**Основные понятия и проблемы БКС**

**Контрольные вопросы:**

**1 Что понимается под защитой информации в системах и сетях?**

*Защита информации —* это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

*Объект защиты —* информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

*Цель защиты информации —* это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкц*Эффективность защиты информации —* степень соответствия результатов защиты информации поставленной цели.

*Защита информации от утечки —* деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

*Защита информации от разглашения —* деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.ионированного и непреднамеренного воздействия на информацию.

Угрозы безопасности сети

Пути утечки информации и несанкционированного доступа в компьютерных сетях в основной своей массе совпадают с таковыми в автономных системах. Дополнительные возможности возникают за счет существования каналов связи и возможности удаленного доступа к информации. К ним относятся:

\* электромагнитная подсветка линий связи;

\* незаконное подключение к линиям связи;

\* дистанционное преодоление систем защиты;

\* ошибки в коммутации каналов;

\* нарушение работы линий связи и сетевого оборудования.

**2 Дайте определения ИБ КИС**

**ИБ** – защищенность инфы и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, направленных на нанесение ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. **Уровни безопасности:** национальный; отраслевой; корпоративный; персонального. **Субъекты ИБ**: гос. организации; коммерческие структуры; отдельные граждане. **Основные категории ИБ**: *доступность* (возможность за приемлемое время получить требуемую информационную услугу); *целостность* (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения); *конфиденциальность* (защита от несанкционированного ознакомления). **Доступность** - один из важнейших элементов ИБ. ИС создаются или приобретаются для получения определенных информационных услуг (сервисов). Если получение эти услуг пользователями становится невозможным по каким-то причинам, это наносит ущерб всем субъектам информационных отношений. **Целостность** – свойство инфы сохранять свою структуру и/или содержание в процессе передачи и хранения. Целостность инфы обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, то есть если не произошло их случайное или преднамеренное искажение или разрушение. **Конфиденциальность** – свойство инфы быть доступной только ограниченному кругу пользователей ИС, в которой циркулирует данная инфа. Для остальных субъектов системы эта инфа должна быть неизвестной. **Доступом к инфе** – ознакомление с инфой, ее обработка (копирование, модификация или уничтожение инфы). Он бывает: **санкционированный** (доступ к инфе, не нарушающий установленные правила разграничения доступа) и **несанкционированный** (нарушение установленных правил разграничения доступа). **Права доступа** – совокупность правил, регламентирующих порядок и условия доступа субъекта к инфе, её носителям и др. ресурсам ИС, установленных правовыми документами или собственником, владельцем инфы. **Разграничение доступа** – 1. Правила, ограничивающие действия субъектов ИС над её ресурсами; 2. Деятельность по реализации этих правил. **Атака на ИС (сеть)** — это действие, предпринимаемое злоумышленником с целью поиска и использования той или иной уязвимости ИС. **Атака** – реализация угрозы безопасности. **Угроза ИБ** – события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программно-аппаратных средств. **Аудит безопасности ИС** позволяет своевременно выявить существующие недостатки и объективно оценить соответствие обеспечения ИБ требуемому уровню решаемых задач организации. **Защита информации** – деятельность, направленная на сохранение гос., служебной, коммерческой или личной тайны, на сохранение носителей инфы любого содержания.

**3 Приведите классификацию угроз информации**

Классификация угроз информационной безопасности В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы.

Нежелательный контент.

Несанкционированный доступ.

Утечки информации.

Потеря данных.

Мошенничество.

Кибервойны.

Кибертерроризм.

Нежелательный контент — это не только вредоносный код, потенциально опасные программы и спам (т.е. то, что непосредственно создано для уничтожения или кражи информации), но и сайты, запрещенные законодательством, а также нежелательные ресурсы с информацией, не соответствующей возрасту потребителя. Источник: международное исследование EY в области информационной безопасности «Путь к киберустойчивости: прогноз, сопротивление, ответная реакция», 2016 год

Несанкционированный доступ — просмотр информации сотрудником, который не имеет разрешения пользоваться ею, путем превышения должностных полномочий. Несанкционированный доступ приводит к утечке информации. В зависимости от того, каковы данные и где они хранятся, утечки могут организовываться разными способами, а именно через атаки на сайты, взлом программ, перехват данных по сети, использование несанкционированных программ.



Утечки информации можно разделять на умышленные и случайные. Случайные утечки происходят из-за ошибок оборудования, программного обеспечения и персонала. Умышленные, в свою очередь, организовываются преднамеренно с целью получить доступ к данным, нанести ущерб.

Потерю данных можно считать одной из основных угроз информационной безопасности. Нарушение целостности информации может быть вызвано неисправностью оборудования или умышленными действиями людей, будь то сотрудники или злоумышленники.

Не менее опасной угрозой является мошенничество с использованием информационных технологий («фрод»). К мошенничеству можно отнести не только манипуляции с кредитными картами («кардинг») и взлом онлайн-банка, но и внутренний фрод. Целями этих экономических преступлений являются обход законодательства, политики безопасности или нормативных актов, присвоение имущества.

Ежегодно по всему миру возрастает террористическая угроза, постепенно перемещаясь при этом в виртуальное пространство. На сегодняшний день никого не удивляет возможность атак на автоматизированные системы управления технологическими процессами (АСУ ТП) различных предприятий. Но подобные атаки не проводятся без предварительной разведки, для чего применяется кибершпионаж, помогающий собрать необходимые данные. Существует также такое понятие, как «информационная война»; она отличается от обычной войны тем, что в качестве оружия выступает тщательно подготовленная информация.

**4 Какие основные направления и методы реализации угроз Вам известны?**

К основным направлениям реализации угроз информационной безопасности относят:

непосредственное обращение к объекту доступа;

создание программных и технических средств, выполняющих обращение в объекту доступа в обход СЗИ;

модификация СЗИ, позволяющая реализовать угрозы информационной безопасности;

внедрение в технические средства АС программ и технических средств, нарушающих структуру и функции АС.

Основные методы реализации угроз информационной безопасности:

1. Определение злоумышленников типа параметров носителей информации.  
2. Получение злоумышленником информации о программно-аппаратной среде, типе и параметрах СВТ, типе и версии ОС, ППО.  
3. Получение злоумышленником детальной информации о функциях, выполняемых АС.  
4. Получение злоумышленником данных и применяемых СЗИ.  
5. Определение способа представления информации.  
6. Определение злоумышленником содержания данных, обрабатываемых в АС, на качественном уровне (дешифрование).  
7. Хищение (копирование) машинных носителей информации (МНИ), содержащих конфиденциальную информацию.  
8. Использование специальных средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН) - конфиденциальные данные перехватываются злоумышленником путем выделения информационных сигналов их ЭМИН по цепям питания СВТ АС.  
9. уничтожение СВТ и МНИ.  
10. хищение (копирование) МНИ.  
11. НСД пользователя к ресурсам АС в обход или путем преодоления СЗИ с использованием специальных средств, приемов и методов.  
12. Несанкционированное превышение пользователем своих полномочий.  
13. Несанкционированное копирование ПО.  
14. Перехват данных, передаваемых по каналам связи.  
15. Визуальное наблюдение: конфиденциальные данные считываются с экрана монитора, либо распечатанной на принтере информации.  
16. Раскрытие представления информации (дешифрование).  
17. Раскрытие содержания информации на семантическом уровне: доступ к смысловой составляющей информации, хранящейся в АС.  
18. Уничтожение МНИ.  
19. Внесение пользователем несанкционированных изменений в программно-аппаратное обеспечение АС.  
20. Установка нештатного аппаратного и программного обеспечения.  
21. Заражение программами-вирусами.  
22. Внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи.  
23. Внедрение дезинформации.  
24. Выведение из строя МНИ без уничтожения самой информации (например, вывод из строя контроллера HDD).  
25. Проявление ошибок проектирования и разработки программных и аппаратных средств АС (любая программа содержит ошибки).  
26. Обход (отключение) СЗИ.  
27. Искажение соответствия синтаксических и семантических конструкций (смысл имеющейся информации в результате становится непонятен на вербальном (словесном) уровне).  
28. Запрет на использование информации.

**5 Что понимают под информационной системой?**

Информационная система – взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели.

Информационная система представляет собой хранилище информации, снабженное процедурами ввода, поиска, размещения и выдачи информации. Наличие таких процедур – главная особенность информационных систем, отличающих их от простых скоплений информационных материалов.

Информационная система определяется следующими свойствами:

* любая информационная система может быть подвергнута анализу, построена и управляема на основе общих принципов построения систем;
* информационная система является динамичной и развивающейся;
* при построении информационной системы необходимо использовать системный подход;
* выходной продукцией информационной системы является информация, на основе которой принимаются решения;
* информационную систему следует воспринимать как человекокомпьютерную систему обработки информации.

Процессы, обеспечивающие работу информационной системы любого назначения, условно можно представить в виде схемы (Рисунок 1), состоящей из блоков:

* ввод информации из внешних или внутренних источников;
* обработка входной информации и представление ее в удобном виде;
* вывод информации для представления потребителям или передачи в другую систему;
* обратная связь – это информация, переработанная людьми данной организации для коррекции входной информации.

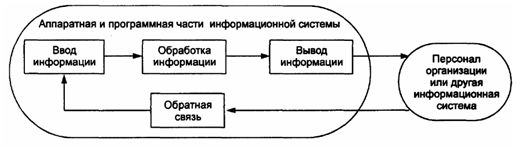


Рисунок 1. Процессы в информационной системе

Работа информационных систем заключается в обслуживании двух встречных потоков информации: ввода новой информации и выдачи текущей информации по запросам. Поскольку главная задача информационной системы:  обслуживание клиентов, система должна быть устроена так, чтобы ответ на любой запрос выдавался быстро и был достаточно полным. Эти требования обеспечиваются наличием стандартных процедур поиска информации и тем, что данные системы расположены в определенном порядке.

**6 Что называют информационными ресурсами?**

Информационные ресурсы - это знания, идеи человечества и указания по их реализации, зафиксированные в любой форме, на любом носителе информации.

Всякий ресурс, кроме информационного, после его использования исчезает. Информационным ресурсом можно пользоваться многократно.

К национальным информационным ресурсам относятся: фонды библиотек и архивов, центры научно-технической информации, отраслевые информационные ресурсы, информационные ресурсы социальной сферы, в том числе сферы образования.

**7 Что составляет основу политики безопасности?**

Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы.

Сегодня лучше всего изучены два вида политики безопасности: избирательная и полномочная (мандатная), основанные соответственно на избирательном и полномочном способах управления доступом.

*Избирательное управление доступом* – метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит. *Мандатное управление доступом* – концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности. Вместе с тем, существует набор требований, усиливающий действие этих политик и предназначенный для управления информационными потоками в системе.

*Избирательная политика безопасности*

Основой избирательной политики безопасности является избирательное управление доступом, ĸᴏᴛᴏᴩᴏᴇ подразумевает, что:

- все субъекты и объекты системы должны быть идентифицированы;

- права доступа субъекта к объекту системы определяются на основании некоторого правила (свойство избирательности).

*Полномочная (мандатная) политика безопасности*

Основу полномочной политик и безопасности составляет полномочное управление доступом, ĸᴏᴛᴏᴩᴏᴇ подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;

- каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

- каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

**8 Проанализируйте механизмы и свойства защиты информации**

Методы обеспечения безопасности информации в ИС:

·   препятствие;

·   управление доступом;

·   механизмы шифрования;

·   противодействие атакам вредоносных программ;

·   регламентация;

·   принуждение;

·   побуждение.

***Препятствие*** – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

***Управление доступом*** – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.

***Механизмы шифрования*** – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

***Противодействие атакам вредоносных программ*** предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования АИС, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС. Овладение этим комплексом мер и средств требует знакомства со специальной литературой.

***Регламентация*** – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

***Принуждение*** – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

***Побуждение***– метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

**9 Дайте понятие объекта защиты информации.**

**Объект защиты информации** - *информация* или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

В соответствии с данным определением можно классифицировать объекты защиты в соответствии с [рисунком 3.1](https://intuit.ru/studies/courses/3649/891/lecture/32324?page=1" \l "image.3.1).



**10 Что относят к информационным процессам?**

К информационным процессам относятся: получение, хранение, поиск, передача, обработка информации.

Хранение – фиксация информации на внешних носителях с помощью условных обозначений.

Поиск – извлечение хранимой информации (ручной и автоматизированный)

Передача – осуществляется от источника к приемнику через канал связи

Обработка – умение делать выводы и получать новую информацию, основываясь на входящую информацию и на запас знаний и опыта

**11 Что понимают под информационной системой?**

**Информационная система** (ИС) — [система](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0" \o "Система), предназначенная для хранения, поиска и обработки [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F" \o "Информация), и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию ([ISO](https://ru.wikipedia.org/wiki/ISO" \o "ISO)/IEC 2382:2015)

ИС предназначена для своевременного обеспечения надлежащих людей надлежащей [информацией](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F" \o "Информация), то есть для удовлетворения конкретных информационных потребностей в рамках определённой [предметной области](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BC%D0%B5%D1%82%D0%BD%D0%B0%D1%8F_%D0%BE%D0%B1%D0%BB%D0%B0%D1%81%D1%82%D1%8C" \o "Предметная область), при этом результатом функционирования информационных систем является *информационная продукция* — документы, информационные массивы, [базы данных](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%B7%D0%B0_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85" \o "База данных) и информационные услуги

Понятие информационной системы интерпретируют по-разному, в зависимости от контекста.

Достаточно широкое понимание информационной системы подразумевает, что её неотъемлемыми компонентами являются [данные](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5" \o "Данные), [техническое](https://ru.wikipedia.org/wiki/%D0%90%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5" \o "Аппаратное обеспечение) и [программное обеспечение](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5" \o "Программное обеспечение), а также [персонал](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB" \o "Персонал) и организационное обеспечение.

ИС в деятельности организации рассматривается как программное обеспечение, реализующее её деловую стратегию и [бизнес-процессы](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%B7%D0%BD%D0%B5%D1%81-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81" \o "Бизнес-процесс).

**12 Что называют информационными ресурсами?**

Информационные ресурсы - это знания, идеи человечества и указания по их реализации, зафиксированные в любой форме, на любом носителе информации.

Всякий ресурс, кроме информационного, после его использования исчезает. Информационным ресурсом можно пользоваться многократно.

К национальным информационным ресурсам относятся: фонды библиотек и архивов, центры научно-технической информации, отраслевые информационные ресурсы, информационные ресурсы социальной сферы, в том числе сферы образования.

**13 Примеры комплексов программно-аппаратных средств и преимущества использования**

Современные комплексы программно-аппаратные (ПАК) позволяют оптимизировать не только отдельные операции, но и целые рабочие процессы, состоящие из множества действий.

Компания Oracle — признанный во всём мире авторитет в вопросах обслуживания баз данных. Начиная с 2008 года компания выпускает Exadata — комплекс аппаратных и программных средств, позволяющих компьютерам и рабочим станциям пользователей одновременный разноуровневый доступ к определённой информации. Отличительной особенностью Exadata является применение ячеек — отдельных автономных серверов, что позволяет быстрее обрабатывать запросы с большим объёмом информации. Среди других готовых решений от Oracle существует ПАК для быстрого развёртывания системы — Database Appliance, специально предназначенный для минимизирования затрат и времени на установку и настройку необходимого ПО. Также есть комплексы для использования облачных технологий (Private Cloud Appliance), для хранения большого объёма информации (Big Data Appliance) и даже для защиты целостности данных (Zero Data Loss Recovery Appliance).

Применение шаговых двигателей позволяет выполнять производственные задания с точностью, недоступной человеческим рукам. Оснащение производственных аппаратов встроенными компьютерами — это и есть применение специализированных ПАК. Принцип действия таких комплексов довольно прост: квалифицированный рабочий задаёт схему изделия, используя встроенное программное обеспечение, после чего станок выполняет заданное количество запланированных действий.