**Технологии защиты информации. Основные понятия о защите информации. Безопасность передачи данных.**

Наряду с позитивным влиянием на все стороны человеческой деятельности широкое внедрение информационных технологий привело к появлению новых угроз безопасности людей. Это связано с тем обстоятельством, что информация, создаваемая, хранимая и обрабатываемая средствами вычислительной техники, стала определять действия большей части людей и технических систем. В связи с этим резко возросли возможности нанесения ущерба, связанные с хищением информации, так как воздействовать на любую систему (социальную, биологическую или техническую) с целью ее уничтожения, снижения эффективности функционирования или воровства ее ресурсов (денег, товаров, оборудования) возможно только в том случае, когда известна информация о ее структуре и принципах функционирования.

Все виды информационных угроз можно разделить на две большие группы:

• отказы и нарушения работоспособности программных и технических средств;

• преднамеренные угрозы, заранее планируемые злоумышленниками для нанесения вреда.

Выделяют следующие основные группы причин сбоев и отказов в работе компьютерных систем:

• нарушения физической и логической целостности хранящихся в оперативной и внешней памяти структур данных, возникающие по причине старения или преждевременного износа их носителей;

• нарушения, возникающие в работе аппаратных средств из-за их старения или преждевременного износа;

• нарушения физической и логической целостности хранящихся в оперативной и внешней памяти структур данных, возникающие по причине некорректного использования компьютерных ресурсов;

• нарушения, возникающие в работе аппаратных средств из-за неправильного использования или повреждения, в том числе из-за неправильного использования программных средств;

• неустраненные ошибки в программных средствах, не выявленные в процессе отладки и испытаний, а также оставшиеся в аппаратных средствах после их разработки.

Помимо естественных способов выявления и своевременного устранения указанных выше причин, используют следующие специальные способы защиты информации от нарушений работоспособности компьютерных систем:

• внесение структурной, временной, информационной и функциональной избыточности компьютерных ресурсов;

• защиту от некорректного использования ресурсов компьютерной системы;

• выявление и своевременное устранение ошибок на этапах разработки программно-аппаратных средств.

Основным видом угроз целостности и конфиденциальности информации являются преднамеренные угрозы, заранее планируемые злоумышленниками для нанесения вреда. Их можно разделить на две группы:

• угрозы, реализация которых выполняется при постоянном участии человека;

• угрозы, реализация которых после разработки злоумышленником соответствующих компьютерных программ выполняется этими программами без непосредственного участия человека.

Задачи по защите от угроз каждого вида одинаковы:

• запрещение несанкционированного доступа к ресурсам вычислительных систем;

• невозможность несанкционированного использования компьютерных ресурсов при осуществлении доступа;

• своевременное обнаружение факта несанкционированных действий, устранение их причин и последствий.

Основным способом запрещения несанкционированного доступа к ресурсам вычислительных систем является подтверждение подлинности пользователей и разграничение их доступа к информационным ресурсам, включающего следующие этапы:

• идентификация;

• установление подлинности (аутентификация);

• определение полномочий для последующего контроля и разграничения доступа к компьютерным ресурсам.

Одной из основных угроз хищения информации является угроза доступа к остаточным данным в оперативной и внешней памяти компьютера. Под остаточной информацией понимают данные, оставшиеся в освободившихся участках оперативной и внешней памяти после удаления файлов пользователя, удаления временных файлов без ведома пользователя, находящиеся в неиспользуемых хвостовых частях последних кластеров, занимаемых файлами, а также в кластерах, освобожденных после уменьшения размеров файлов и после форматирования дисков.

Основным способом защиты от доступа к конфиденциальным остаточным данным является своевременное уничтожение данных во всех областях памяти компьютера.

Уничтожение остаточных данных может быть реализовано либо средствами операционных сред, либо с помощью специализированных программ. защиты) Подсистема защиты от компьютерных вирусов, является одним из основных компонентов системы защиты информации и процесса ее обработки в вычислительных системах.

Выделяют три уровня защиты от компьютерных вирусов:

• защита от проникновения в вычислительную систему вирусов известных типов;

• углубленный анализ на наличие вирусов известных и неизвестных типов, преодолевших первый уровень защиты;

• защита от деструктивных действий и размножения вирусов, преодолевших первые два уровня.

Поиск и обезвреживание вирусов осуществляются как автономными антивирусными программными средствами (сканеры), так и в рамках комплексных систем защиты информации.

Безопасность информации при сетевом обмене данными требует также обеспечения их конфиденциальности и подлинности. Защита информации в процессе передачи достигается на основе зашиты каналов передачи данных, а также криптографического закрытия передаваемых сообщений. В идеальном случае защита каналов передачи данных должна обеспечивать их защиту как от нарушений работоспособности, так и несанкционированных действий (например, подключения к линиям связи). По причине большой протяженности каналов связи, а также возможной доступности их отдельных участков (например, при беспроводной связи) защита каналов передачи данных от несанкционированных действий экономически неэффективна, а в ряде случаев невозможна. Поэтому реально защита каналов передачи данных строится на основе защиты нарушений их работоспособности.