ***защитой информации*** в более широком смысле понимают комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

Защита информации направлена на:

- предупреждение угроз как превентивных мер по обеспечению безопасности в интересах учреждения возможности их возникновения.

- выявление угроз, которое выражается в систематическом анализе и контроле возможности появления реальных и потенциальных угроз и своевременных мер по их предупреждению.

- обнаружение угроз, целью которого является определение реальных угрозы или конкретных преступных деятельности.

- ликвидацию последствий угроз и преступных действий и восстановления статуса-кво.

Обнаружение угроз — это действие по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба.

Пресечение или локализация угроз — это действие, направленное на устранение действующей угрозы и конкретных преступных действий

Ликвидация последствий имеет целью восстановлению состояния, предшествовавшего наступлению угрозы.

1.1.2 Актуальность проблемы обеспечения информационной безопасности. Задачи защиты информации

Актуальность и важность информационной безопасности(ИБ) обусловленна следующими факторами:

- высокие темпы роста парка ПК, применимых в разных сферах деятельности, и как следствие, резкое расширение круга пользователей, имеющих непосредственный доствуп к вычислительным сетям и информационным ресурсам.

- увеличение объеммов информации с помощью ПК и др. средств автоматизации

- бурное развитие апаратно–программных средств и технологий не удовлетворяющих современных ТБ.

- несоответствию развития средств обработки информации и проработки теорий ИБ разработки международных стандартов и

правовых норм, обеспечивающих необходимый уровень ЗИ защиты информации

- повсеместное распространения сетевых технологиой, создание единого информационно-коммуникативной сети Интернет, которая не может обеспечить достойного уровня ИБ.

Цели защиты иформации являются

- предотвращения утечи хищения утраты искажения поделки информации
- предостващение угроз безопасности личности, общества, гос–ва.
- предотвращение ненксанционированного действий по уничтожению, модификации, искажению, кописрования, блокировки информации.
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы
- обеспечение правого режима документированной информации как объекта собственности
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах
- сохранение государственной тайны документированной информации в соответствии с законодательством
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения

1.1.3 Задачи информационной безопасности

Основные задачи системы ИБ является

- своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующей нанесению финансовой или другого ущерба.

- создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия.

- эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и техническим мер и средств обеспечения безопасности

- Создание условий для возмещения м локализации нанесённого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушений безопасности на достижение целий организаций

1.2 Угрозы безопасности в информационно вычислительных системах

Вопросы

- Понятия угрозы безопасности
- Актуальность проблемы обеспечение информационной безопасности
- Задачи защиты информации
- Задачи информационной безопасности

Угроза — это потенциальное возможная событие, действия(воздействия), процесс или явления которые может провести к нанесению ущерба чьим либо интересам.

Существуют три разновидности угроз

- Угрозы нарушения конффендициальности
- Угрозы нанесения целостности
- Угрозы отказа служб

Угроза нарушения конфендициальности — информация становится известна тому кто не располагает полномочий к ней

Угроза нарушения целостности — заключает в себе любое умышленное изменение информации хранящая в себе(вычислительной системы) или передаваемой из одной системы в другую.

Угроза отказа служб — когда в результате преднамеренных действий предпринимаемый другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы.

Доступность информации — это свойство системы (среды, средств и технологий обработки) в которой циркулирует информация харктерезующая способность обеспечивать своевременную беспрепятственный доступ субъектов к интересующих их информации и

готовность соответствующему автоматизированных служб к обслуживанию от субъектов запросов всегда, когда в обращении к ним.
Классификация угроз информационной безопасности

- По природе возникновения
- По степени предномерености появления
    1. появление ошибок в программно-апаратных средств АС
    2. некомпетентное использование или настройка или неправомерное средств защиты персоналом службы безопасности
    3. неумышленное действие, приводящая к частичному или полному отказу системы или разрушения апоратных, программынх, информационных ресурсов системы
    4. Неправомерное включение оборудования или изменение режимов работы устройств и программ
    5. Неумышленная порча носителей информации
    6. Пересылка данных по ошибочному адресу абонента(устройства)
    7. Ввод ошибочных данных
    8. Неумышленное повреждение каналов связи
- Угрозы преднемерного действия
    1. Традиционный или универсальный шпионаж и диверсия.
    2. Несанкционированный доступ к информации
    3. Несанкционирование модификация структур
    4. Информационные инфекции
    5.