Защита информации и информационная безопасность

Определения

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

Информационная безопасность — это состояние (качество) определённого объекта (в качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства и т. п.) и/или деятельность, направленная на обеспечение защищённого состояния объекта (в этом значении чаще используется термин «защита информации»).

Безопастность информационной защиты и источники угроз

Безопасность информационной системы - это свойство, заключающее в способности системы обеспечить ее нормальное функционирование, то есть обеспечить целостность и секретность информации. Для обеспечения целостности и конфиденциальности информации необходимо обеспечить защиту информации от случайного уничтожения или несанкционированного доступа к ней.

Известны следующие источники угроз безопасности информационных систем:

антропогенные источники, вызванные случайными или преднамеренными действиями субъектов;

техногенные источники, приводящие к отказам и сбоям технических и программных средств из-за устаревших программных и аппаратных средств или ошибок в ПО

стихийные источники, вызванные природными катаклизмами или форс-мажорными обстоятельствами.

В свою очередь антропогенные источники угроз делятся:

на внутренние (воздействия со стороны сотрудников компании) и внешние (несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения) источники;

на непреднамеренные (случайные) и преднамеренные действия субъектов.

Виды информационной безопасности и умышленных угроз безопасности информации

Информационная безопасность – защищенность информации и соответствующей инфраструктуры от случайных или преднамеренных воздействий сопровождающихся нанесением ущерба владельцам или пользователям информации.

Основные типы угроз информационной безопасности:

1. Угрозы конфиденциальности – несанкционированный доступ к данным (например, получение посторонними лицами сведений о состоянии счетов клиентов банка).

2. Угрозы целостности – несанкционированная модификация, дополнение или уничтожение данных

3. Угрозы доступности – ограничение или блокирование доступа к данным.

Источники угроз:

1. Внутренние:

а) ошибки пользователей и сисадминов;

б) ошибки в работе ПО;

в) сбои в работе компьютерного оборудования;

г) нарушение сотрудниками компании регламентов по работе с информацией.

2. Внешние угрозы:

а) несанкционированный доступ к информации со стороны заинтересованных организаций и отдельных лица

б) компьютерные вирусы и иные вредоносные программы;

Правовые основы защиты информации и закон о защите информации

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение состояния защищённости информационной среды.

- Статья 272.Лицо будет привлечено к уголовной ответственности за неправомерный доступ к информации,за порчу,изменение, уничтожение,нарушение гласности и правовых норм.
- статья 273. За распространение,создание,использование вирусного и другого вредоносного программного ПО.
- Статья 274. нарушение правил эксплуатации эвм лицом,имеющим доступ к этой информации,повлекшее уничтожение,простой в работе, изменение информации и т.д.

Информационная безопасность

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:

- целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на обеспечение компьютерной безопасности, основными среди них являются технические, организационные и правовые.

Обеспечение безопасности информации — дорогое дело, и не только из-за затрат на закупку или установку средств защиты, но также из-за того, что трудно квалифицированно определить границы разумной безопасности и обеспечить соответствующее поддержание системы в работоспособном состоянии.

Средства зашиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен соответствующий анализ.

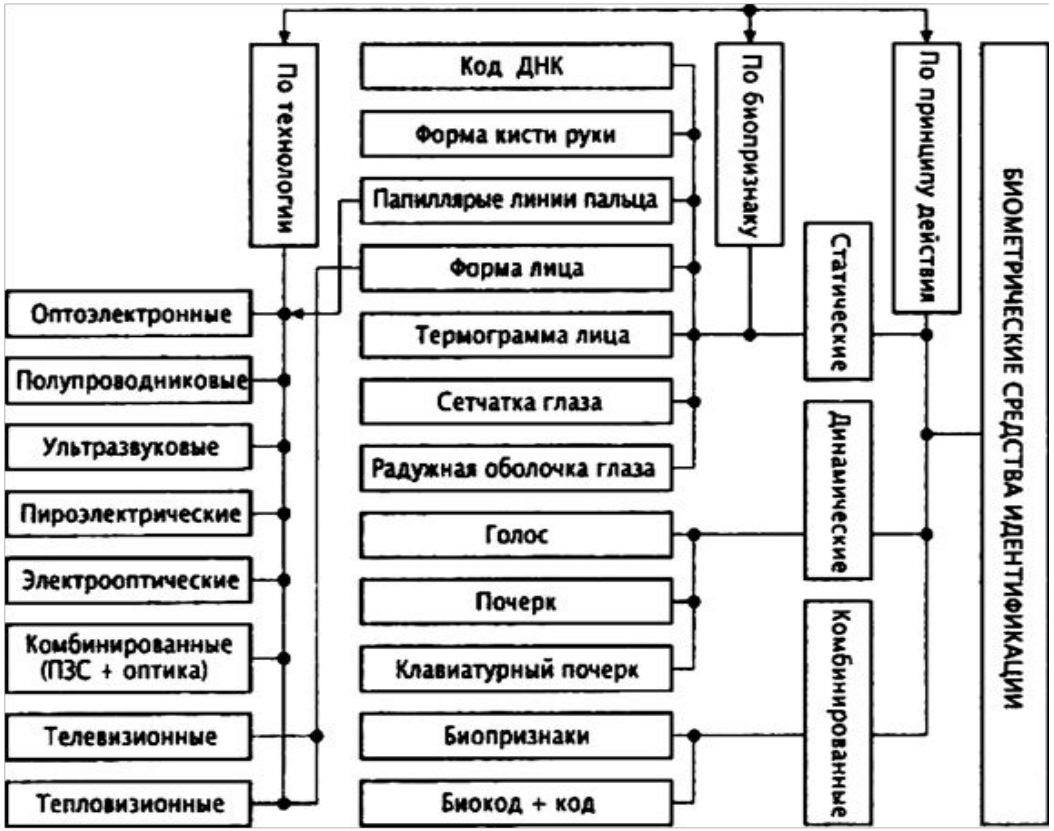
На сайте анализируется информационная безопасность и ее место в системе национальной безопасности, определяются жизненно важные интересы в информационной сфере и угрозы для них. Рассмотрены вопросы информационной войны, информационного оружия, принципы, основные задачи и функции обеспечения информационной безопасности, функции государственной системы по

Биометрические системы защиты

Биометрические системы распознают людей на основе их анатомических особенностей (отпечатков пальцев, образа лица, рисунка линий ладони, радужной оболочки, голоса) или поведенческих черт (подписи, походки). Поскольку эти черты физически связаны с пользователем, биометрическое распознавание надежно в роли механизма, следящего, чтобы только те, у кого есть необходимые полномочия, могли попасть в здание, получить доступ к компьютерной системе или пересечь границу государства. Биометрические системы также обладают уникальными преимуществами — они не позволяют отречься от совершенной транзакции и дают возможность определить, когда индивидуум пользуется несколькими удостоверениями (например, паспортами) на разные имена. Таким образом, при грамотной реализации в соответствующих приложениях биометрические системы обеспечивают высокий уровень защищенности.Биометрическая система на этапе регистрации записывает образец биометрической черты пользователя с помощью датчика — например, снимает лицо на камеру. Затем из биометрического образца извлекаются индивидуальные черты — например, минуции (мелкие подробности линий пальца) — с помощью программного алгоритма экстракции черт (feature extractor). Система сохраняет извлеченные черты в качестве шаблона в базе данных наряду с другими идентификаторами, такими как имя или идентификационный номер. Для аутентификации пользователь предъявляет датчику еще один биометрический образец. Черты, извлеченные из него, представляют собой запрос, который система сравнивает с шаблоном заявленной личности с помощью алгоритма сопоставления. Он возвращает рейтинг соответствия, отражающий степень схожести между шаблоном и запросом. Система принимает заявление, только если рейтинг соответствия превышает заранее заданный порог.

Биометрические системы защиты

Биометрические системы защиты информации - системы контроля доступа, основанные на идентификации и аутентификации человека по биологическим признакам, таким как структура ДНК, рисунок радужной оболочки глаза, сетчатка глаза, геометрия и температурная карта лица, отпечаток пальца, геометрия ладони. Также эти методы аутентификации человека называют статистическими методами, так как основаны на физиологических характеристиках человека, присутствующих от рождения и до смерти, находящиеся при нем в течение всей его жизни, и которые не могут быть потеряны или украдены. Часто используются еще и уникальные динамические методы биометрической аутентификации - подпись, клавиатурный почерк, голос и походка, которые основаны на поведенческих характеристиках людей.



Распознавание лица

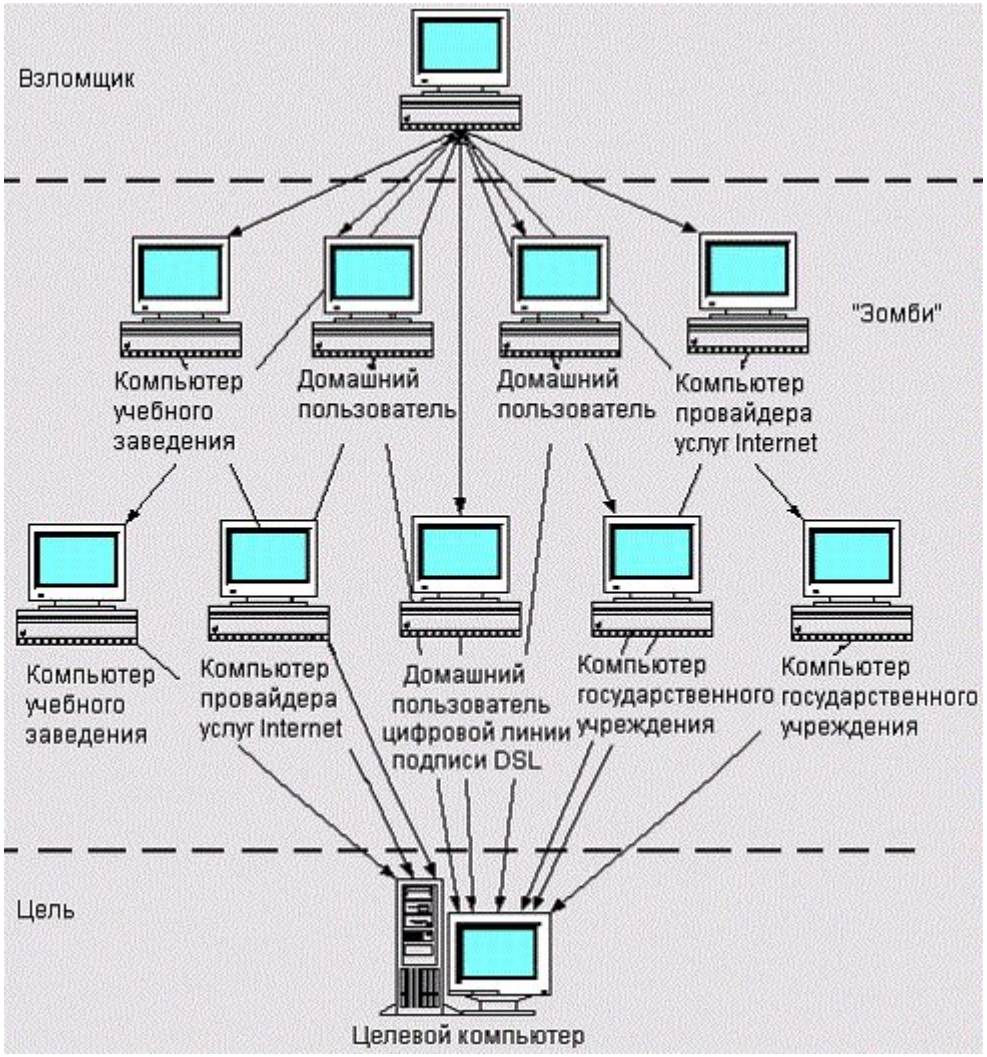
Технология распознавания позволяет сканировать человеческие лица в режиме реального времени. Видеокамера подключается к терминалу, и система определяет, соответствует ли лицо в кадре фотографиям из базы данных. Для надежного опознания человека программе достаточно всего несколько десятков базовых точек. Фотография и цифровое описание лица заносятся в базу данных, с которой впоследствии сравнивается распознаваемое лицо. Для идентификации и верификации можно использовать и старые фотографии. Технология в принципе позволяет работать даже с рентгеновскими снимками. Для защиты данных и информации также предпочтительно использовать системы распознавания лица. Кроме того, контроль лица выполняется с определенным комфортом: он бесконтактен и обеспечивает удобную и быструю обработку данных. Метод распознавания лица — это единственный биометрический способ идентификации персон и с точки зрения многоцелевого применения. В отличие от других биометрических методов, применимых только для контроля доступа или сравнения в базе данных, технология распознавания образа позволяет детектировать (находить) лицо человека в видеокадре, либо для последующего сравнения с базой данных, либо наоборот, чтобы скрыть его от случайного зрителя.

Идентификация по отпечаткам пальцев

Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш - диски, а также применяются в виде отдельных внешних устройств и терминалов. Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации не возможен.

DDos-Атаки

DoS-атака характеризуется перегрузкой атакуемых Сетевых ресурсов (порта или канала) и/или перегрузкой атакуемого Информационного ресурса (сервера), в результате чего нарушается нормальный порядок их функционирования. DDoS-атака (Distribute Denial of Service) — Сетевая атака, по своим целям и методам реализации аналогичная DoS-атаке, но осуществляющаяся с нескольких узлов сети Интернет.



Органы (подразделения), обеспечивающие информационную безопасность

В зависимости от приложения деятельности в области защиты информации (в рамках государственных органов власти или коммерческих организаций), сама деятельность организуется специальными государственными органами (подразделениями), либо отделами (службами) предприятия.

Государственные органы РФ, контролирующие деятельность в области защиты информации:
Комитет Государственной думы по безопасности;

Совет безопасности России;

Федеральная служба по техническому и экспортному контролю (ФСТЭК России);

Федеральная служба безопасности Российской Федерации (ФСБ России);

Служба внешней разведки Российской Федерации (СВР России);

Министерство обороны Российской Федерации (Минобороны России);

Министерство внутренних дел Российской Федерации (МВД России);

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

Защита речевой (акустической системы)

Защита речевой (акустической) информации является одной из важнейших задач в общем комплексе мероприятий по обеспечению информационной безопасности объекта технической защиты информации (ЗИ). Это связано с тем, что в процессе обсуждения служебных вопросов может озвучиваться конфиденциальная информация (информация ограниченного доступа). Перехват этой информации может происходить максимально оперативно в момент ее первого озвучивания. Объектами технической защиты речевой (акустической) информации (ТЗРИ) являются учреждения системы государственного управления, военные и военно-промышленные объекты, научно-исследовательские учреждения и т.д. При этом на объектах ТЗРИ защищаются:

1. специально предназначенные для обмена речевой информацией ограниченного доступа (звукозаписи, звуковоспроизведения такой информации) помещения;
2. помещения, специально не предназначенные, но используемые для такого рода деятельности в силу обстоятельств;
3. открытые площадки.

Для обеспечения защиты используют пассивные и активные методы. Пассивные методы включают в себя звукопоглощение и звукоизоляцию. Звукопоглощение обеспечивается применением специальных герметичных панелей из стекловаты высокой плотности различной толщины. Звукоизоляция обеспечивается специальными звукоизолирующими покрытиями стен. Звукоизоляцию целесообразно применять только в небольших помещениях, т.к. в больших помещениях звуковая энергия максимально поглощается, не достигнув стен. В тех случаях, когда пассивные меры не обеспечивают необходимого уровня безопасности, применяются активные методы.

К активным средствам относятся генераторы шума – технические средства, вырабатывающие шумоподобные электронные сигналы. Эти сигналы подаются на соответствующие датчики акустического или вибрационного преобразования. Акустические датчики предназначены для создания акустического шума в помещениях или вне их, а вибрационные – для маскирующего шума в ограждающих конструкциях (приклеиваются к ним, создавая в них звуковые колебания). Примером данного генератора является система виброакустического зашумления «Заслон».