Чеченский государственный педагогический университет

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Лекция № 3. Угрозы информационной безопасности

Лектор – Иноркаев Вахид Абу-Рашидович,
Старший преподаватель кафедры «Информационные технологии»

Угрозы информационной безопасности

В настоящей лекции рассматриваются основные аспекты информационной безопасности, включая анализ уязвимостей систем, классификацию угроз, методы их реализации и построение модели нарушителя.

Угроза — это фактор, стремящийся нарушить работу системы.

Угрозы информационной безопасности

При построении системы защиты информации необходимо определить, что следует защищать и и от кого или чего следует строить защиту. Угрозы возникают в случае наличия в системе уязвимостей, которые могут привести к нарушению информационной безопасности.

Перечень наиболее вероятных угроз безопасности и характеристика наиболее вероятного нарушителя индивидуальны для каждой системы. Поэтому важно провести анализ уязвимостей системы и построить неформальную модель нарушителя на этапе проектирования системы защиты.

Оценка уязвимости системы позволяет выявить слабые места и разработать эффективные меры по обеспечению информационной безопасности. Это включает в себя классификацию угроз, основные направления и методы их реализации, а также анализ возможных действий нарушителя.

Классификация угроз информационной безопасности

Природа возникновения: естественные угрозы (связанные с природными процессами) и искусственные (вызванные деятельностью человека).

Степень преднамеренности проявления: случайные или преднамеренные.

Источник угроз: природная среда, человек, санкционированные программно-аппаратные средства, несанкционированные программно-аппаратные средства.

Положение источника угроз: в пределах или вне контролируемой зоны.

Зависимость от активности системы: проявляются только в процессе обработки данных или в любое время.

Степень воздействия на систему: пассивные, активные (вносят изменения в структуру и содержание системы).

Этап доступа к ресурсам: на этапе доступа, после получения доступа.

Способ доступа к ресурсам: стандартный, нестандартный.

Место расположения информации: внешние носители, оперативная помять, линии связи, устройства ввода-вывода.

Классификация угроз информационной безопасности

Угроза нарушения конфиденциальности реализуется в том случае, если информация становится известной лицу, не располагающему полномочиями доступа к ней. Угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в информационной системе или передаваемой от одной системы к другой. Иногда в связи с угрозой нарушения конфиденциальности используется термин «утечка».

Угроза нарушения целостности реализуется при несанкционированном изменении информации, хранящейся в информационной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена.

Угроза нарушения доступности (отказа служб) реализуется, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Блокирование может быть постоянным — запрашиваемый ресурс никогда не будет получен, или может вызывать только задержку запрашиваемого ресурса.

Виды угроз конфиденциальности

Виды угроз для информационных систем:
- угроза нарушения конфиденциальности;
- угроза нарушения целостности;
- угроза нарушения доступности.

Основные свойства защищаемой информации:
- конфиденциальность (защита от несанкционированного доступа);
- целостность (защита от несанкционированных изменений);
- доступность (обеспечение бесперебойной работы системы).

Классификация угроз:
- по положению источника угроз (в пределах или вне контролируемой зоны);
- по зависимости от активности системы (проявляются только в процессе обработки данных или в любое время);
- по степени воздействия на систему (пассивные, активные).

Этапы доступа к ресурсам:
- на этапе доступа;
- после получения доступа.

Способы доступа к ресурсам:
- стандартный;
- нестандартный.

Угрозы информационной безопасности

Угрозы информационной безопасности могут включать в себя утечку секретной информации, несанкционированное изменение данных и отказ служб. Эти угрозы могут привести к серьёзным последствиям, поэтому важно принимать меры по защите информационных систем.

Нарушение целостности информации может произойти как из-за преднамеренных действий злоумышленников, так и из-за случайных ошибок программного или аппаратного обеспечения. Поддержание целостности данных является ключевым аспектом информационной безопасности.

Для предотвращения угроз доступности необходимо принимать меры по защите информационных систем от преднамеренных действий, которые могут привести к отказу служб. Это включает в себя использование надёжных паролей, регулярное обновление программного обеспечения и обеспечение безопасности сети.

Угрозы информационной безопасности

В открытых системах без мер защиты информации реализация угроз, связанных с блокировкой доступа к ресурсам, может привести к непосредственному воздействию на защищаемую информацию.

Угрозы, сформулированные в 1960-х годах для открытых UNIX-подобных систем, остаются актуальными и в настоящее время.

Для современных информационных систем необходимо разрабатывать и внедрять эффективные меры защиты, чтобы предотвратить реализацию этих угроз.

Отсутствие систем защиты делает информационные системы уязвимыми для атак, направленных на блокировку доступа к ресурсам.

Угрозы информационной безопасности

Системы защиты информации являются неотъемлемой частью комплексов по обработке информации, и преодоление этих систем представляет собой отдельную угрозу.

Разведка перед проведением мероприятий позволяет определить основные параметры и характеристики системы, что может привести к выбору оптимальных технических средств и реализации первичных угроз.

Угроза раскрытия параметров системы является опосредованной, поскольку сама по себе не причиняет ущерба обрабатываемой информации, но создаёт условия для реализации других, более непосредственных угроз.

Методы реализации угроз

Основные направления реализации информационных угроз включают непосредственное обращение к объектам доступа, создание обходных средств, модификацию средств защиты и внедрение механизмов, нарушающих структуру системы. Эти действия позволяют злоумышленнику получить несанкционированный доступ к информации.

Методы реализации информационных угроз разнообразны: определение типа и параметров носителей информации, получение данных о программно-аппаратной среде и средствах вычислительной техники. Такие методы помогают злоумышленнику эффективно атаковать информационные системы.

Разведка параметров информационной системы является реализованной угрозой для открытых систем. Это подчёркивает важность защиты информации и необходимость применения соответствующих мер для предотвращения утечек и несанкционированного доступа.

В интернете есть много сайтов с информацией на эту тему. [Посмотрите, что нашлось в поиске](https://ya.ru

В интернете есть много сайтов с информацией на эту тему. [Посмотрите, что нашлось в поиске](https://ya.ru)

Угрозы информационной безопасности

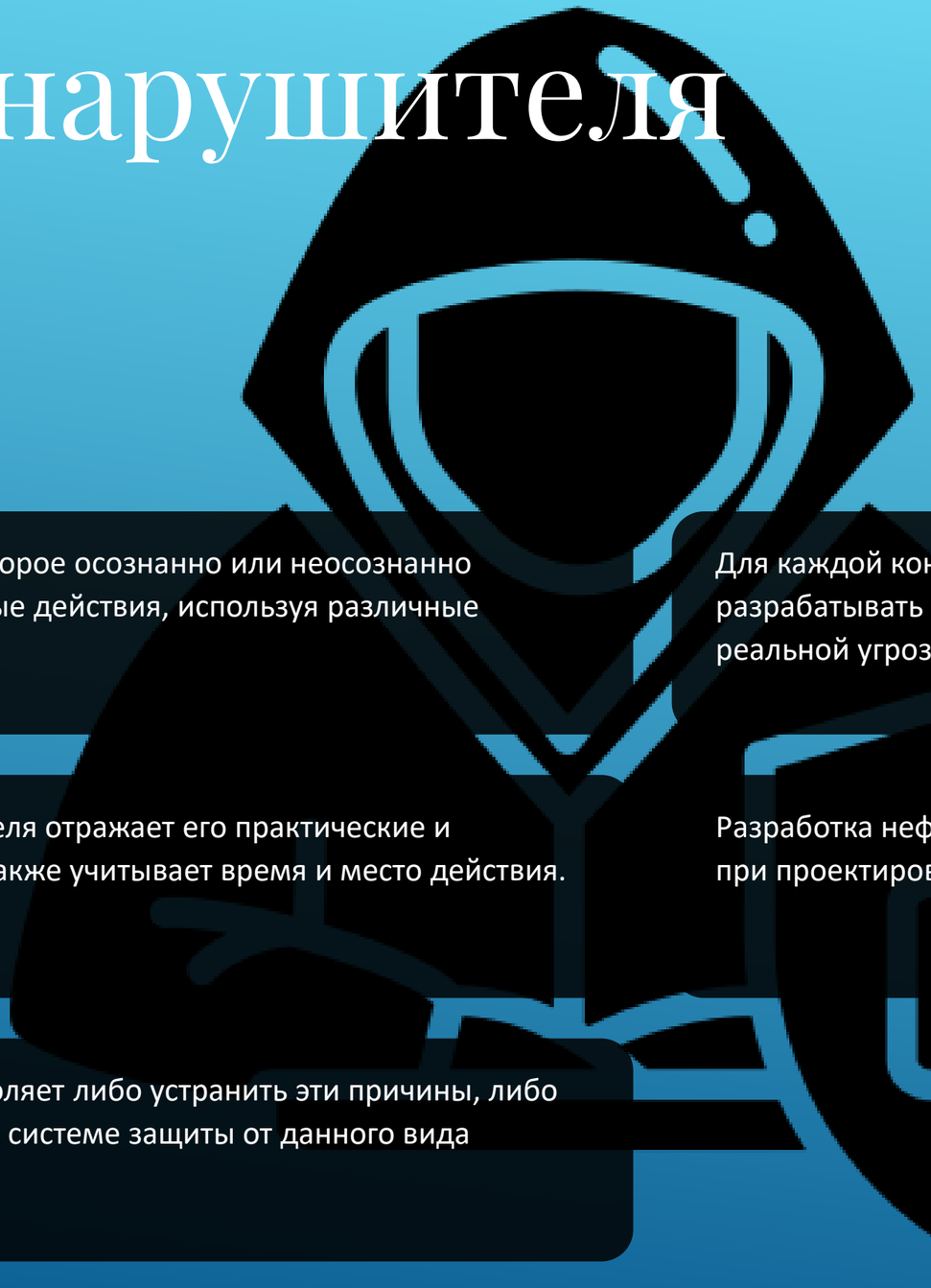
Угрозы информационной безопасности включают в себя различные методы, такие как раскрытие содержания информации на семантическом уровне, уничтожение носителей информации и внесение несанкционированных изменений в систему.

Методы реализации угроз охватывают все уровни представления информации: от каналов связи до семантического уровня.

Нарушитель может использовать разнообразные способы, включая установку нештатного оборудования, заражение вирусами и внедрение дезинформации, чтобы нанести ущерб информационной безопасности.

Важно учитывать, что угрозы могут проявляться не только через технические средства, но и через ошибки в проектировании и разработке аппаратных и программных компонентов.

Модель нарушителя



Злоумышленник — это лицо, которое осознанно или неосознанно пытается выполнить запрещённые действия, используя различные методы и средства.

Неформальная модель нарушителя отражает его практические и теоретические возможности, а также учитывает время и место действия.

Анализ причин нарушений позволяет либо устранить эти причины, либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

Для каждой конкретной технологии обработки информации необходимо разрабатывать свою модель нарушителя, которая будет соответствовать реальной угрозе для данной системы.

Разработка неформальной модели нарушителя является важным этапом при проектировании системы защиты и оценке её защищённости.

Модель нарушителя

1

При разработке модели нарушителя важно учитывать, что большинство нарушений совершается внутренними нарушителями — персоналом системы. К внутренним нарушителям относятся руководители различных уровней, пользователи системы, сотрудники отделов разработки и сопровождения программного обеспечения, персонал, обслуживающий технические средства, и технический персонал.

2

Мотивы действий нарушителя могут быть разными: от несанкционированного доступа к информации до намеренного нанесения ущерба системе. Предположения о мотивах действий нарушителя помогают определить возможные угрозы и разработать меры по их предотвращению.

3

Квалификация и техническая оснащённость нарушителя также являются важными факторами. Необходимо учитывать, какие методы и средства может использовать нарушитель для совершения преступления, чтобы разработать эффективные меры защиты.

Модель нарушителя

Неформальная модель нарушителя включает в себя высокий уровень знаний и опыт работы с техническими средствами системы, а также опыт их обслуживания. Нарушитель обладает глубокими знаниями в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем.

Уровень возможностей нарушителя определяет его способность вести диалог с системой. Первый уровень позволяет запускать задачи из фиксированного набора, второй — создавать и запускать собственные программы, третий — управлять функционированием системы, а четвёртый даёт возможность вносить изменения в базовое программное обеспечение и конфигурацию оборудования.

Чем выше уровень возможностей нарушителя, тем больше вреда он может причинить системе. На первом уровне он ограничен заранее предусмотренными функциями, на втором может создавать новые программы, на третьем — влиять на базовое программное обеспечение, а на четвёртом — вносить значительные изменения в систему.

Для защиты от нарушителей разных уровней необходимо применять различные меры. От первого уровня можно защититься с помощью стандартных средств безопасности, от второго — с помощью дополнительных настроек и ограничений, от третьего — с помощью специализированных средств защиты, а от четвёртого — путём разработки уникальной системы безопасности.

Классификация нарушителей

Виды нарушителей информационной безопасности: к основным категориям относятся сотрудники организации, посторонние лица (посетители, клиенты, представители организаций и конкуренты) и любые лица за пределами контролируемой территории.

Мотивы нарушений: можно выделить три основных мотива — безответственность, самоутверждение и корыстный интерес. Нарушения, вызванные безответственностью, обычно являются следствием некомпетентности или небрежности.

Классификация нарушителей по уровню знаний о системе: нарушители могут обладать различными уровнями знаний о функционировании системы, от поверхностных до глубоких, что влияет на их способность совершать целенаправленные и эффективные атаки на информационную безопасность.

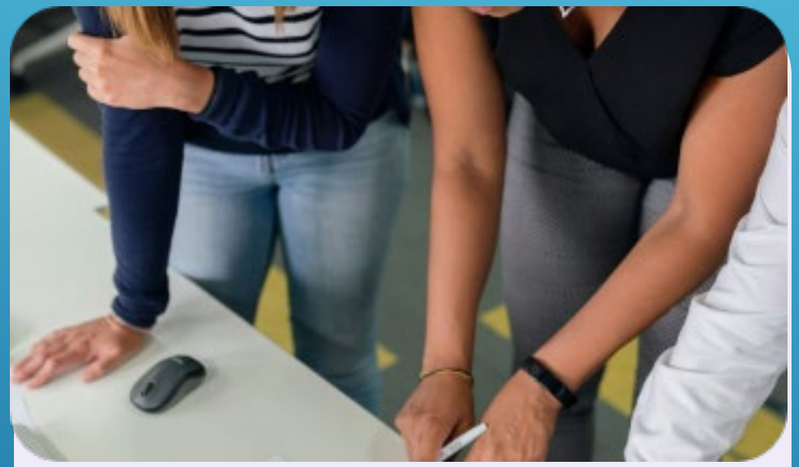
Угрозы информационной безопасности

В руководящем документе Гостехкомиссии представлена классификация нарушителей по уровню возможностей. Каждый следующий уровень включает в себя функциональные возможности предыдущего, при этом нарушитель на своём уровне является специалистом высшей квалификации и знает всё об информационной системе и её защите.

Угрозы информационной безопасности в автоматизированных системах могут возникать как в процессе функционирования компонентов системы, так и в период их неактивности — в нерабочее время, во время плановых перерывов в работе системы или перерывов для обслуживания.

Классификация угроз информационной безопасности является иерархической, что позволяет учитывать различные уровни квалификации нарушителей и время возникновения угроз, обеспечивая более эффективный подход к защите информации.

Оценка уязвимости системы



Для обеспечения эффективной защиты информации необходимо учитывать различные типы возможных нарушителей, их характеристики и места действия. Это позволяет создать модель нарушителя, которая будет соответствовать особенностям конкретной предметной области и технологии обработки информации.

Количественная оценка уязвимости системы является важным этапом в решении практических задач защиты информации. Она позволяет определить слабые места в системе и разработать меры по их устранению.

При построении модели нарушителя важно учитывать субъективные факторы, связанные с определением его характеристик. Это помогает создать более точную и реалистичную модель, которая будет способствовать повышению уровня безопасности информации.

Методы защиты информации

Для защиты от случайных угроз в автоматизированных системах используются средства повышения надёжности и достоверности информации, а также её резервирование.

При проектировании защиты от преднамеренных угроз важно определить перечень и классификацию данных, подлежащих защите, а также оценить квалификацию и модель поведения потенциального нарушителя.

В соответствии с моделью нарушителя в системе выявляются возможные каналы несанкционированного доступа к данным, которые делятся на технически контролируемые и неконтролируемые.

Эффективная защита информации требует комплексного подхода, включающего как меры по предотвращению случайных угроз, так и меры по противодействию преднамеренным угрозам.

Защита информации

Для обеспечения информационной безопасности создаётся автоматизированная система, которая объединяет средства защиты в единую оболочку. Эта оболочка анализирует состав и принципы построения информации и перекрывает возможные пути её утечки.

Степень защиты информации определяется полнотой перекрытия каналов утечки и прочностью защиты. Прочность оболочки зависит от модели поведения потенциального нарушителя.

Защитная оболочка информации строится на основе анализа каналов связи и выбора готовых средств защиты или создания новых. Это позволяет предотвратить несанкционированный доступ к данным.

Прочность защиты

Прочность защитной преграды считается достаточной, если ожидаемое время её преодоления нарушителем больше времени жизни защищаемого объекта или времени обнаружения и блокировки доступа.

Для обеспечения эффективной защиты информационная система должна иметь отдельные виртуальные защитные оболочки: контролируемую и превентивную. Это позволит использовать разные принципы построения средств защиты на контролируемых и неконтролируемых каналах доступа.

На контролируемых каналах нарушитель рискует быть пойманным, поэтому прочность защиты на этих каналах может быть ниже. На неконтролируемых каналах нарушитель может работать в комфортных условиях, не ограниченных временем и средствами, поэтому прочность защиты на этих каналах должна быть значительно выше.

СПАСИБО ЗА ВНИМАНИЕ

Лектор – Иноркаев Вахид Абу-Рашидович,
Старший преподаватель кафедры «Информационные технологии»