# Принципы построения систем защиты информации

# Основные принципы построения системы защиты (29 пунктов: 1-3)

1. Простота механизма защиты.
   - Этот принцип общеизвестен, но не всегда глубоко осознается. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением трудоемких действий при обычной работе законных пользователей.
2. Постоянство защиты.
   - Надежный механизм, реализующий это требование, должен быть постоянно защищен от несанкционированных изменений. Ни одна компьютерная система не может рассматриваться как безопасная, если основные аппаратные и программные механизмы, призванные обеспечивать безопасность, сами являются объектами несанкционированной модификации или видоизменения.
3. Всеобъемлющий контроль.
   - Этот принцип предполагает необходимость проверки полномочий любого обращения к любому объекту и лежит в основе системы защиты.

# Основные принципы построения системы защиты (29 пунктов: 4-5)

4. Несекретность проектирования.
   - Механизм защиты должен функционировать эффективно даже в том случае, если его структура и содержание известны злоумышленнику. Не имеет смысла засекречивать детали реализации системы защиты, предназначенной для широкого использования. Эффективность защиты не должна зависеть от того, насколько опытны потенциальные нарушители. Защита не должна обеспечиваться только секретностью структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно способствовать ее преодолению (даже автору).
5. Идентификация.
   - Каждый объект ИС должен однозначно идентифицироваться. При попытке получения доступа к информации решение о санкционировании его следует принимать на основании данных претендента и определения высшей степени секретности информации, с которой ему разрешается работать. Такие данные об идентификации и полномочиях должны надежно сохраняться и обновляться компьютерной системой для каждого активного участника системы, выполняющего действия, затрагивающие ее безопасность. Пользователи должны иметь соответствующие полномочия, объекты (файлы) — соответствующий гриф, а система должна контролировать все попытки получения доступа.

# Основные принципы построения системы защиты (29 пунктов: 6-10)

6. Разделение полномочий.
   - Применение нескольких ключей защиты. Это удобно в тех случаях, когда право на доступ определяется выполнением ряда условий.
7. Минимальные полномочия.
   - Для любой программы и любого пользователя должен быть определен минимальный круг полномочий, необходимых для работы.
8. Надежность.
   - Система ЗИ должна иметь механизм, который позволил бы оценить обеспечение достаточной надежности функционирования СЗИ (соблюдение правил безопасности, секретности, идентификации и отчетности). Для этого необходимы выверенные и унифицированные аппаратные и программные средства контроля. Целью применения данных механизмов является выполнение определенных задач методом, обеспечивающим безопасность.
9. Максимальная обособленность механизма защиты
   - защита должна быть отделена от функций управления данными.
10. Защита памяти.
   - Пакет программ, реализующих защиту, должен размещаться в защищенном поле памяти, чтобы обеспечить системную локализацию попыток проникновения извне. Даже попытка проникновения со стороны программ операционной системы должна автоматически фиксироваться, документироваться и отвергаться, если вызов выполнен некорректно.

# Основные принципы построения системы защиты (29 пунктов: 11-14)

11. Удобство для пользователей:
    - схема защиты должна быть в реализации простой, чтобы механизм защиты не создавал для пользователей дополнительных трудностей.
12. Контроль доступа
    - на основании авторизации пользователя по его физическому ключу и личному PIN-коду. Это обеспечивает защиту от атак неавторизованных пользователей на доступ: к ресурсам ПК; к областям HD ПК; к ресурсам и серверам сети; к модулям выполнения авторизации пользователей.
13. Авторизация пользователя
    - на основании физического ключа позволяет исключить непреднамеренную дискредитацию его прав доступа.
14. Отчетность.
    - Необходимо защищать контрольные данные от модификации и несанкционированного уничтожения, чтобы обеспечить обнаружение и расследование выявленных фактов нарушения безопасности. Надежная система должна сохранять сведения о всех событиях, имеющих отношение к безопасности, в контрольных журналах. Кроме того, она должна гарантировать выбор интересующих событий при проведении аудита, чтобы минимизировать стоимость аудита и повысить эффективность анализа. Наличие программных средств аудита или создание отчетов еще не означает ни усиления безопасности, ни наличия гарантий обнаружения нарушений.

# Основные принципы построения системы защиты (29 пунктов: 15-19)

15. Доступность к исполнению только тех команд операционной системы,
    - которые не могут повредить операционную среду и результат контроля предыдущей аутентификации.
16. Наличие механизмов защиты от:
    - несанкционированного чтения информации;
    - модификации хранящейся и циркулирующей в сети информации;
    - навязывания информации;
    - несанкционированного отказа от авторства переданной информации.
17. Системный подход к защите информации
    - предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенных для обеспечения безопасности ИС.
18. Возможность наращивания защиты.
    - Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.
19. Комплексный подход
    - предполагает согласованное применение разнородных средств защиты информации.

# Основные принципы построения системы защиты (29 пунктов: 20-24)

20. Адекватность
    - обеспечение необходимого уровня защиты (определяется степенью секретности подлежащей обработке информации) при минимальных издержках на создание механизма защиты и обеспечение его функционирования. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и масштаб возможного ущерба были бы приемлемыми (задача анализа риска).
21. Минимизация привилегий в доступе, предоставляемых пользователям
    - каждому пользователю должны предоставляться только действительно необходимые ему права по обращению к ресурсам системы и данным.
22. Полнота контроля
    - обязательный контроль всех обращений к защищаемым данным.
23. Наказуемость нарушений
    - наиболее распространенная мера наказания — отказ в доступе к системе.
24. Экономичность механизма
    - обеспечение минимальности расходов на создание и эксплуатацию механизма.

# Основные принципы построения системы защиты (29 пунктов: 25-27)

25. Принцип системности

- сводится к тому, что для обеспечения надежной защиты информации в современных ИС должна быть обеспечена надежная и согласованная защита во всех структурных элементах, на всех технологических участках автоматизированной обработки информации и во все время функционирования ИС.

26. Специализация, как принцип организации защиты,

- предполагает, что надежный механизм защиты может быть спроектирован и организован лишь профессиональными специалистами по защите информации. Кроме того, для обеспечения эффективного функционирования механизма защиты в состав ИС должны быть включены соответствующие специалисты.

27. Принцип неформальности

- означает, что методология проектирования механизма защиты и обеспечения его функционирования в основе своей — неформальна. В настоящее время не существует инженерной (в традиционном понимании этого термина) методики проектирования механизма защиты. Методики проектирования, разработанные к настоящему времени, содержат комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое их осуществление в общем случае невозможно.

# Основные принципы построения системы защиты (29 пунктов: 28-29)

28. Гибкость системы защиты.

- Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью.
- Особенно важно это свойство в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

29. Принцип непрерывности защиты

- предполагает, что защита информации — это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС.
- Разработка системы защиты должна осуществляться параллельно с разработкой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные защищенные информационные системы.

# Понятие защиты

- На формулирование понятия защиты оказывает влияние большое количество разноплановых факторов, основными из которых выступают:
  - влияние информации на эффективность принимаемых решений;
  - концепции построения и использования защищенных информационных систем;
  - техническая оснащенность информационных систем;
  - характеристики информационных систем и их компонентов с точки зрения угроз сохранности информации;
  - потенциальные возможности злоумышленного воздействия на информацию, ее получение и использование;
  - наличие методов и средств защиты информации.

# Развитие понятия защиты

- Можно выделить три периода развития СЗИ:
  - первый — относится к тому времени, когда обработка информации осуществлялась по традиционным (ручным, бумажным) технологиям;
  - второй — когда для обработки информации на регулярной основе применялись средства электронно-вычислительной техники первых поколений;
  - третий — когда использование ИТ приняло массовый и повсеместный характер.

# Системность подхода

- Защита информации представляет собой регулярный процесс
  - заключается не только в создании соответствующих механизмов,
  - а осуществляется на всех этапах жизненного цикла систем обработки данных при комплексном использовании всех имеющихся средств защиты.
  - Все средства, методы и мероприятия, используемые для ЗИ, непременно и наиболее рационально объединяются в единый целостный механизм — систему защиты, которая должна обеспечивать глубокоэшелонированную оборону, не только от злоумышленников, но и от некомпетентных или недостаточно подготовленных пользователей и персонала.
- В системе защиты должно быть, по крайней мере, 4 защитных пояса:
  - внешний, охватывающий всю территорию, на которой расположены сооружения;
  - пояс сооружений, помещений или устройств системы;
  - пояс компонентов системы (технических средств, программного обеспечения, элементов баз данных) и
  - пояс технологических процессов обработки данных (ввод/вывод, внутренняя обработка и т.п.).

# Трудности реализации СЗИ

- При реализации СЗИ учитываются две группы противоречивых требований, обеспечивающих надежную защиту находящейся в системе информации
  1. исключение случайной и преднамеренной выдачи информации посторонним лицам и разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала.
  2. системы защиты не должны создавать заметных неудобств в процессе работы с использованием ресурсов системы.
- В частности должны быть гарантированы:
  - полная свобода доступа каждого пользователя и независимость его работы в пределах предоставленных ему прав и полномочий;
  - удобство работы с информацией для групп взаимосвязанных пользователей;
  - возможности пользователям допускать друг друга к своей информации.

# Основные правила защиты

- Основные правила, которыми рекомендуют руководствоваться специалисты при организации работ по защите информации, сводятся к следующему:

1. Обеспечение безопасности информации есть непрерывный процесс, состоящий в систематическом контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.
2. Безопасность информации в системе обработки данных может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты.
3. Никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты.
4. Никакую систему защиты нельзя считать абсолютно надежной, следует исходить из того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

# Основные средства, используемые для защиты - технические и программные

- Технические средства - реализуются в виде электрических, электромеханических, электронных устройств.
- Их принято делить на аппаратные и физические.
  - Под аппаратными средствами защиты понимают устройства, внедряемые непосредственно в аппаратуру обработки данных, или устройства, которые сопрягаются с ней по стандартному интерфейсу.
  - Наиболее известные аппаратные средства, используемые на первом этапе — это схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры (например, регистры границ поля ЗУ) и т.п.
  - Физическими средствами названы такие, которые реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения, замки на дверях, решетки на окнах и т.п.).
- Программные средства защиты – программы, специально предназначенные для выполнения функций, связанных с ЗИ.

# Защищенная ИС и система ЗИ

- Многие специалисты считают, что точный ответ на вопрос, что же такое “защищенная информационная система”, пока не найден.
- Существуют следующие представления защищенности ИС:
  - это совокупность средств и технологических приемов, обеспечивающих защиту компонентов ИС;
  - это минимизация риска, которому могут быть подвергнуты компоненты и ресурсы ИС;
  - это комплекс процедурных, логических и физических мер, направленных на предотвращение угроз информации и компонентам ИС.

# Рекомендации по созданию СЗИ

1. Определиться, имеется ли у Вас информация, которую нельзя не защищать; это важно, поскольку, как правило, ЗИ потребует дополнительных средств и достаточно больших.
2. Определить конкретные сведения, подлежащие защите, для чего и от кого их защищать, а так же степень надежности такой защиты — проделать это не сложно.
3. Выявить потенциальные угрозы и наиболее вероятные каналы утечки информации для конкретных условий. Их может оказаться достаточно много, но не стоит огорчаться, так все сразу они не будет их использоваться.
4. Выбор из множества предлагаемых вариантов таких методов, мероприятий и средств, которые можно было бы использовать конкретно в Вашей ИС.
5. После того как удалось найти конкретные варианты организационных и технических решений, необходимо подсчитать затраты на их реализацию. Вот здесь можно и огорчиться.
6. Сомнения и чувство досады, возникающие в такие моменты — это вполне нормальное явление.
7. Часто при этом всплывают воспоминания о том, как спокойно жилось, пока проблемы защиты информации не были Вам знакомы.

# Закон Мерфи.
# Актуален и для проблем ЗИ

**Если какая-нибудь неприятность может случиться, она случается.**

Следствия.

1. Все не так легко, как кажется.
2. Всякая работа требует больше времени, чем вы думаете.
3. Из всех неприятностей произойдет именно та, ущерб от которой больше.
4. Если четыре причины возможных неприятностей заранее устранены, то всегда найдется пятая.
5. Предоставленные самим себе, события имеют тенденцию развиваться от плохого к худшему.
6. Как только вы принимаетесь делать какую-то работу, находится другая, которую надо сделать еще раньше.
7. Всякое решение плодит новые проблемы.