33 вопрос

Информационная безопасность – это защита информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб ее владельцу или пользователю.

Основныепринципыинформационнойбезопасности

1. **Целостность данных** - такое свойство, в соответствии с которым информация сохраняет свое содержание и структуру в процессе ее передачи и хранения. Создавать, уничтожать или изменять данные может только пользователь, имеющий право доступа.
2. **Конфиденциальность** — свойство, которое указывает на необходимость ограничения доступа к конкретной информации для обозначенного круга лиц. Таким образом, конфиденциальность дает гарантию того, что в процессе передачи данных, они могут быть известны только авторизованным пользователям
3. **Доступность информации** - это свойство характеризует способность обеспечивать своевременный и беспрепятственный доступ полноправных пользователей к требуемой информации.
4. **Достоверность** – данный принцип выражается в строгой принадлежности информации субъекту, который является ее источником или от которого она принята.

Задача обеспечения информационной безопасности подразумевает реализацию многоплановых и комплексных мер по предотвращению и отслеживанию несанкционированного доступа неавторизованных лиц, а также действий, предупреждающих неправомерное использование, повреждение, искажение, копирование, блокирование информации.

Вопросы информационной безопасности становятся первоочередными в тех случаях, когда выход из строя или возникновение ошибки в конкретной компьютерной системе могут привести к тяжелым последствиям.

34 вопрос

Под угрозой информационной безопасности принято понимать потенциально возможные действия, явления или процессы, способные оказать нежелательное воздействие на систему или на хранящуюся в ней информацию.

Такие угрозы, воздействуя на ресурсы, могут привести к искажению данных, копированию, несанкционированному распространению, ограничению или блокированию к ним доступа. В настоящее время известно достаточно большое количество угроз, которые классифицируют по различным признакам.

По природе возникновения различают **естественные** и **искусственные** угрозы. К первой группе относятся те, что вызваны воздействием на компьютерную систему объективных физических процессов или стихийных природных явлений. Вторая группа – те угрозы, которые обусловлены деятельностью человека.

По степени преднамеренности проявления**,** угрозы разделяют на **случайные** и**преднамеренные**.

Также есть разделение в **зависимости от их непосредственного источника**, в качестве которого может выступать природная среда (например, стихийные бедствия), человек (разглашение конфиденциальных данных), программно-аппаратные средства: санкционированные (ошибка в работе операционной системы) и несанкционированные (заражение системы вирусами).

Источник угроз может иметь разное положение. В зависимости от этого фактора также выделяют **три группы**:

- *Угрозы, источник которых находятся вне контролируемой группы компьютерной системы (пример – перехват данных, передаваемых по каналам связи)*
- *Угрозы, источник которых – в пределах контролируемой зоны системы (это может быть хищение носителей информации)*
- *Угрозы, находящиеся непосредственно в самой системе (например, некорректное использование ресурсов).*

Угрозы способны по-разному воздействовать на компьютерную систему. Это могут быть**пассивные воздействия**, реализация которых не влечет за собой изменение структуры данных (например, копирование). **Активные угрозы** — это такие, которые, наоборот, меняют структуру и содержание компьютерной системы (внедрение специальных программ).

В соответствии с разделением угроз **по этапам доступа пользователей или программ к ресурсам системы** существуют такие опасности, которые проявляются на этапе доступа к компьютеру и обнаружимые после разрешения доступа (несанкционированное использование ресурсов).

Классификация **по месту расположения в системе** подразумевает деление на три группы: угрозы доступа к информации, находящейся на внешних запоминающих устройствах, в оперативной памяти и к той, что циркулирует в линиях связи.

Угрозы могут использовать прямой стандартный путь к ресурсам с помощью незаконно полученных паролей или посредством неправомерного применения терминалов законных пользователей, а могут «обойти» существующие средства защиты иным путем.

Такие действия, как хищение информации, относят к угрозам, проявляющимся независимо от активности системы. А, например, распространение вирусов может быть обнаружено исключительно в процессе обработки данных.

Случайными, или **непреднамеренными** называются такие угрозы, которые не связаны с действиями злоумышленников. Механизм их реализации изучен достаточно хорошо, поэтому существуют разработанные методы противодействия.

Аварии и стихийные бедствия представляют особую опасность для компьютерных систем, так как они влекут за собой наиболее негативные последствия. Вследствие физического разрушения систем информация становится недоступной, либо утрачивается. Кроме того, невозможно полностью избежать или предупредить сбои и отказы в сложных системах, в результате которых, как правило, хранящаяся на них информация искажается или уничтожается, нарушается алгоритм работы технических устройств.

Ошибки, которые могут быть допущены в процессе разработки компьютерной системы, включая неверные алгоритмы работы и некорректное программное обеспечение, способны привести к последствиям, которые аналогичны тем, что происходят при сбое и отказе в работе технических средств. Более того, подобные ошибки могут использоваться злоумышленниками в целях воздействия на ресурсы системы.

Ошибки пользователей приводят к ослаблению информационной безопасности в 65 % случаев. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками на предприятиях приводит к уничтожению, нарушению целостности и конфиденциальности информации.

Выделяют также **преднамеренные угрозы**, которые связаны с целенаправленными действиями нарушителя. Изучение этого класса затруднено, так как он имеет очень динамичный характер и постоянно пополняется новыми видами угроз.

Для проникновения в компьютерную систему с целью дальнейшего хищения или уничтожения информации используются такие методы и средства шпионажа, как прослушивание, хищение программ, атрибутов защиты, документов и носителей информации, визуальное наблюдение и другие.

При несанкционированном доступе к данным обычно используют штатные аппаратные и программные средства компьютерных систем, вследствие чего нарушаются установленные правила разграничения доступа пользователей или процессов к информационным ресурсам. Самые распространенные нарушения – это перехват паролей (производится с помощью специально разработанных программ), выполнение каких-либо действий под именем другого человека, а также использование злоумышленником привилегий законных пользователей.

35 вопрос

При разработке методов защиты информации в информационной среде следует учесть следующие важные факторы и условия:

- расширение областей использования компьютеров и увеличение темпа роста компьютерного парка (то есть проблема защиты информации должна решаться на уровне технических средств);
- высокая степень концентрации информации в центрах ее обработки и, как следствие, появление централизованных баз данных, предназначенных для коллективного пользования;
- расширение доступа пользователя к мировым информационным ресурсам (современные системы обработки данных могут обслуживать неограниченное число абонентов, удаленных на сотни и тысячи километров);
- усложнение программного обеспечения вычислительного процесса на компьютере.

При таких режимах работы в памяти компьютера одновременно могут находиться программы и массивы данных различных пользователей, что делает актуальным сохранение информации от нежелательных воздействий, ее физическую защиту.

К традиционным методам защиты от преднамеренных информационных угроз относятся: ограничение доступа к информации, шифрование (криптография) информации, контроль доступа к аппаратуре, законодательные меры. Рассмотрим эти методы.

Ограничение доступа к информации осуществляется на двух уровнях:

- на уровне среды обитания человека, то есть путем создания искусственной преграды вокруг объекта защиты: выдачи допущенным лицам специальных пропусков, установки охранной сигнализации или системы видеонаблюдения;
- на уровне защиты компьютерных систем, например, с помощью разделения информации, циркулирующей в компьютерной системе, на части и организации доступа к ней лиц в соответствии с их функциональными обязанностями. При защите на программном уровне каждый пользователь имеет пароль, позволяющий ему иметь доступ только к той информации, к которой он допущен.

Шифрование (криптография) информации заключается в преобразовании (кодировании) слов, букв, слогов, цифр с помощью специальных алгоритмов. Для ознакомления с шифрованной информацией нужен обратный процесс — декодирование. Шифрование обеспечивает существенное повышение безопасности передачи данных в сети, а также данных, хранящихся на удаленных устройствах.

Контроль доступа к аппаратуре означает, что вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры. Подобные меры позволяют избежать, например, подключения посторонних устройств, изменения режимов работы компьютерной системы, загрузки посторонних программ и т. п.

Законодательные меры заключаются в исполнении существующих в стране законов, постановлений, инструкций, регулирующих юридическую ответственность должностных лиц — пользователей и обслуживающего персонала за утечку, потерю или модификацию доверенной им информации.

При выборе методов защиты информации для конкретной компьютерной сети необходим тщательный анализ всех возможных способов несанкционированного доступа к информации. По результатам анализа проводится планирование мер, обеспечивающих необходимую защиту, то есть осуществляется разработка политики безопасности.

Вопрос 36

Конституция РФ является основным источником права в области обеспечения информационной безопасности в России.
Согласно Конституции РФ:
каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23);
сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (статья 24);
каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом (статья 29);
каждый имеет право на достоверную информацию о состоянии окружающей среды (статья 42).
Основополагающим законодательным актом в России, регулирующим отношения в информационной сфере (в том числе связанные с защитой информации), является Федеральный закон «Об информации, информатизации и защите информации», принятый в 1995 году.
Предметом регулирования данного Закона являются общественные отношения, возникающие в трех взаимосвязанных направлениях:
формирование и использование информационных ресурсов;
создание и использование информационных технологий и средств их обеспечения;
защита информации, прав субъектов, участвующих в информационных процессах и информатизации.
В Законе даны определения важнейших терминов в информационной сфере. Согласно статье 2 Закона , информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
Одним из существенных достижений Закона является разграничение информационных ресурсов по категориям доступа.
Согласно Закону, документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.
В Законе также отражены вопросы, связанные с порядком обращения с персональными данными, сертификацией информационных систем, технологий, средств их обеспечения и лицензированием деятельности по формированию и использованию информационных ресурсов.
Глава 5 Закона «Защита информации и прав субъектов в области информационных процессов и информатизации» является «базовой» для российского законодательства в области защиты информации.
Основными целями защиты информации являются:
предотвращение утечки, хищения, утраты, искажения и подделки информации (защите подлежит любая информация, в том числе и открытая);
предотвращение угроз безопасности личности, общества и государства (то есть защита информации является одним из способов обеспечения информационной безопасности РФ);
защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством.