Информационная безопасность

Лекция 2

Угрозы информационной безопасности

Анализ уязвимостей системы

При построении системы защиты информации обязательно нужно определить, что следует защищать и от кого (или чего) следует строить защиту.

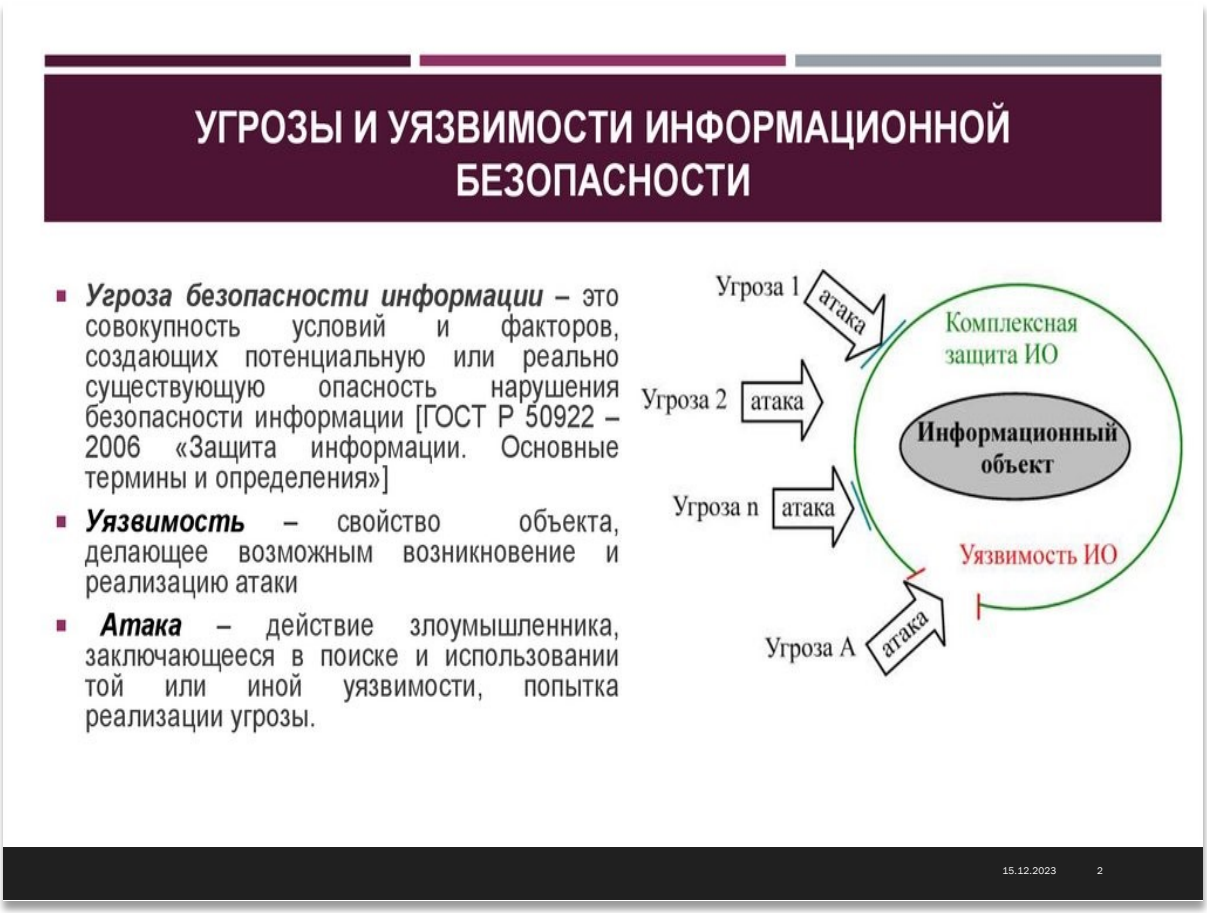
Защищаться следует от множества угроз, которые проявляются через действия нарушителя. Угрозы возникают в случае наличия в системе уязвимостей, то есть таких свойств информационной системы, которые могут привести к нарушению информационной безопасности.

Определение перечня угроз и построение модели нарушителя являются обязательным этапом проектирования системы защиты. Для каждой системы перечень наиболее вероятных угроз безопасности, а также характеристика наиболее вероятного нарушителя индивидуальны, поэтому перечень и модель должны носить неформальный характер.

Защищенность информации обеспечивается только при соответствии предполагаемых угроз и качеств нарушителя реальной обстановке.

При наличии в системе уязвимости потенциальная угроза безопасности может реализоваться в виде атаки. Атаки принято классифицировать в зависимости от целей, мотивов, используемого механизма, места в архитектуре системы и местонахождения нарушителя.

Для предупреждения успешных атак необходим поиск и анализ уязвимостей системы. Уязвимости различаются в зависимости от источника возникновения, степени риска, распространенности, места в жизненном цикле системы, соотношения с подсистемами защиты. Анализ уязвимостей — обязательная процедура при аттестации объекта информатизации. В связи с возможностью появления новых уязвимостей необходим их периодический анализ на уже аттестованном объекте.



Классификация угроз информационной безопасности

Угроза — это фактор, стремящийся нарушить работу системы.

В настоящее время рассматривается достаточно обширный перечень угроз информационной безопасности, насчитывающий сотни пунктов.

Кроме выявления возможных угроз, должен быть проведен анализ этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из требований к системе защиты. При этом угрозы, соответствующие каждому признаку классификации, позволяют уточнить требования.

Для защищаемой системы составляют не полный перечень угроз, а перечень классов угроз, определяемых по ряду базовых признаков. Это связано с тем, что описать полное множество угроз невозможно из-за большого количества факторов, влияющих на информацию.

Например, можно предложить классифицировать угрозы по следующим признакам:

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

2. Степень преднамеренности проявления: случайные или

преднамеренные.

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

4. Положение источника угроз: в пределах или вне контролируемой зоны.

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

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

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

8. Способ доступа к ресурсам: стандартный, нестандартный.

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

Вне зависимости от конкретных видов угроз было признано целесообразным связать угрозы с основными свойствами защищаемой информации.

Соответственно для информационных систем было предложено рассматривать три основных вида угроз:

- 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 формации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).
- 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.

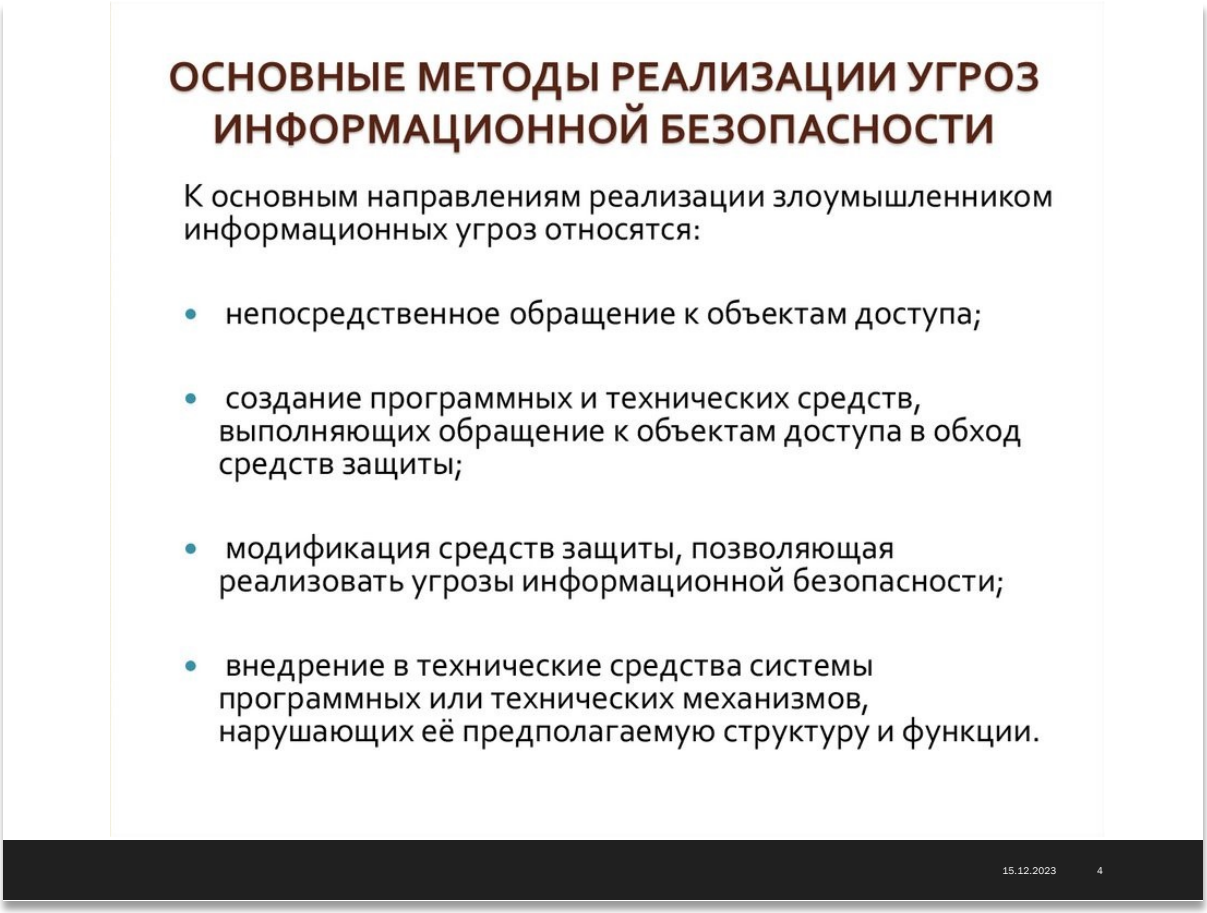
Данные виды угроз можно считать первичными, или непосредственными, т. к. если рассматривать понятие угрозы как некоторой потенциальной опасности, реализация которой наносит ущерб информационной системе, то реализация вышеперечисленных угроз приведет к непосредственному воздействию на защищаемую информацию.

В то же время непосредственное воздействие на информацию возможно для атакующей стороны в том случае, если система, в которой циркулирует информация, для нее «прозрачна», т. е. не существует никаких систем защиты или других препятствий. Описанные выше угрозы были сформулированы в 1960-х гг. применительно к открытым UNIX-подобным системам, для которых не предусматривались меры по защите информации.

На современном этапе развития информационных технологий подсистемы или функции защиты являются неотъемлемой частью комплексов по обработке информации. Информация не представляется «в чистом виде», на пути к ней имеется хотя бы какая-нибудь система защиты, и поэтому, чтобы угрожать, атакующая сторона должна преодолеть эту систему. Поскольку преодоление защиты также представляет собой угрозу, для защищенных систем будем рассматривать ее четвертый вид — угрозу раскрытия параметров системы, включающей в себя систему защиты. На практике любое проводимое мероприятие предваряется этапом разведки, в ходе которой определяются основные параметры системы, ее характеристики и т. п. Результатом разведки является уточнение поставленной задачи, а также выбор наиболее оптимального технического средства.

Угрозу раскрытия параметров системы можно рассматривать как опосредованную. Последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность реализоваться первичным, или непосредственным, угрозам. Введение данного вида угроз позволяет описывать с отличия защищенных информационных систем от открытых. Для последних угроза разведки параметров системы считается реализованной.

Основные направления и методы реализации угроз



К основным направлениям реализации злоумышленником информационных угроз относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;
- внедрение в технические средства программных или технических механизмов, нарушающих предполагаемую структуру и функции системы.

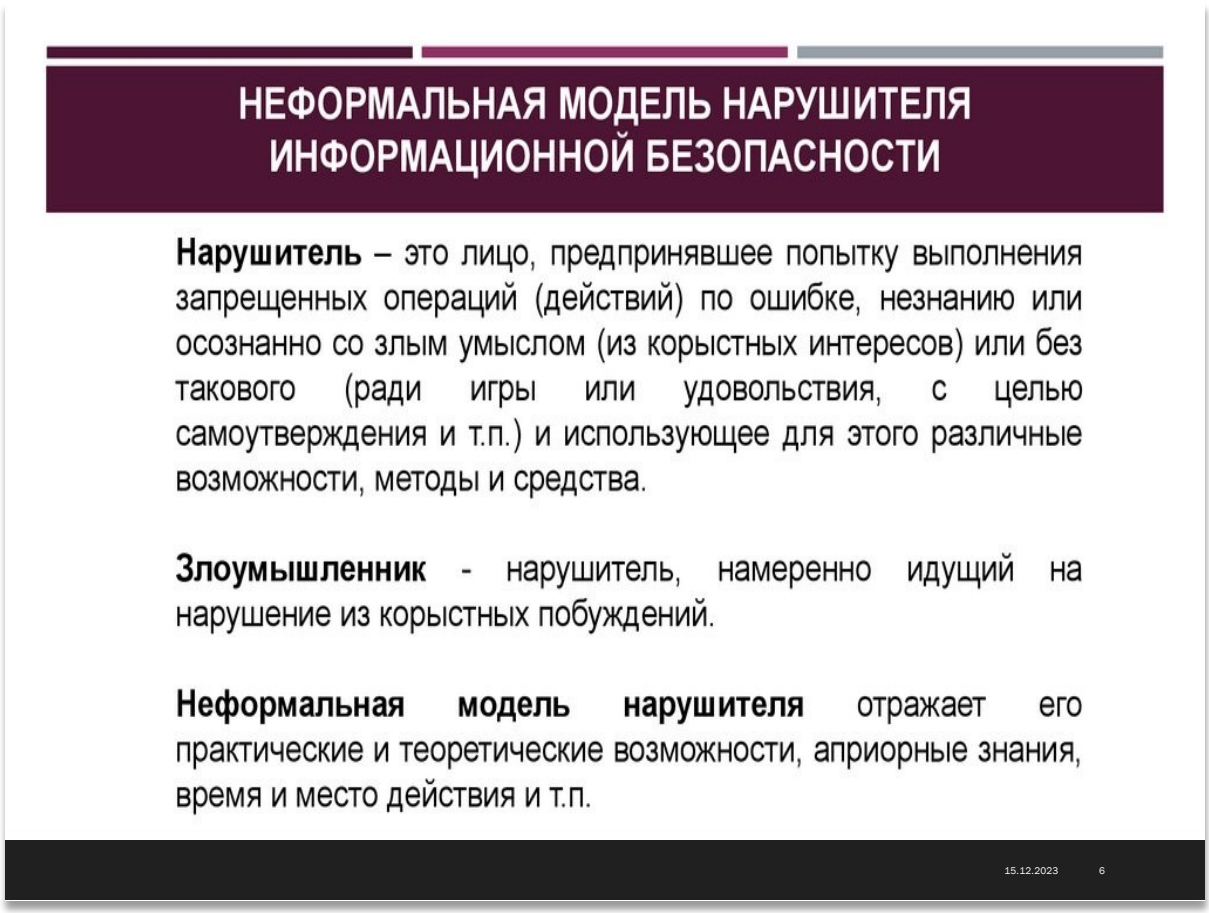
К числу основных методов реализации угроз информационной безопасности относятся :

- определение злоумышленником типа и параметров носителей информации;
- получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;
- получение злоумышленником детальной информации о функциях, выполняемых системой;
- получение злоумышленником данных о применяемых системах защиты;
- определение способа представления информации;
- определение злоумышленником содержания данных, обрабатываемых в системе, на качественном уровне (применяется для мониторинга и для дешифрования сообщений);
- хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные;
- использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН);

- уничтожение средств вычислительной техники и носителей информации;
- несанкционированный доступ пользователя к ресурсам системы в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;
- несанкционированное превышение пользователем своих полномочий;
- несанкционированное копирование программного обеспечения;
- перехват данных, передаваемых по каналам связи;
- визуальное наблюдение;
- раскрытие представления информации (дешифрование данных);
- раскрытие содержания информации на семантическом уровне;
- уничтожение носителей информации;
- внесение пользователем несанкционированных изменений в программно-аппаратные компоненты системы и обрабатываемые данные;
- установка и использование нештатного аппаратного и/или программного обеспечения;
- заражение программными вирусами;
- внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи;
- внедрение дезинформации;
- выведение из строя носителей информации без уничтожения;
- проявление ошибок проектирования и разработки аппаратных и программных компонентов;
- искажение соответствия синтаксических и семантических конструкций языка;
- запрет на использование информации.

Перечисленные методы реализации угроз охватывают все уровни представления информации.

Неформальная модель нарушителя



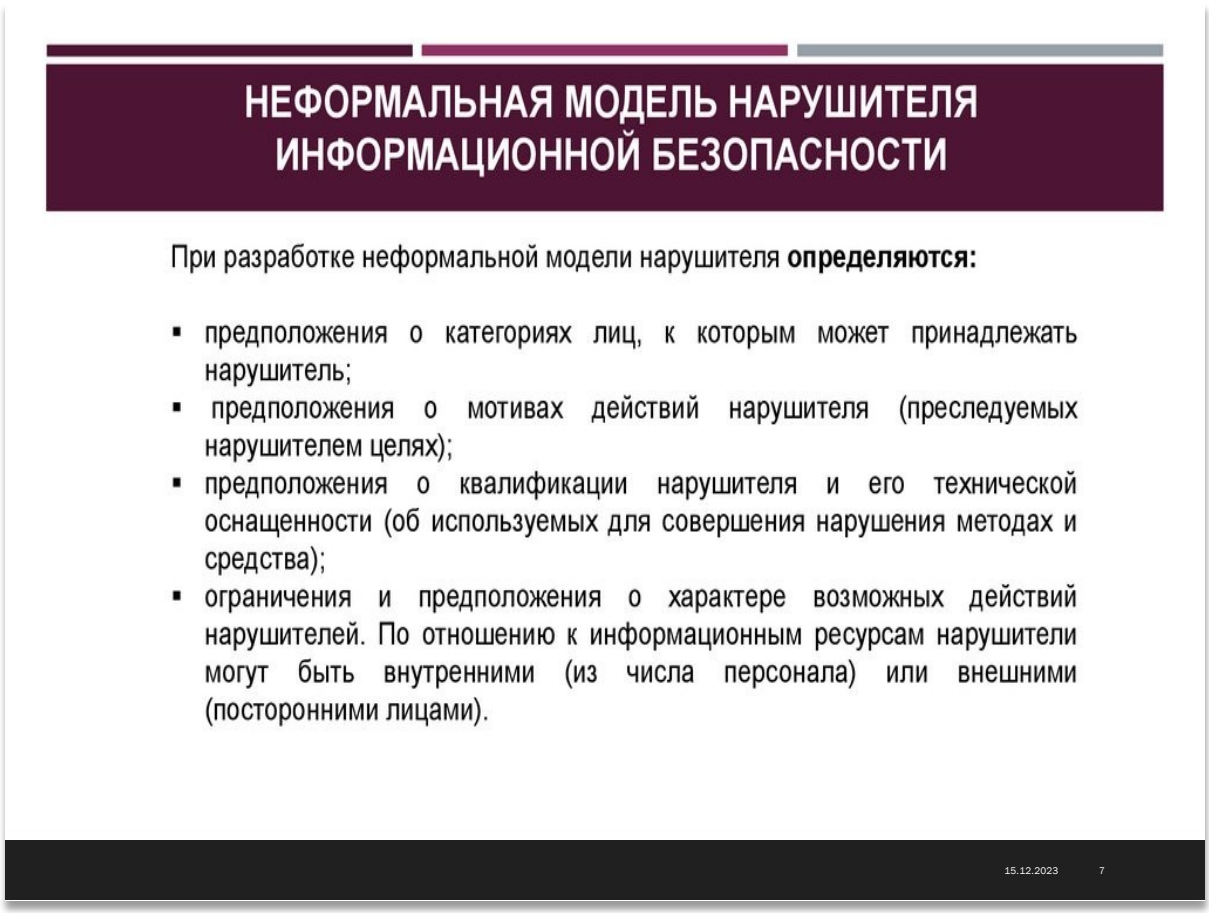
Нарушитель — это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т. п.) и использующее для этого различные возможности, методы и средства.

Злоумышленник — нарушитель, намеренно идущий на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т. п. Исследовав причины нарушений, можно либо повлиять на сами эти причины, либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

В каждом конкретном случае исходя из конкретной технологии обработки информации может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной системы.

Неформальная модель нарушителя разрабатывается при проектировании системы защиты и оценке защищенности информации.



При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителей.

По отношению к системе нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Практика показывает, что на долю внутренних нарушителей приходится более 2/3 от общего числа нарушений.

Внутренним нарушителем может быть лицо из следующих категорий персонала:

- руководители различных уровней должностной иерархии.
- пользователи системы;
- сотрудники отделов разработки и сопровождения программного обеспечения;
- персонал, обслуживающий технические средства;
- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и др.);
- сотрудники службы безопасности.

Посторонние лица, которые могут быть нарушителями:

- посетители;
- клиенты;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т. п.);

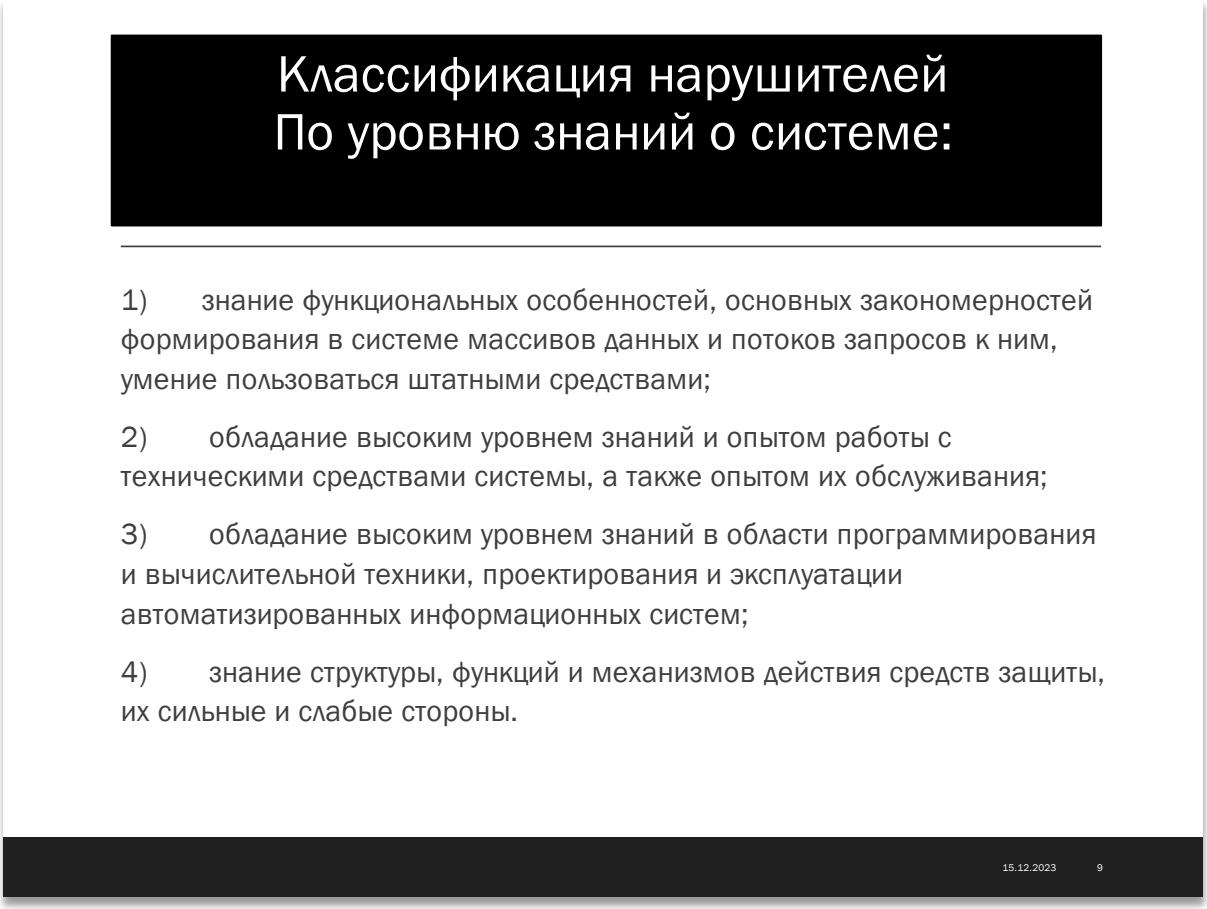
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность);
- любые лица за пределами контролируемой территории.

Можно выделить три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Классификация нарушителей

По уровню знаний о системе:



1) знание функциональных особенностей, основных закономерностей формирования в системе массивов данных и потоков запросов к ним, умение пользоваться штатными средствами;
2) обладание высоким уровнем знаний и опытом работы с техническими средствами системы, а также опытом их обслуживания;

3) обладание высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
4) знание структуры, функций и механизмов действия средств защиты, их сильные и слабые стороны.

По уровню возможностей:

Первый уровень определяет самый низкий уровень возможностей ведения диалога: запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяет возможность создания и запуска собственных программ с новыми функциями по обработке информации.

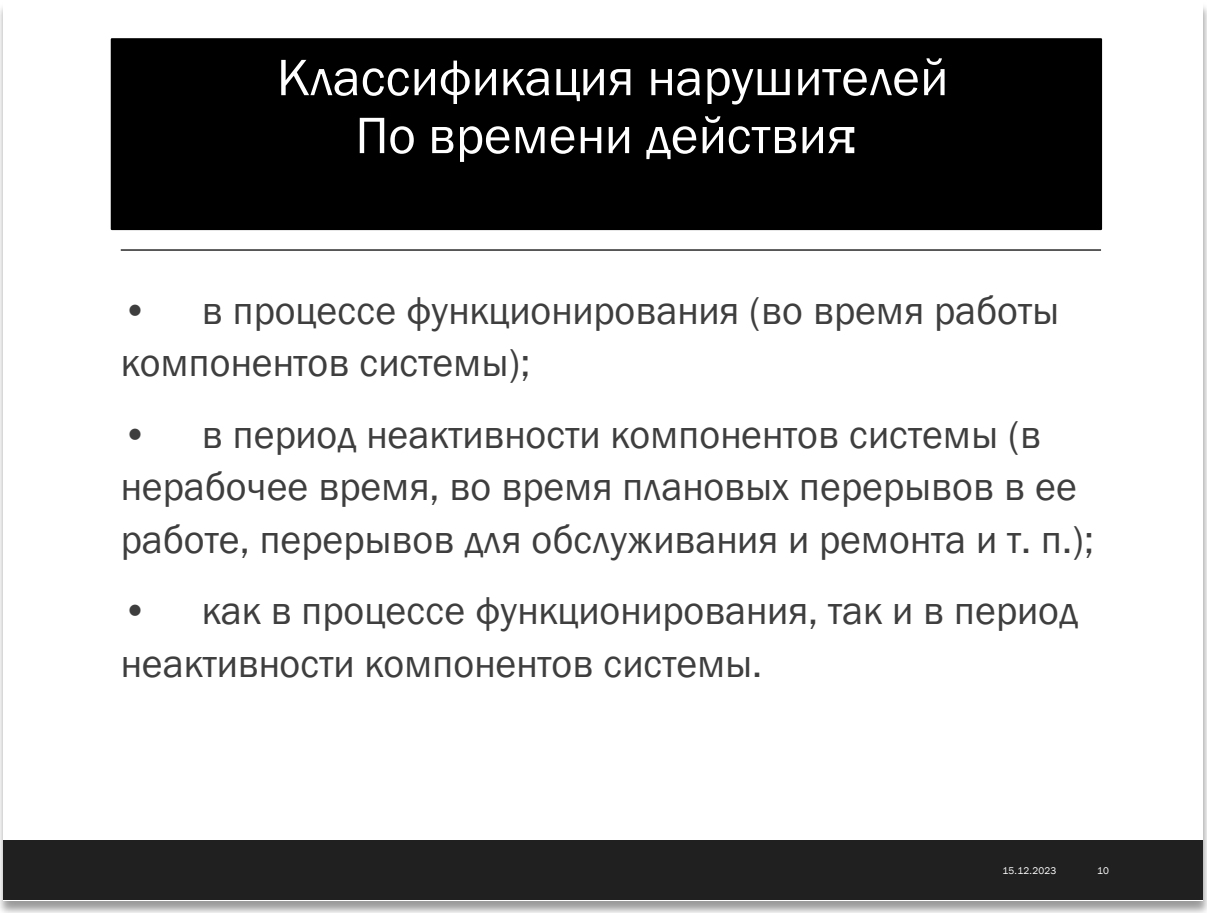
Третий уровень определяет возможность управления функционированием системы, т. е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяет весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств системы, вплоть до включения в состав собственных технических средств с новыми функциями по обработке информации.

Классификация является иерархической, т. е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

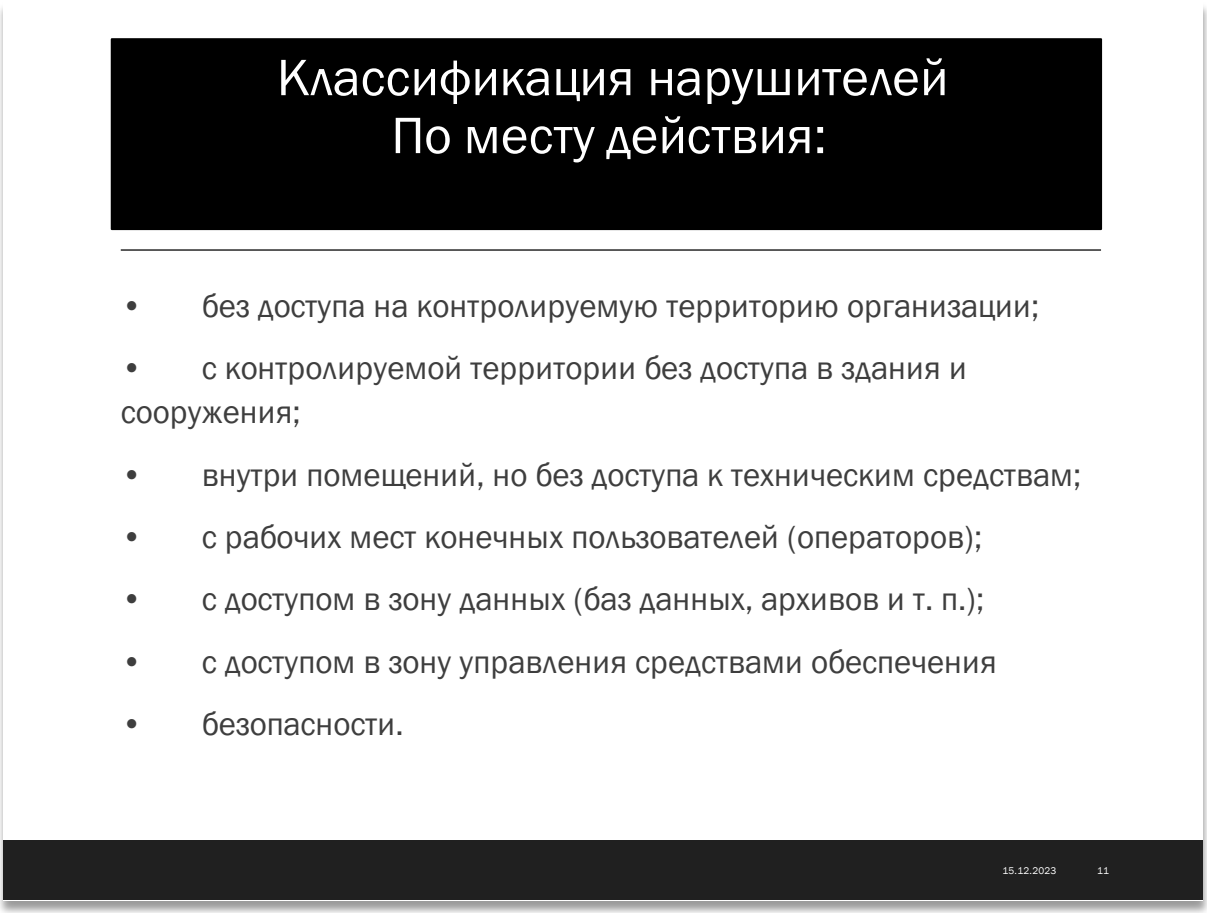
В своем уровне нарушитель является специалистом высшей квалификации, знает все о информационной системе, в частности, о системе и средствах ее защиты.

Классификация по уровню возможностей приводится в руководящем документе Гостехкомиссии «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» в разделе «Модель нарушителя в автоматизированной системе».



По времени действия:

- в процессе функционирования (во время работы компонентов системы);
- в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т. п.);
- как в процессе функционирования, так и в период неактивности компонентов системы.



По месту действия:

- без доступа на контролируемую территорию организации;
- с контролируемой территории без доступа в здания и сооружения;
- внутри помещений, но без доступа к техническим средствам;
- с рабочих мест конечных пользователей (операторов);
- с доступом в зону данных (баз данных, архивов и т. п.);
- с доступом в зону управления средствами обеспечения
- безопасности.

Определение конкретных характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть определен с помощью характеристик, приведенных выше.

Оценка уязвимости системы

При решении практических задач защиты информации большое значение имеет количественная оценка ее уязвимости.

Ряд специалистов в области информационной безопасности разделяют методы и средства защиты от случайных и от преднамеренных угроз.

Для защиты от случайных угроз используются средства повышения надежности функционирования автоматизированных систем, средства повышения достоверности и резервирования информации.

При проектировании защиты от преднамеренных угроз определяются перечень и классификация по характеру, размещению, важности и времени жизни данных, подлежащих защите в заданной информационной системе. В соответствии с характером и важностью этих данных выбираются ожидаемая квалификация и модель поведения потенциального нарушителя.

Рассмотрим ситуацию, когда угроза реализуется путем несанкционированного доступа к информации.

В соответствии с моделью нарушителя в проектируемой системе выявляются виды и количество возможных каналов несанкционированного доступа к защищаемым данным. Данные каналы делятся на технически контролируемые и неконтролируемые. Например, вход в систему со стороны клавиатуры может контролироваться специальной программой, а каналы связи территориально-распределенной системы — не всегда.

На основе анализа каналов выбираются готовые или создаются новые средства защиты с целью перекрытия этих каналов.

Для создания единого постоянно действующего механизма защиты средства защиты с помощью специально выделенных средств централизованного управления объединяются в одну автоматизированную систему безопасности информации, которая путем анализа ее состава и принципов построения проверяется на предмет наличия возможных путей ее обхода. Если таковые обнаруживаются, то они перекрываются соответствующими средствами, которые также включаются в состав защитной оболочки. В результате будет построена замкнутая виртуальная оболочка защиты информации.

Степень защиты определяется полнотой перекрытия каналов утечки информации и возможных путей обхода средств защиты, а также прочностью защиты. Согласно принятой модели поведения нарушителя прочность защитной оболочки определяется средством защиты с наименьшим значением прочности из числа средств, составляющих эту оболочку.

Под прочностью защиты (преграды) понимается величина вероятности ее непреодоления нарушителем.

Прочность защитной преграды является достаточной, если ожидаемое время преодоления ее нарушителем больше времени жизни предмета защиты или больше времени обнаружения и блокировки доступа при отсутствии путей обхода этой преграды.

Защитная оболочка должна состоять из средств защиты, построенных по одному принципу (контроля или предупреждения несанкционированного доступа) и размещаемых на каналах доступа одного типа (технически

контролируемых или неконтролируемых). На контролируемых каналах нарушитель рискует быть пойманным, а на неконтролируемых он может работать в комфортных условиях, не ограниченных временем и средствами. Прочность защиты во втором случае должна быть значительно выше. Поэтому целесообразно в информационной системе иметь отдельные виртуальные защитные оболочки: контролируемую и превентивную.

Кроме того, необходимо учитывать применение организационных мероприятий, которые в совокупности могут образовать свою защитную оболочку.

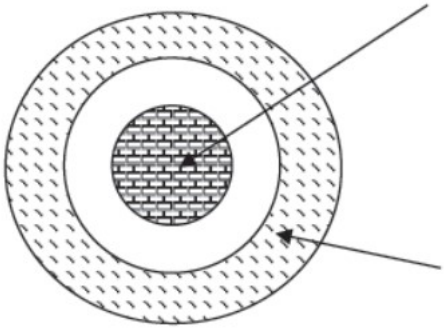
Стратегия и тактика защиты от преднамеренного несанкционированного доступа заключается в применении на возможных каналах доступа к информации средств контроля, блокировки и предупреждения событий. Средства контроля и блокировки устанавливаются на возможных каналах доступа, где это возможно технически или организационно, а средства предупреждения (превентивные средства) применяются там, где такие возможности отсутствуют.

При расчете прочности средства защиты учитывается временной фактор, позволяющий получить количественную оценку его прочности — ожидаемую величину вероятности непреодоления его потенциальным нарушителем.

Рассмотрим варианты построения защитной оболочки и оценку ее прочности.

В простейшем случае предмет защиты помещен в замкнутую однородную защитную оболочку.

Модель однозвенной защиты



Рн + Рп = 1,
где
Рн-вероятность непреодоления
Рн-вероятность преодоления

Рн = min {(1 — Рп), (1 — Ро)}
где Ро –вероятность обхода

Рн = min {(1 — Рп), (1 — Ро1), (1 — Ро2), (1 — Ро3), … (1 — Рok)},
где k — количество путей обхода.

Рн = (1 — Рп) (1 — Ро1) (1 — Ро2) (1 — Ро3) … (1 — Рok)

Прочность защиты зависит от свойств преграды. Считается, что прочность созданной преграды достаточна, если стоимость ожидаемых затрат на ее преодоление потенциальным нарушителем превышает стоимость защищаемой информации.

Если обозначить вероятность непреодоления преграды нарушителем через Рн, вероятность преодоления преграды нарушителем через Рп, то согласно теории вероятности

$Р_н + Р_п = 1.$

В реальном случае у преграды могут быть пути ее обхода.

Обозначим вероятность обхода преграды нарушителем через Ро. Нарушитель, действующий в одиночку, выберет один из путей: преодоление преграды или обходной вариант. Тогда, учитывая несовместность событий, формальное выражение прочности преграды можно представить в виде

$Р_н = \min \{(1 — Р_п), (1 — Р_о)\}.$

Рассмотрим наиболее опасную ситуацию, когда нарушитель знает и выберет путь с наибольшей вероятностью преодоления преграды. В таком случае можно предположить, что прочность преграды определяется вероятностью ее преодоления или обхода потенциальным нарушителем по пути с наибольшим значением этой вероятности. То есть в случае действий

единственного нарушителя прочность защиты определяется ее слабейшим звеном.

У преграды может быть несколько путей обхода. Тогда последнее выражение примет вид

$$Рн = \min \{(1 — Рп), (1 — Ро1), (1 — Ро2), (1 — Ро3), \ldots (1 — Рok)\},$$

где k — количество путей обхода.

Для случая, когда нарушителей более одного и они действуют одновременно (организованная группа) по каждому пути, это выражение с учетом совместности действий будет выглядеть так:

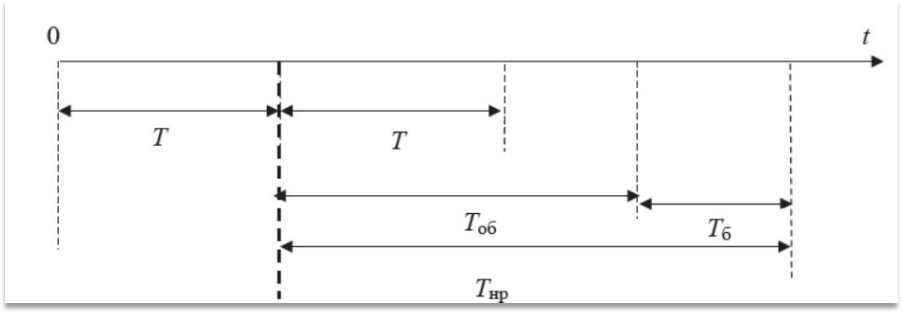
$$Рн = (1 — Рп)\ (1 — Ро1)\ (1 — Ро2)\ (1 — Ро3)\ \ldots\ (1 — Рok).$$

Данная формула применима для неконтролируемой преграды.

Рассмотрим особенности расчета соотношений для контролируемой преграды. Когда к предмету защиты, имеющему постоянную ценность, необходимо и технически возможно обеспечить контроль доступа, обычно применяется постоянно действующая преграда, обладающая свойствами обнаружения и блокировки доступа нарушителя к предмету или объекту защиты.

Для анализа ситуации рассмотрим временную диаграмму процесса контроля и обнаружения несанкционированного доступа, приведенную на слайде.

Временная диаграмма процесса контроля



T — период опроса датчиков; $T_{об}$ — время передачи сигнала и обнаружения НСД; $T_б$ — время блокировки доступа; $T_{нр}$ — время нарушения

Нарушитель может быть не обнаружен в двух случаях:

а) когда время нарушения меньше периода опроса датчиков:Тнр < Т;
б) когда Т < Тнр < Тоб + Тб.

$$P_1 = \begin{cases} \frac{T_{нр}}{T}, T_{нр} < T, \\ 1, T_{нр} \geq T. \end{cases}$$ вероятность обнаружения нарушения

$$P_2 = \frac{T_{нр}}{T_{об} + T_б}.$$ вероятность обнаружения и блокировки доступа

T — период опроса датчиков; $T_{об}$ — время передачи сигнала и обнаружения НСД; $T_б$ — время блокировки доступа; $T_{нр}$ — время нарушения

Из данного рисунка следует, что нарушитель может быть не обнаружен в двух случаях:

а) когда время нарушения меньше периода опроса датчиков: Тнр < Т;

б) когда Т < Тнр < Тоб + Тб.

В случае а) требуется дополнительное условие — попадание интервала времени t в интервал Т, т. е. необходима синхронизация действий нарушителя с частотой опроса датчиков обнаружения.

Формально эту задачу можно представить следующим образом. Есть последовательное множество событий в виде контрольных импульсов с расстоянием Т между ними и есть определенное множество элементарных событий в виде отрезка длиной Тнр, который случайным образом накладывается на первое множество. Задача состоит в определении вероятности попадания отрезка Тнр на контрольный импульс, если Тнр < Т.

Если обозначить вероятность попадания отрезка на контрольный импульс, то есть вероятность обнаружения нарушения, через Р1, то

$$P_1 = \begin{cases} \frac{T_{\text{нр}}}{T}, T_{\text{нр}} < T, \\ 1, T_{\text{нр}} \geq T. \end{cases}$$

В случае б), когда Т < Тнр < Тоб + Т, несанкционированный доступ фиксируется наверняка и вероятность обнаружения действий нарушителя будет определяться соотношением между Тнр и (Тоб + Тб).

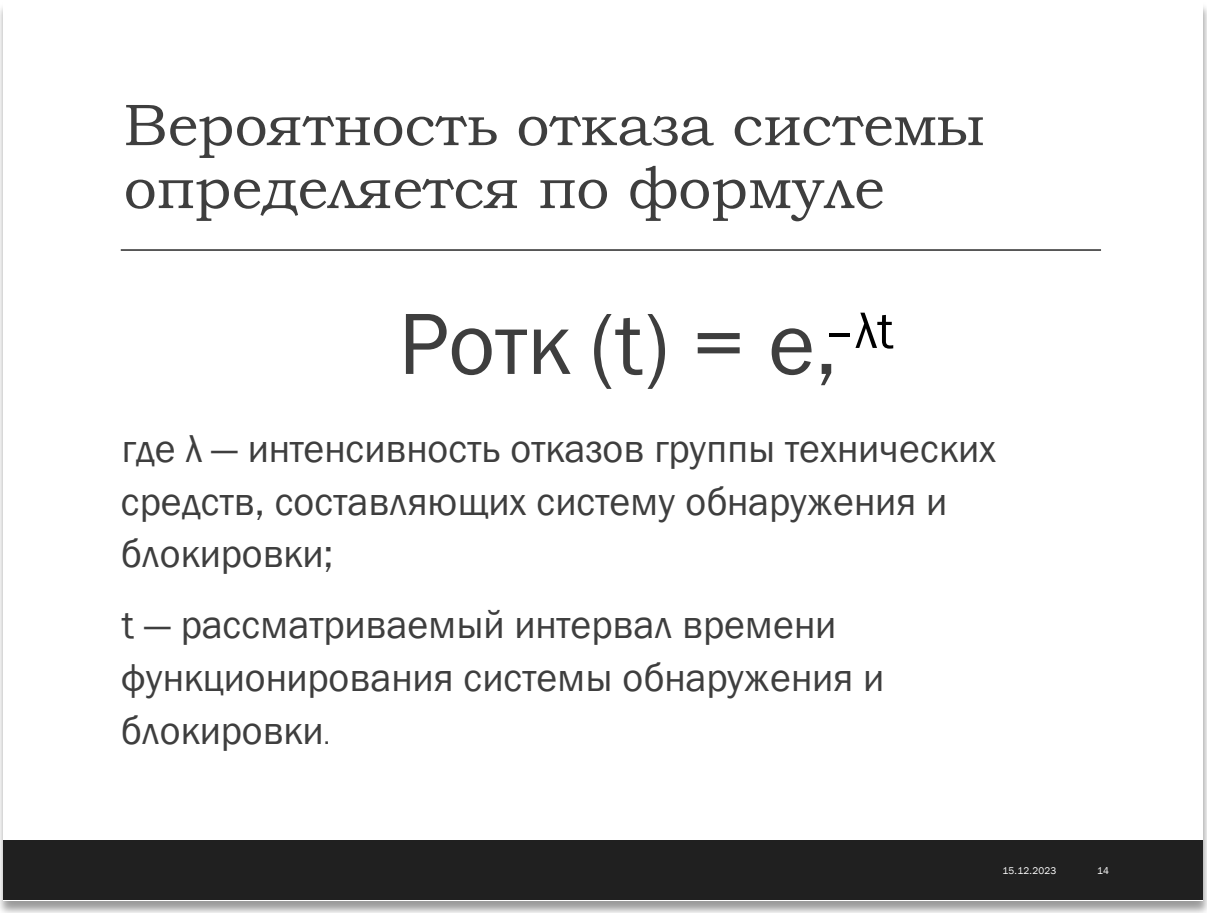
Величина ожидаемого Тнр зависит от многих факторов:

- характера поставленной задачи нарушения,
- метода и способа нарушения,
- технических возможностей и квалификации нарушителя,
- технических возможностей автоматизированной системы.

Поэтому можно говорить о вероятностном характере величины Тнр. Если обозначить вероятность обнаружения и блокировки доступа через Р2, то

$$P_2 = \frac{T_{\text{нр}}}{T_{\text{об}} + T_{\text{б}}}.$$

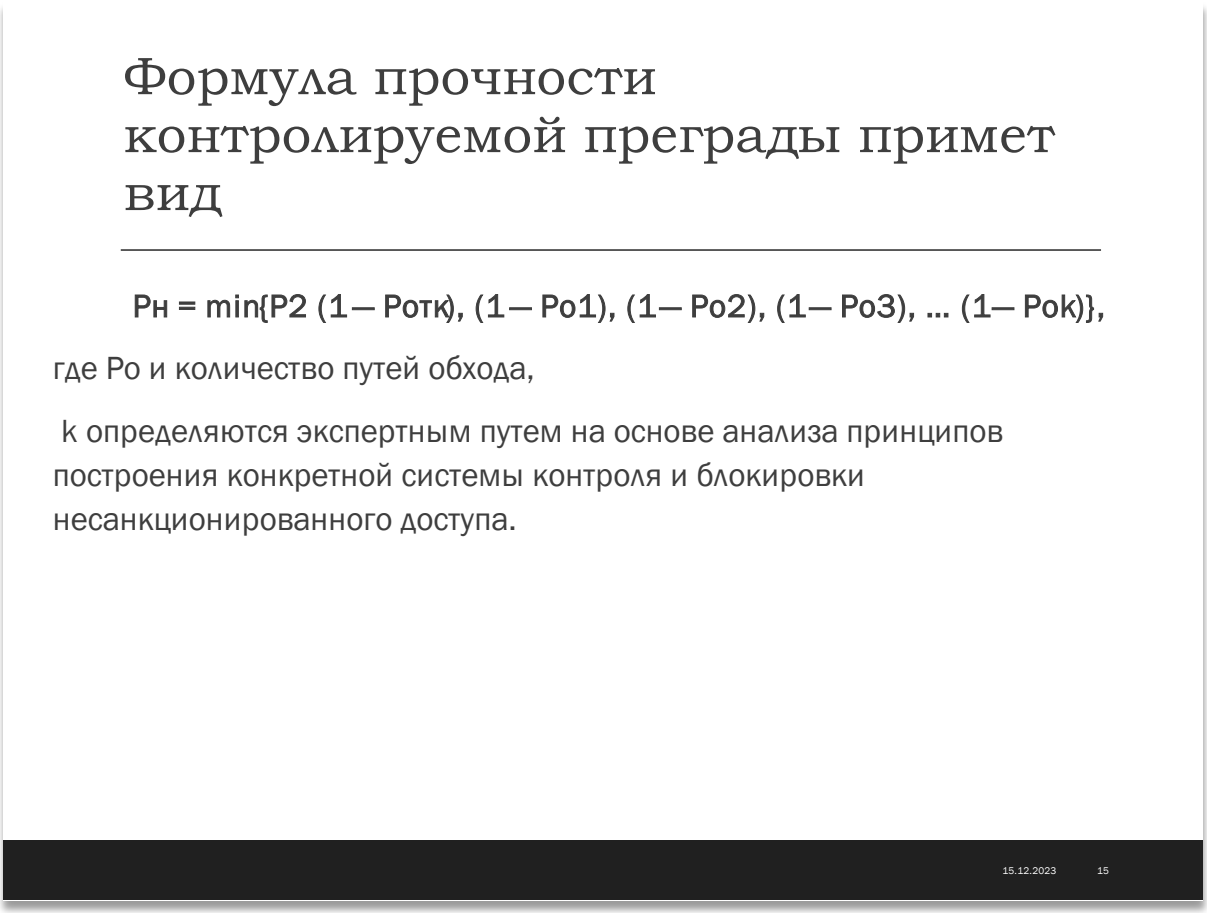
Для более полного формального представления прочности преграды в виде системы обнаружения и блокировки несанкционированного доступа необходимо учитывать надежность ее функционирования и пути возможного обхода ее нарушителем.



Вероятность отказа системы определяется по формуле

$Ротк\ (t) = e^{-\lambda t}$,

где λ — интенсивность отказов группы технических средств, составляющих систему обнаружения и блокировки; t — рассматриваемый интервал времени функционирования системы обнаружения и блокировки.



Исходя из наиболее опасной ситуации, считаем, что отказ системы контроля и НСД могут быть совместными событиями. Поэтому, с учетом этой ситуации формула прочности контролируемой преграды примет вид

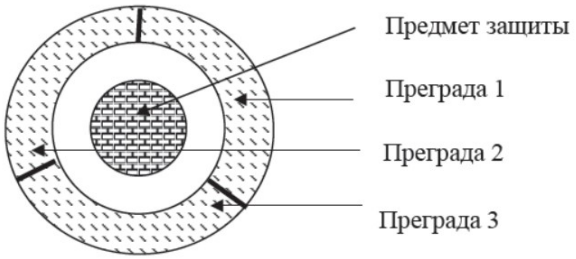
$$Рн = \min\{Р2\ (1 — Ротк), (1 — Ро1), (1 — Ро2), (1 — Ро3), \ldots (1 — Рok)\},$$

где Ро и количество путей обхода k определяются экспертным путем на основе анализа принципов построения конкретной системы контроля и блокировки несанкционированного доступа.

В случае, если ценность информации падает с течением времени, за условие достаточности защиты можно принять превышение затрат времени на преодоление преграды нарушителем над временем жизни информации. В качестве такой защиты может быть использовано криптографическое преобразование информации. Возможными путями обхода криптографической преграды могут быть криптоанализ исходного текста зашифрованного сообщения или доступ к действительным значениям ключей шифрования при хранении и передаче.

На практике в большинстве случаев защитный контур (оболочка) состоит из нескольких соединенных между собой преград с различной прочностью.

Модель многозвенной защиты



Рзи = min{Рсзи1, Рсзи2, Рсзиі, (1 — Ро1), (1 — Ро2), (1 — Ро3), ... (1 — Рok)},
где Рсзиі — прочность і-й преграды;
Рok — вероятность обхода преграды по kму пути.

Прочность многозвенной защиты, построенной из неконтролируемых преград для защиты от организованной группы квалифицированных нарушителей, рассчитывается следующим образом:

Рзи0 = Рсзи1 · Рсзи2 · ..Рсзиі (1 — Ро1) (1 — Ро2) (1 — Ро3) ... (1 — Рok).

Примером такого вида защиты может служить помещение, в котором хранится аппаратура. В качестве преград с различной прочностью здесь могут служить стены, потолок, пол, окна и замок на двери.

Формальное описание прочности многозвенной оболочки защиты почти полностью совпадает с однозвенной, т. к. наличие нескольких путей обхода одной преграды, не удовлетворяющих заданным требованиям, потребует их перекрытия другими преградами, которые в конечном итоге образуют многозвенную оболочку защиты.

Прочность многозвенной защиты из неконтролируемых преград, построенной для противостояния одному нарушителю, определяется по формуле

Рзи = min{Рсзи1, Рсзи2, Рсзиі, (1 — Ро1), (1 — Ро2), (1 — Ро3), … (1 — Рok)},

где Рсзиі — прочность і-й преграды; Рok — вероятность обхода преграды по k-му пути.

Прочность многозвенной защитной оболочки от одного нарушителя равна прочности ее слабейшего звена. Это правило справедливо и для защиты от неорганизованной группы нарушителей, действующих самостоятельно.

Прочность многозвенной защиты, построенной из неконтролируемых преград для защиты от организованной группы квалифицированных нарушителей, рассчитывается следующим образом:

$P_{зи0} = P_{сзи1} \cdot P_{сзи2} \cdot \ldots P_{сзиi} (1 — P_{о1}) (1 — P_{о2}) (1 — P_{о3}) \ldots (1 — P_{ok})$.

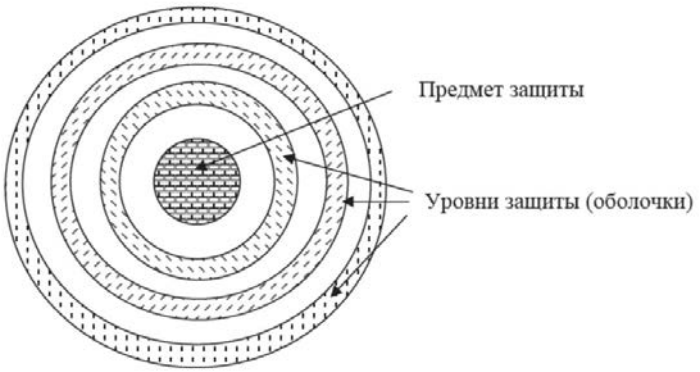
Прочность многозвенной защиты от организованной группы нарушителей равна произведению вероятностей непреодоления потенциальным нарушителем каждого из звеньев, составляющих эту защиту.

Расчет прочности многозвенной защиты с контролируемыми преградами аналогичен.

Расчеты итоговых прочностей защиты для неконтролируемых и контролируемых преград должны быть раздельными, поскольку исходные данные для них различны и, следовательно, на разные задачи должны быть разные решения — две разные оболочки защиты одного уровня.

Если прочность слабейшего звена защиты удовлетворяет предъявленным требованиям оболочки защиты в целом, возникает вопрос об избыточности прочности на остальных звеньях данной оболочки. Отсюда следует, что экономически целесообразно применять в многозвенной оболочке защиты равнопрочные преграды.

Модель многоуровневой защиты



В этом случае, если обозначить прочность дублирующих друг друга преград соответственно через $Р_{д1}$, $Р_{д2}$, $Р_{д3}$, ...$Р_{дi}$, то вероятность преодоления каждой из них определяется как вероятность противоположного события:
$(1 — Р_{д1})$, $(1 — Р_{д2})$, $(1 — Р_{д3})$, ... $(1 — Р_{дi})$.
Считаем, что факты преодоления этих преград нарушителем– события совместные. Это позволяет вероятность преодоления суммарной преграды нарушителем представить в виде
$Р_п = (1 — Р_{д1}) (1 — Р_{д2}) (1 — Р_{д3}) \ldots (1 — Р_{дi})$.

Если звено защиты не удовлетворяет предъявленным требованиям, преграду в этом звене следует заменить на более прочную или данная преграда

дублируется еще одной преградой, а иногда двумя и более. Дополнительные преграды должны перекрывать то же количество или более возможных каналов несанкционированного доступа, что и первая.

В этом случае, если обозначить прочность дублирующих друг друга преград соответственно через $P_{д1}$, $P_{д2}$, $P_{д3}$, …, $P_{дi}$, то вероятность преодоления каждой из них определяется как вероятность противоположного события:

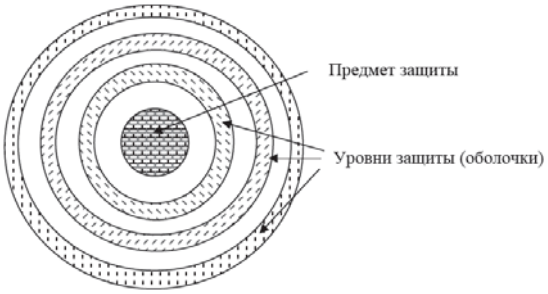
$(1 — P_{д1})$, $(1 — P_{д2})$, $(1 — P_{д3})$, … $(1 — P_{дi})$.

Считаем, что факты преодоления этих преград нарушителем — события совместные. Это позволяет вероятность преодоления суммарной преграды нарушителем представить в виде

$P_{п} = (1 — P_{д1}) (1 — P_{д2}) (1 — P_{д3}) … (1 — P_{дi})$.

В ответственных случаях при повышенных требованиях к защите применяется многоуровневая защита, модель которой представлена на слайде

При расчете суммарной прочности многоуровневой защиты суммируются прочности отдельных уровней.



Выводы

- Система защиты информации должна предусматривать защиту от всех видов случайных и преднамеренных воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.
- Имеется широчайший спектр вариантов путей и методов доступа к данным и вмешательства в процессы обработки и обмена информацией. Анализ всех уязвимостей системы, оценка возможного ущерба позволят верно определить мероприятия по защите информации. Расчет эффективности защитных мероприятий можно производить различными методами в зависимости от свойств защищаемой информации и модели нарушителя.
- Правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и другие характеристики, является важной составляющей успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.