**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 несанкционированного и непреднамеренного воздействия на информацию.

**2. Дайте определения ИБ КИС**

**Информационная безопасность (ИБ)** — практика предотвращения [несанкционированного доступа](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF), использования, раскрытия, искажения, изменения, исследования, записи или уничтожения [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).

**Корпоративная Информационная Система** (**КИС**) — это масштабируемая система, предназначенная для комплексной автоматизации всех видов хозяйственной деятельности компаний, а также корпораций, требующих единого управления.

**3. Приведите классификацию угроз информации**

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.

**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 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 АС программных или технических механизмов, нарушающих предполагаемую структуру и функции АС

**5. 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), 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), и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

**6. Что называют информационными ресурсами?**

**Информационный ресурс** — [данные](https://dic.academic.ru/dic.nsf/ruwiki/71919) в любом виде, которые можно многократно использовать для решения проблем пользователей. Например, это может быть [файл](https://dic.academic.ru/dic.nsf/ruwiki/6904), [документ](https://dic.academic.ru/dic.nsf/ruwiki/15385), [веб-сайт](https://dic.academic.ru/dic.nsf/ruwiki/23679), [фотография](https://dic.academic.ru/dic.nsf/ruwiki/1227), [видеофрагмент](https://dic.academic.ru/dic.nsf/ruwiki/117701). Для информационных ресурсов в [Интернете](https://dic.academic.ru/dic.nsf/ruwiki/189) характерно определённое время жизни и доступность более, чем одному пользователю.

**7. Что составляет основу политики безопасности?**

Существуют два типа политики безопасности: **дискреционная** и **мандатная**.

Основой **дискреционной (дискретной) политики безопасности** является дискреционное управление доступом ( Descretionary Access Control - DAC ), которое определяется двумя свойствами:

* все субъекты и объекты должны быть идентифицированы
* права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила

Основу **мандатной ( полномочной ) политики безопасности** составляет мандатное управление доступом ( Mandatory Access Control - MAC ), которое подразумевает, что:

* все субъекты и объекты системы должны быть однозначно идентифицированы
* задан линейно упорядоченный набор меток секретности
* каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации - его уровень секретности в АС
* каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в АС - максимальное значение метки секретности объектов, к которым субъект имеет доступ; метка секретности субъекта называется его уровнем доступа

Основная цель мандатной политики безопасности - предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа, т.е. противодействие возникновению в АС информационных каналов сверху вниз.

**8. Проанализируйте механизмы и свойства защиты информации**

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

**10. Что относят к информационным процессам?**

**Поиск.**   
**Поиск информации -** это извлечение хранимой информации.

**Сбор и хранение.**   
Сбор информации не является самоцелью. Чтобы полученная информация могла использоваться, причем многократно, необходимо ее хранить.   
**Хранение информации -** это способ распространения информации в пространстве и времени.

**Передача.**   
В процессе передачи информации обязательно участвуют источник и приемник информации: первый передает информацию, второй ее получает. Между ними действует канал передачи информации - канал связи.

**Обработка.**   
Обработка информации - преобразование информации из одного вида в другой, осуществляемое по строгим формальным правилам.

**Использование.**   
Информация используется при принятии решений.

**Защита.**

**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), 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), и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

**12. Что называют информационными ресурсами?**

**Информационный ресурс** — [данные](https://dic.academic.ru/dic.nsf/ruwiki/71919) в любом виде, которые можно многократно использовать для решения проблем пользователей. Например, это может быть [файл](https://dic.academic.ru/dic.nsf/ruwiki/6904), [документ](https://dic.academic.ru/dic.nsf/ruwiki/15385), [веб-сайт](https://dic.academic.ru/dic.nsf/ruwiki/23679), [фотография](https://dic.academic.ru/dic.nsf/ruwiki/1227), [видеофрагмент](https://dic.academic.ru/dic.nsf/ruwiki/117701). Для информационных ресурсов в [Интернете](https://dic.academic.ru/dic.nsf/ruwiki/189) характерно определённое время жизни и доступность более, чем одному пользователю.

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

**Программно-аппаратный комплекс** — это набор технических и программных средств, работающих совместно для выполнения одной или нескольких сходных задач.

Состоит, соответственно, из двух основных частей:

* [Аппаратная часть](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) ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) hardware) — устройство сбора и обработки информации например [компьютер](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80), [плата видеозахвата](https://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D1%82%D0%B0_%D0%B2%D0%B8%D0%B4%D0%B5%D0%BE%D0%B7%D0%B0%D1%85%D0%B2%D0%B0%D1%82%D0%B0), [биометрический детектор](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8), [калибратор](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BB%D0%B8%D0%B1%D1%80%D0%B0%D1%82%D0%BE%D1%80) и т. п.
* [Программная часть](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) ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) software) — специализированное программное обеспечение (как правило, написанное компанией-производителем аппаратной части), обрабатывающее и интерпретирующее [данные](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5), собранные аппаратной частью. Например: [встроенное программное обеспечение](https://ru.wikipedia.org/wiki/%D0%92%D1%81%D1%82%D1%80%D0%BE%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BF%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), [операционная система](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0).

**Программно-аппаратный комплекс (ПАК) "Омега"**

**Назначение:**

унифицированный программно-аппаратный комплекс (ПАК) "Омега" предназначен для построения на его основе рабочих мест, локальных вычислительных сетей и распределенных автоматизированных систем, обрабатывающих информацию ограниченного распространения, в том числе мультисервисных систем связи (МСС); также ПАК "Омега" предназначен для управления телекоммуникационными сетями, построенными с использованием различных оборудования и технологий.

**Преимущества:**

* реализация комплексного подхода к решению вопросов информационной безопасности;
* возможность различной комплектации, учитывающей требования потребителей (от рабочих мест до распределенных автоматизированных систем);
* наличие в составе комплекса проверенных на совместимость аппаратных и программных средств;
* ПО, реализующее функционал управления телекоммуникационными сетями, построено с использованием модульной архитектуры, имеет упрощенный интерфейс для добавления модулей управления оборудованием без остановки всей системы, сочетает в себе все преимущества традиционных систем управления и контроллеров для программно-конфигурируемых сетей.