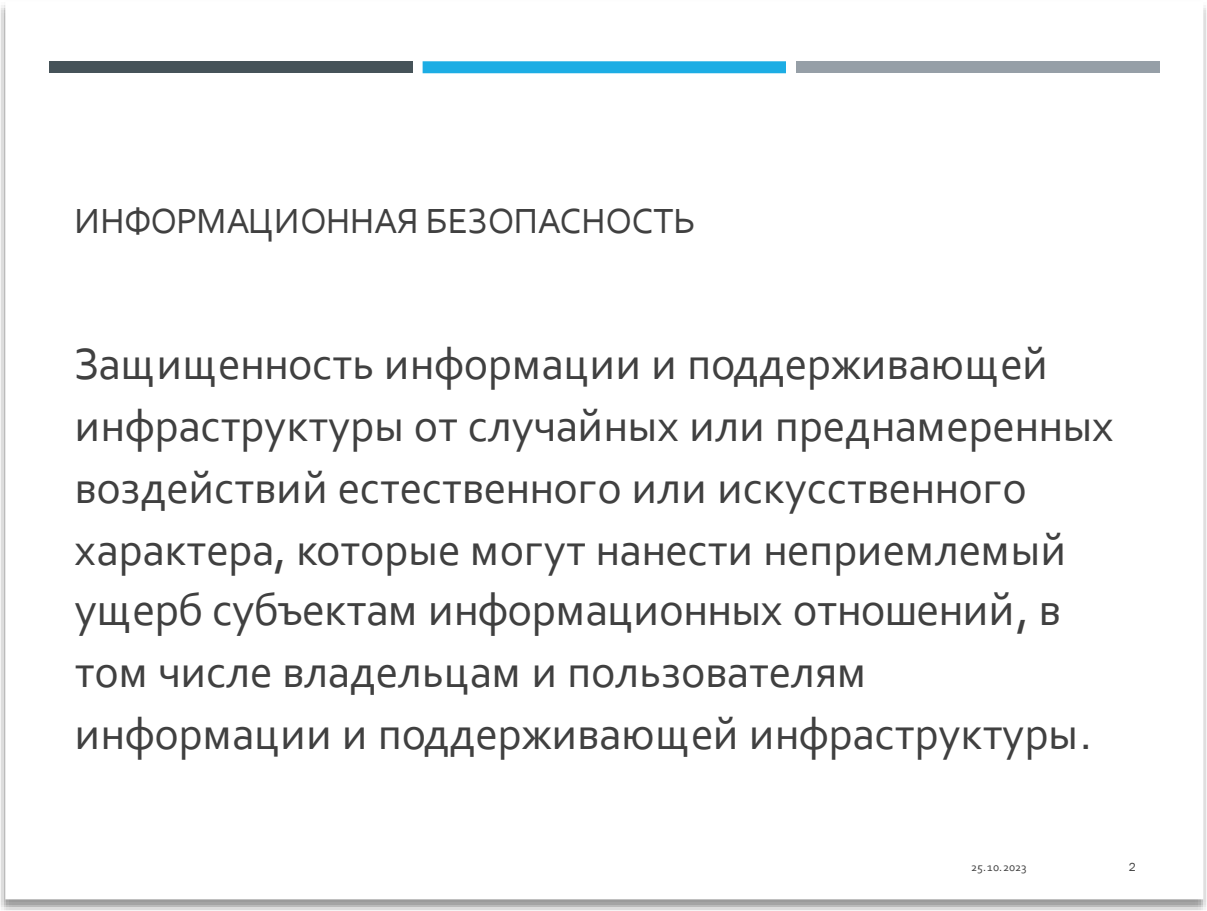
Информационная безопасность

Лекция 1

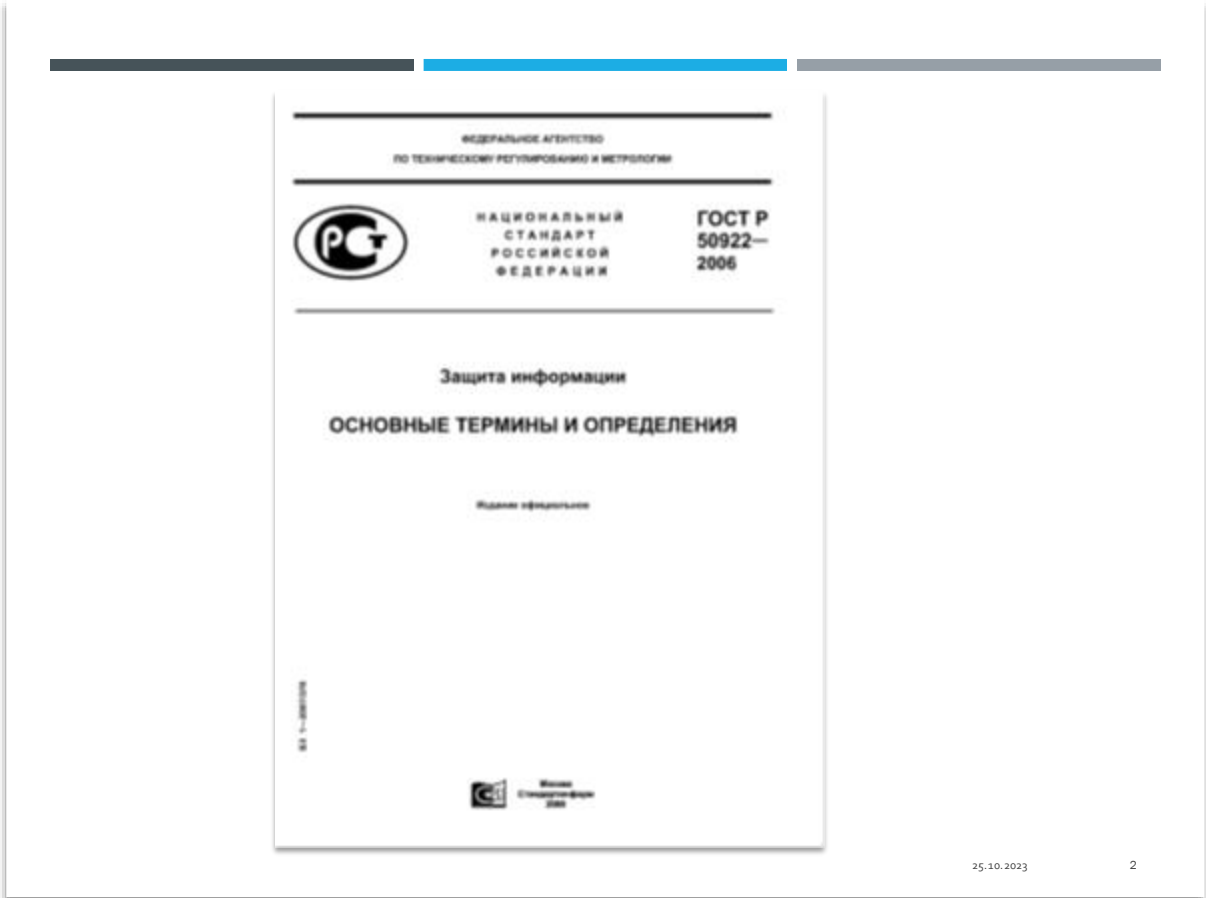
Введение в информационную безопасность

Основные понятия информационной безопасности

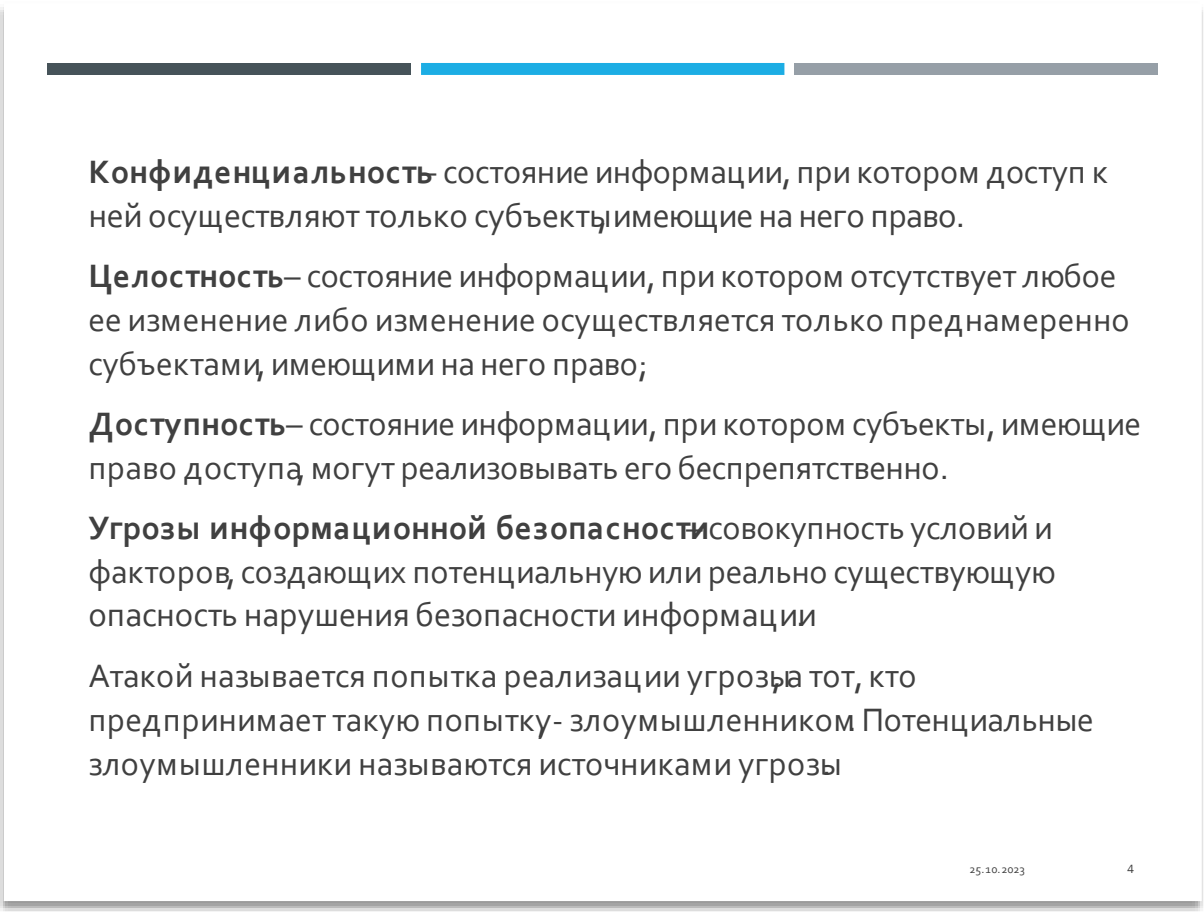
Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое *информационная безопасность*. Термин "*информационная безопасность*" может иметь различный смысл и трактовку в зависимости от контекста.



В данном курсе под **информационной безопасностью** мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб субъектам информационных отношений*, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.



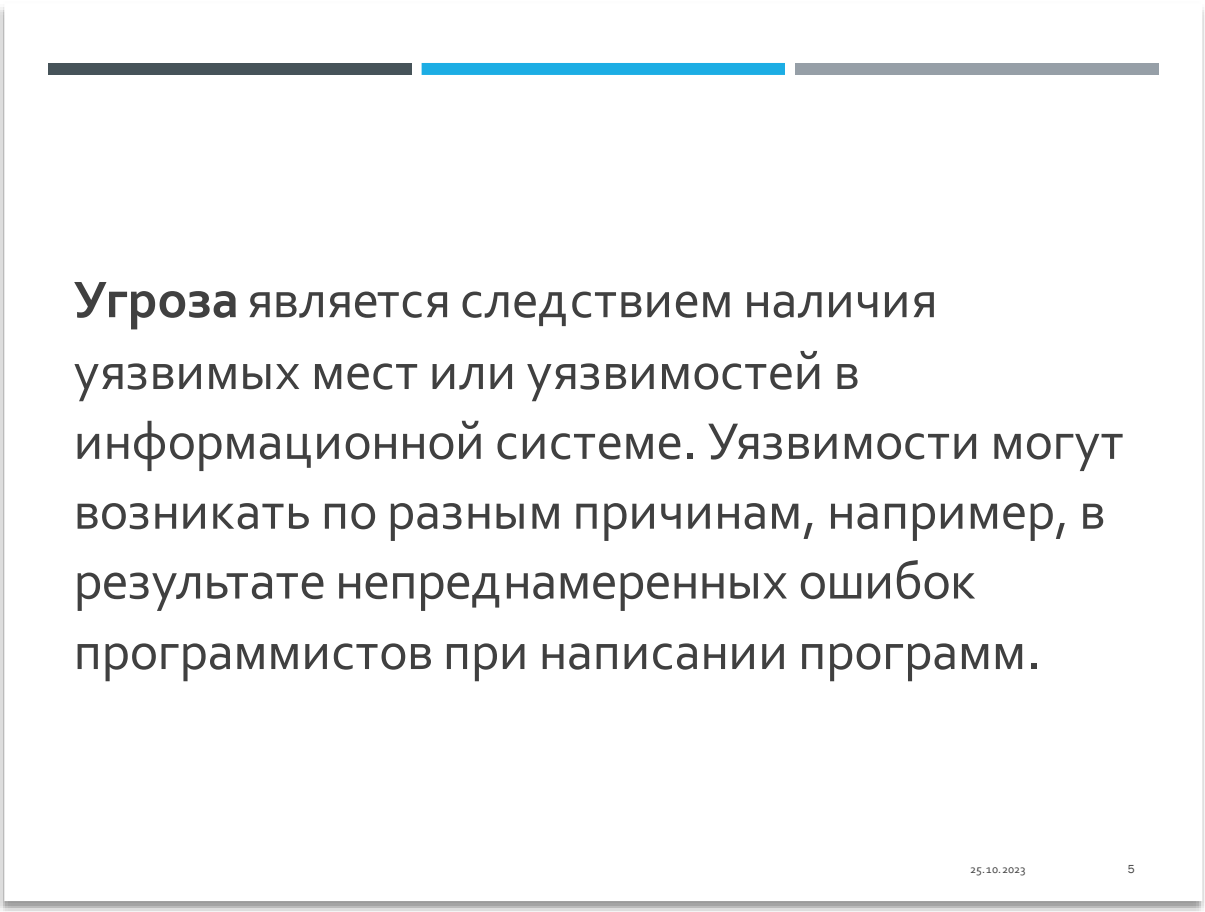
ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения" вводит понятие информационной безопасности как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.



- **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Атакой называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются *источниками угрозы*.

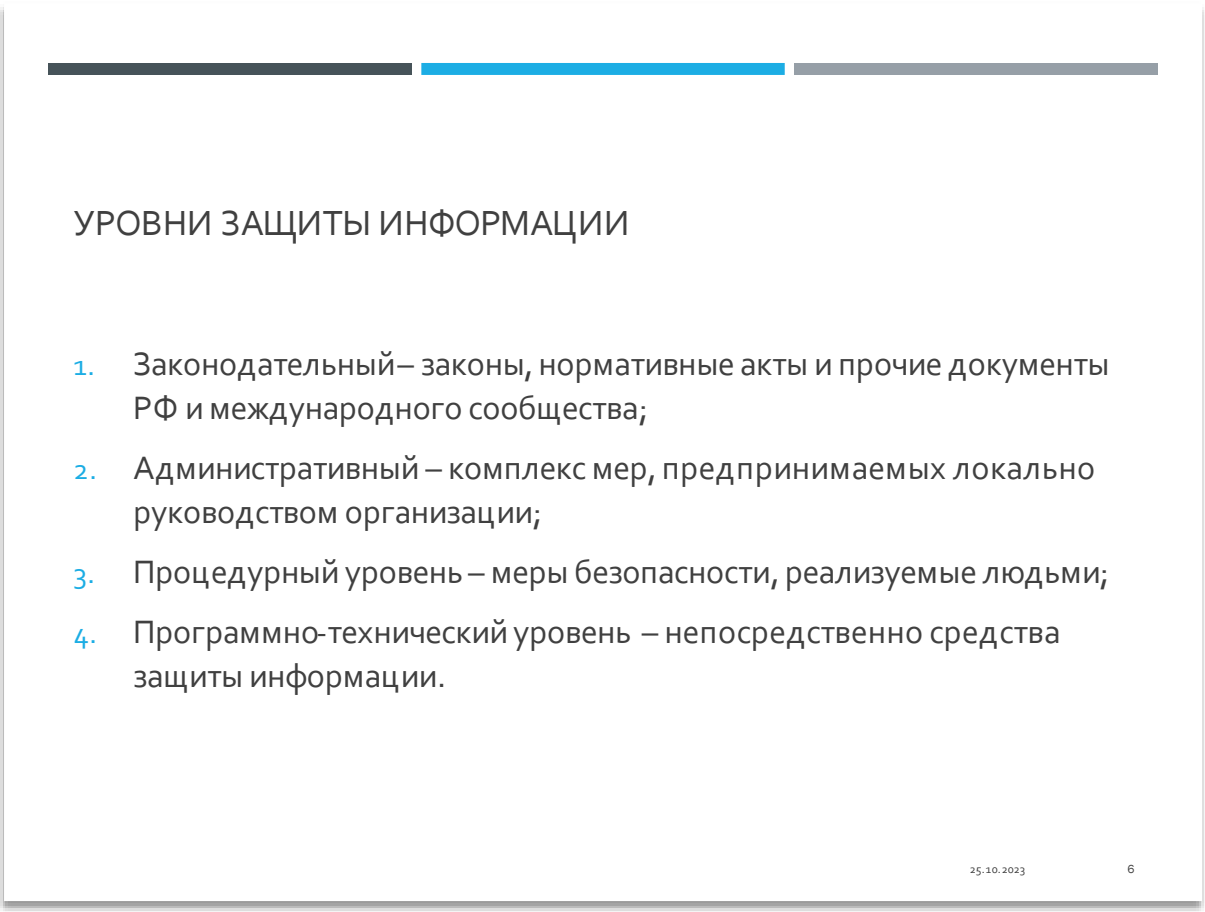


Угроза является следствием наличия **уязвимых мест или уязвимостей** в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

- по *свойствам информации* (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, *поддерживающая инфраструктура*);
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется *комплексный подход*. Выделяют следующие уровни защиты информации:



1. законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;
2. административный – комплекс мер, предпринимаемых локально руководством организации;
3. процедурный уровень – меры безопасности, реализуемые людьми;
4. *программно-технический уровень* – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия *предметной области* и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) *отношение* к людям, нарушающим информационную *безопасность*.

ФЗ "Об информации, информационных технологиях и о защите информации"

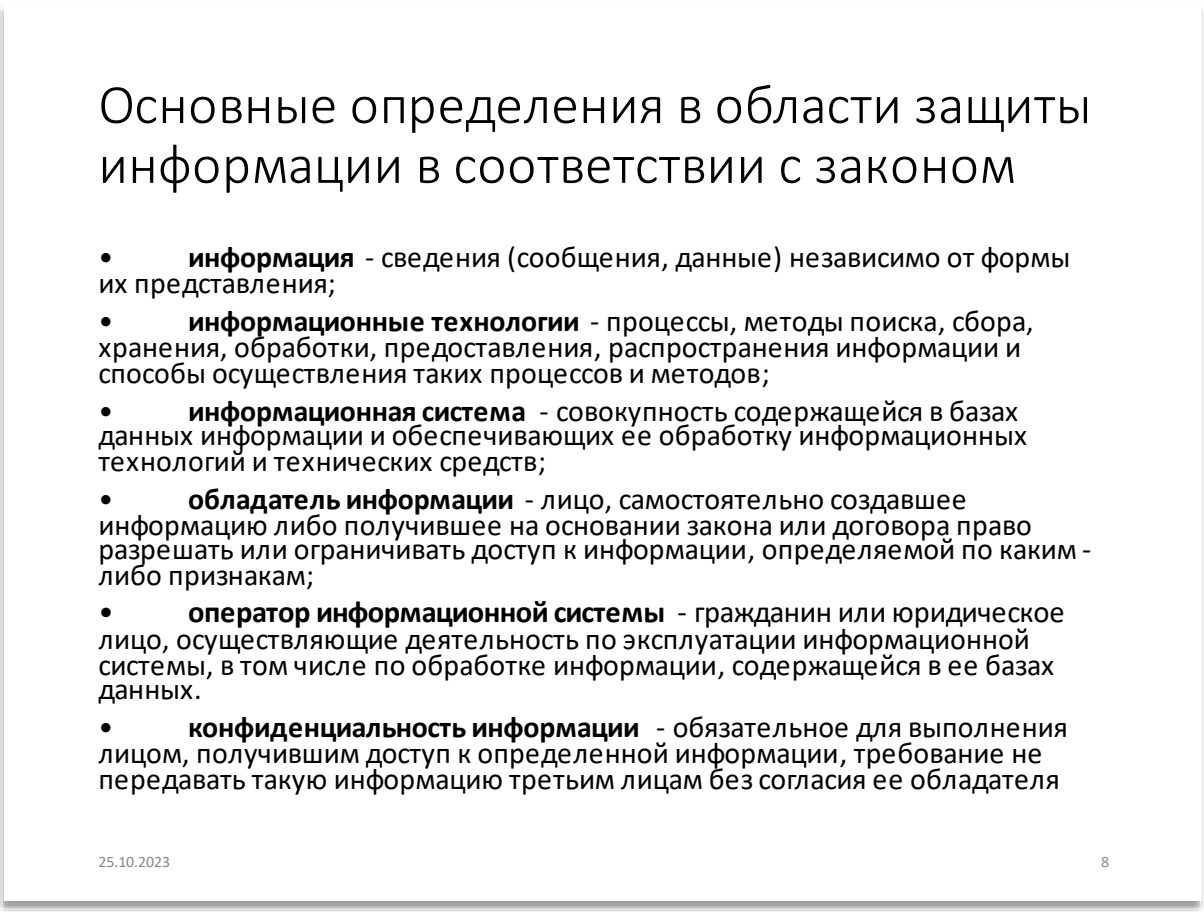
25.10.2023 7

В российском законодательстве базовым законом в области защиты информации является ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них:



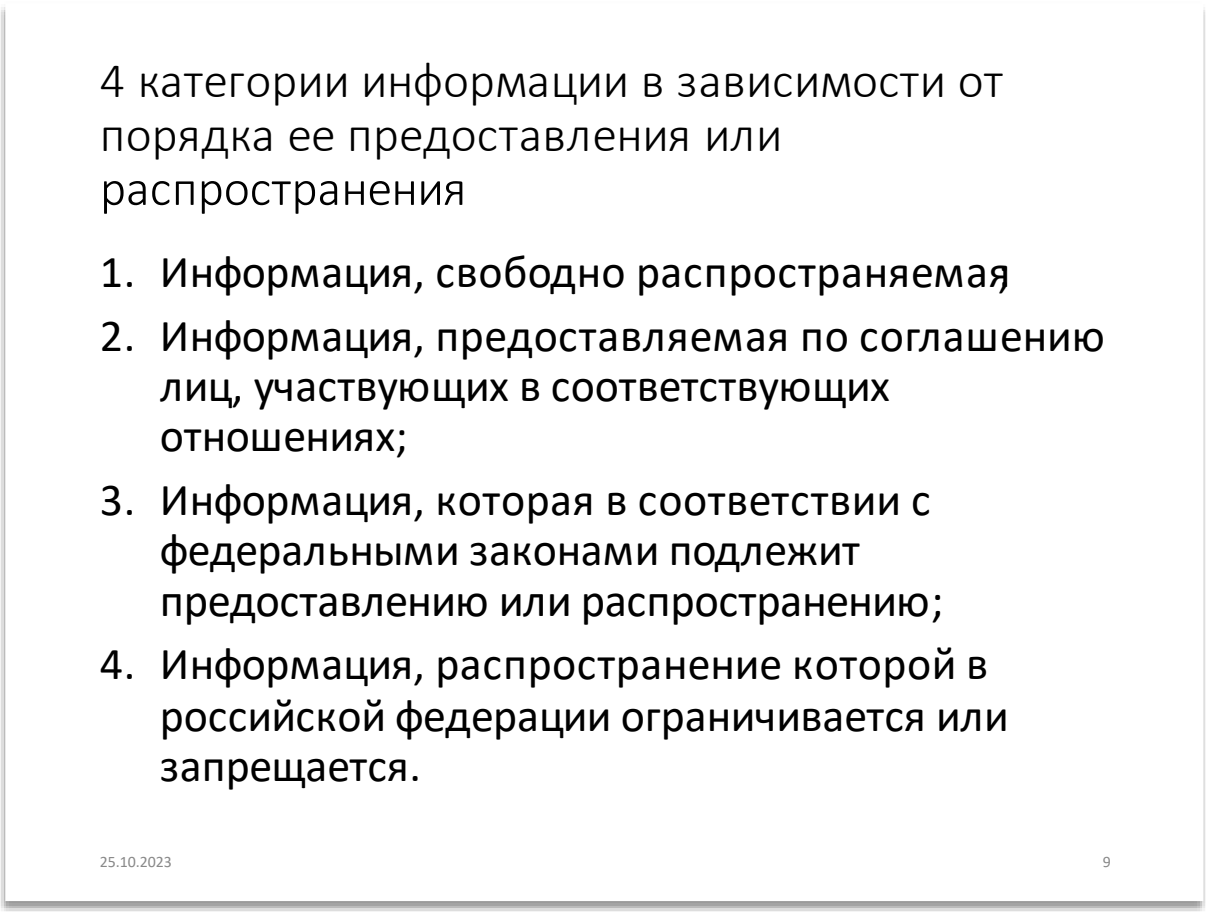
- **информация** - сведения (сообщения, данные) независимо от формы их представления;
- **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
- **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [4].

В статье 3 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2. установление ограничений доступа к информации только федеральными законами;
3. открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
4. равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
5. обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
6. достоверность информации и своевременность ее предоставления;
7. неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
8. недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся *информация* делится на **общедоступную** и ограниченного **доступа**. К общедоступной информации относятся общеизвестные сведения и иная *информация*, *доступ* к которой не ограничен. В законе, определяется *информация*, к которой нельзя ограничить *доступ*, например, *информация* об окружающей среде или деятельности государственных органов. Оговаривается также, что *ограничение доступа* к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, *доступ* к которой ограничен федеральными законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.



Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

1. информацию, свободно распространяемую;
2. информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3. информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
4. информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Дается следующее *определение* защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. соблюдение конфиденциальности информации ограниченного доступа;
3. реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1. предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2. своевременное обнаружение фактов несанкционированного доступа к информации;
3. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5. возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6. постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, ФЗ "Об информации, информационных технологиях и о защите информации" создает правовую основу информационного обмена в РФ и определяет *права* и обязанности его субъектов.

Требования к архитектуре ИС для обеспечения безопасности ее функционирования

Идеология открытых систем существенно отразилась на методологических аспектах и направлении развития сложных распределенных ИС.

Она базируется на строгом соблюдении совокупности профилей, протоколов и стандартов де-факто и де-юре. Программные и аппаратные компоненты по этой идеологии должны отвечать важнейшим требованиям переносимости и возможности согласованной, совместной работы с другими удаленными компонентами.

Это позволяет обеспечить совместимость компонент различных информационных систем, а также средств передачи данных. Задача сводится к максимально возможному повторному использованию разработанных и апробированных программных и информационных компонент при изменении вычислительных аппаратных платформ, ОС и процессов взаимодействия.

При создании сложных, распределенных информационных систем, проектировании их архитектуры, инфраструктуры, выборе компонент и связей между ними следует учитывать помимо общих (открытость, масштабируемость, переносимость, мобильность, защита инвестиций и т.п.) ряд специфических концептуальных требований, направленных на обеспечение безопасности функционирования самой системы и данных:

- архитектура системы должна быть достаточно гибкой, т.е. должна допускать относительно простое, без коренных структурных изменений, развитие инфраструктуры и изменение конфигурации используемых средств, наращивание функций и ресурсов ИС в соответствии с расширением сфер и задач ее применения;
- должны быть обеспечены безопасность функционирования системы при различных видах угроз и надежная защита данных от ошибок проектирования, разрушения или потери информации, а также авторизация пользователей, управление рабочей загрузкой, резервированием данных и вычислительных ресурсов, максимально быстрым восстановлением функционирования ИС;
- следует обеспечить комфортный, максимально упрощенный доступ пользователей к сервисам и результатам функционирования ИС на основе современных графических средств, мнемосхем и наглядных пользовательских интерфейсов;
- систему должна сопровождать актуализированная, комплектная документация, обеспечивающая квалифицированную эксплуатацию и возможность развития ИС.

Подчеркнем, что технические системы безопасности, какими бы мощными они ни были, сами *по* себе не могут гарантировать *надежность* программно-технического уровня защиты. Только сфокусированная на *безопасность архитектура* ИС способна сделать эффективным *объединение* сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая *производительность*, простота и *удобство использования*. Для того чтобы выполнить эти требования *архитектура* ИС должна строиться на следующих принципах.

Проектирование ИС на принципах открытых систем, следование признанным стандартам, использование апробированных решений, иерархическая организация ИС с небольшим числом сущностей на каждом уровне — все это способствует прозрачности и хорошей управляемости ИС.

Непрерывность защиты в пространстве и времени, невозможность преодолеть защитные средства, *исключение* спонтанного или вызванного перехода в небезопасное состояние — при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует *доступ* в систему или ее часть

Усиление самого слабого звена, минимизация *привилегий* доступа, разделение функций обслуживающих сервисов и обязанностей персонала. Предполагается такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите *по* неведению или заказу злоумышленников.

Применительно к программно-техническому уровню принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права *доступа*, которые необходимы им для выполнения служебных обязанностей. Это позволяет уменьшить *ущерб* от случайных или умышленных некорректных действий пользователей и администраторов.

Эшелонирование обороны, разнообразие защитных средств, простота и управляемость информационной системы и системой ее безопасности. Принцип эшелонирования обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией — *управление доступом*, *протоколирование* и *аудит*.

Эшелонированная оборона способна не только не пропустить злоумышленника, но и в некоторых случаях идентифицировать его благодаря протоколированию и аудиту. Разнообразие защитных средств предполагает создание различных *по* своему характеру оборонительных рубежей, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками.

Простота и управляемость ИС в целом и защитных средств в особенности. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществлять централизованное *администрирование*. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный *интерфейс*. Соответственно, если объекты некоторого вида (например, таблицы *базы данных*) доступны через *Интернет*, необходимо заблокировать *прямой доступ* к ним, поскольку в противном случае система будет уязвимой, сложной и плохо управляемой.

Продуманная и упорядоченная структура программных средств и баз данных. *Топология* внутренних и внешних сетей непосредственно отражается на достигаемом качестве и безопасности ИС, а также на трудоемкости их разработки. При строгом соблюдении правил структурного построения значительно облегчается достижение высоких показателей качества и безопасности, так как сокращается число возможных ошибок в реализующих программах, отказов и сбоев оборудования, упрощается их *диагностика* и *локализация*.

В хорошо структурированной системе с четко выделенными компонентами (клиент, *сервер* приложений, ресурсный *сервер*) контрольные точки выделяются достаточно четко, что решает задачу доказательства достаточности применяемых средств защиты и обеспечения невозможности обхода этих средств потенциальным нарушителем.

Высокие требования, предъявляемые к формированию архитектуры и инфраструктуры на стадии проектирования ИС, определяются тем, что именно на этой стадии можно в значительной степени минимизировать число уязвимостей, связанных с непредумышленными дестабилизирующими факторами, которые влияют на *безопасность* программных средств, баз данных и систем коммуникации.

Анализ безопасности ИС при отсутствии злоумышленных факторов базируется на модели взаимодействия основных *компонент* ИС (рис. 6.1) [Липаев В. В., 1997]. В качестве объектов уязвимости рассматриваются:

- динамический вычислительный процесс обработки данных, автоматизированной подготовки решений и выработки управляющих воздействий;
- объектный код программ, исполняемых вычислительными средствами в процессе функционирования ИС;
- данные и информация, накопленная в базах данных;
- информация, выдаваемая потребителям и на исполнительные механизмы.

Рис. 6.1. Модель анализа безопасности информационных систем при отсутствии злоумышленных угроз

Полное устранение перечисленных угроз принципиально невозможно. Задача состоит в выявлении факторов, от которых они зависят, в создании методов и средств уменьшения их влияния на *безопасность* ИС, а также в эффективном распределении ресурсов для обеспечения защиты, равнопрочной *по* отношению ко всем негативным воздействиям.

Стандартизация подходов к обеспечению информационной безопасности

Специалистам в области ИБ сегодня практически невозможно обойтись без знаний соответствующих профилей защиты, стандартов и спецификаций. Формальная причина состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и "Руководящим документам" Гостехкомиссии РФ) закреплена законодательно. Убедительны и содержательные причины: стандарты и спецификации - одна из форм накопления и реализации знаний, прежде всего о процедурном и программно-техническом уровнях ИБ и ИС, в них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными компаниями в области разработки ПО и безопасности программных средств.

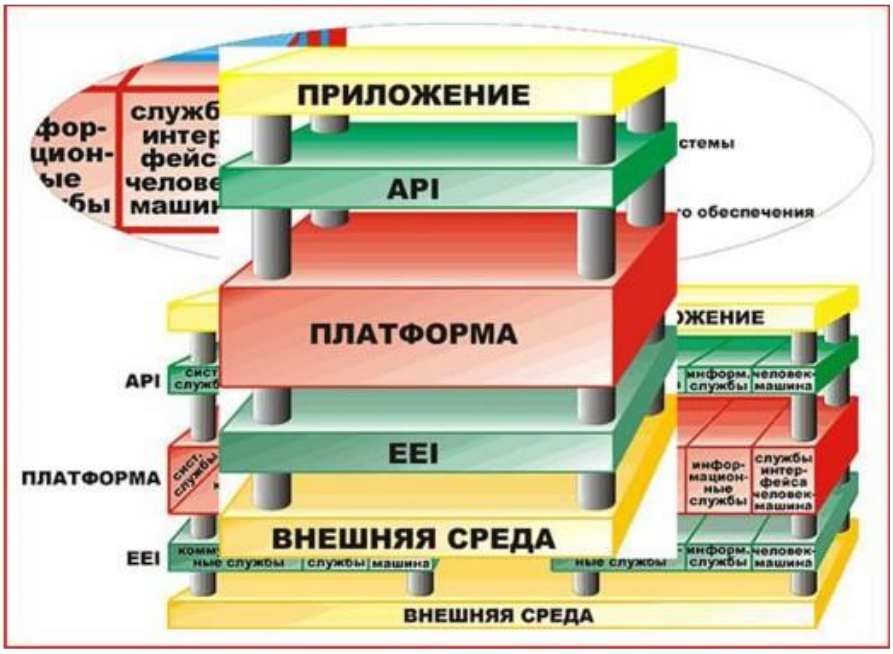
На верхнем уровне можно выделить две существенно отличающиеся друг от друга группы стандартов и спецификаций:

1. оценочные стандарты, предназначенные для оценки и классификации ИС и средств защиты по требованиям безопасности;

2. спецификации, регламентирующие различные аспекты реализации и использования средств и методов защиты.

Эти группы дополняют друг друга. Оценочные стандарты описывают важнейшие с точки зрения ИБ понятия и аспекты ИС, играя роль организационных и архитектурных спецификаций. Специализированные стандарты и спецификации определяют, как именно строить ИС предписанной архитектуры и выполнять организационные и технические требования для обеспечения информационной безопасности (рис. 6.2, рис. 6.3).

Объекты стандартизации в открытой информационной системе



25.10.2023 11

Рис. 6.2. Объекты стандартизации в открытой информационной системе

Хронология стандартизации в сфере информационной безопасности

25.10.2023 12

Рис. 6.3. Хронология стандартизации в сфере информационной безопасности

Из числа оценочных необходимо выделить стандарт "Критерии оценки доверенных компьютерных систем" и его интерпретацию для сетевых конфигураций (Министерство обороны США), "Гармонизированные критерии Европейских стран", международный стандарт "Критерии оценки безопасности информационных технологий" и, конечно, "Руководящие документы" Гостехкомиссии РФ. К этой же группе относится и Федеральный стандарт США "Требования безопасности для криптографических модулей", регламентирующий конкретный, но очень важный и сложный аспект информационной безопасности.

Технические спецификации, применимые к современным распределенным ИС, создаются главным образом "Тематической группой по технологии Интернет" (Internet Engineering Task Force - IETF) и ее подразделением - рабочей группой по безопасности. Ядром технических спецификаций служат документы по безопасности на IP-уровне (IPSec). Кроме этого, анализируется защита на транспортном уровне (Transport Layer Security - TLS), а также на уровне приложений (спецификации GSS-API, Kerberos).

Интернет-сообщество уделяет должное внимание административному и процедурному уровням безопасности, создав серию руководств и рекомендаций: "Руководство по информационной безопасности предприятия", "Как выбирать поставщика Интернет-услуг", "Как реагировать на нарушения информационной безопасности" и др.

В вопросах сетевой безопасности востребованы спецификации X.800 "Архитектура безопасности для взаимодействия открытых систем", X.500 "Служба директорий: обзор концепций, моделей и сервисов" и X.509 "Служба директорий: каркасы сертификатов открытых ключей и атрибутов".

В последние 15 лет утверждена большая серия международной организацией по стандартизации (International Organization for Standardization - ISO) стандартов по обеспечению безопасности информационных систем и их компонентов. Подавляющее большинство из этих стандартов относятся к телекоммуникациям, процессам и протоколам обмена информацией в распределенных системах и защите ИС от несанкционированного доступа. В связи с этим при подготовке системы защиты и обеспечения безопасности из стандартов должны быть отобраны наиболее подходящие для всего жизненного цикла конкретного проекта ПС.

В следующей главе "Технологии и стандартизация открытых вычислительных и информационных систем" будет подробно рассказано о структуре и деятельности ISO и её технических комитетах, в частности об Объединенном техническом комитете № 1 (Joint Technical Committee 1 - JTC1), предназначенном для формирования всеобъемлющей системы базовых стандартов в области ИТ и их расширений для конкретных сфер деятельности. В зависимости от проблем, методов и средств защиты вычислительных и информационных систем международные стандарты ISO можно разделить на несколько групп.

Первая группа стандартов - ISO/IEC JTC1/SC22 "Поиск, передача и управление информацией для взаимосвязи открытых систем (ВОС)" - создана и развивается под руководством подкомитета SC22. Стандарты этой группы посвящены развитию и детализации концепции ВОС. Защита информации в данной группе рассматривается как один из компонентов, обеспечивающих возможность полной реализации указанной концепции. Для этого определены услуги и механизмы защиты по уровням базовой модели ВОС, изданы и разрабатываются стандарты, последовательно детализирующие методические основы защиты информации и конкретные протоколы защиты на разных уровнях открытых систем.

Вторая группа стандартов - ISO/IEC JTC1/SC27 - разрабатывается под руководством подкомитета SC27 и ориентирована преимущественно на конкретные методы и алгоритмы защиты. В эту группу объединены методологические стандарты защиты информации и криптографии, независимо от базовой модели ВОС. Обобщаются конкретных методов и средств защиты в систему организации и управления защитой ИС.

В процессе планирования и проектирования программной системы защиты ИС целесообразно использовать третью группу из представленных ниже наиболее общих методологических стандартов, регламентирующих создание комплексов защиты. Вследствие близких целей стандартов их концепции и содержание частично перекрещиваются и дополняют друг друга. Поэтому стандарты целесообразно использовать совместно (создать профиль стандартов), выделяя и адаптируя их компоненты в соответствии с требованиями конкретного проекта ИС.

1. ISO 10181:1996. Ч. 1-7. "ВОС. Структура работ по обеспечению безопасности в открытых системах". Часть 1. Обзор. Часть 2. Структура работ по аутентификации. Часть 3. Структура работ по управлению доступом. Часть 4. Структура работ по безотказности. Часть 5. Структура работ по конфиденциальности. Часть 6. Структура работ по обеспечению целостности. Часть 7. Структура работ по проведению аудита на безопасность.

2. ISO 13335:1996-1998. Ч. 1-5. ИТ. ТО. "Руководство по управлению безопасностью". Часть 1. Концепция и модели обеспечения безопасности информационных технологий. Часть 2. Планирование и управление безопасностью информационных технологий. Часть 3. Техника управления безопасностью ИТ. Часть 4. Селекция (выбор) средств обеспечения безопасности. Часть 5. Безопасность внешних связей.

3. ISO 15408:1999. Ч.26 1-3. "Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий". Часть 1. Введение и общая модель. Часть 2. Защита функциональных требований. Часть 3. Защита требований к качеству.

Первый стандарт этой группы, ISO 10181, состоит из семи частей и начинается с общей концепции обеспечения безопасности открытых

информационных систем и развивает положения стандарта ISO 7498-2. В первой его части приводятся основные понятия и общие характеристики методов защиты и акцентируется внимание на необходимости сертификации системы обеспечения безопасности ИС при ее внедрении. Далее кратко описаны основные средства обеспечения безопасности ИС, особенности работ по их созданию, основы взаимодействия механизмов защиты, принципы оценки возможных отказов от обслуживания задач ИС по условиям защиты. Показаны примеры построения общих схем защиты ИС в открытых системах. Содержание частей стандарта достаточно ясно определяется их названиями.

Второй стандарт, ISO 13335, отражает широкий комплекс методологических задач, которые необходимо решать при проектировании систем обеспечения безопасности любых ИС. В его пяти частях внимание сосредоточено на основных принципах и методах проектирования равнопрочных систем защиты ИС от угроз различных видов. Это руководство достаточно полно систематизирует основные методы и процессы подготовки проекта защиты для последующей разработки конкретной комплексной системы обеспечения безопасности функционирования ИС.

Изложение базируется на понятии риска от угроз любых негативных воздействий на ИС. В первой части стандарта описаны функции средств защиты и необходимые действия по их реализации, модели уязвимости и принципы взаимодействия средств защиты. При проектировании систем защиты рекомендуется учитывать: необходимые функции защиты, возможные угрозы и вероятность их осуществления, уязвимость, негативные воздействия исполнениюгроз, риски; защитные меры; ресурсы (аппаратные, информационные, программные, людские) и их ограниченность. В остальных частях стандарта предложены и развиваются концепция и модель управления и планирования построения системы защиты, взаимодействие компонентов которой в общем виде представлено на рис. 6.4.

В стандарте ISO 13335 выделены функциональные компоненты и средства обеспечения безопасности, а также принципы их взаимодействия. Процессы управления защитой должны включать: управление изменениями и конфигурацией; анализ и управление риском; прослеживаемость функций; регистрацию, обработку и мониторинг инцидентов. Приводятся общие требования к оценке результатов обеспечения безопасности, а также возможные варианты организации работы специалистов для комплексного обеспечения безопасности ИС.

Систематизированы политика и техника планирования, выбора, построения и использования средств обеспечения безопасности для ограничения допустимого риска при различных схемах взаимодействия и средствах защиты. Рекомендуются различные подходы и стратегии при создании систем защиты и поддержке их последующего развития. Содержание частей стандарта детализирует общие концепции и достаточно точно определяется их названиями. Изложенную в стандарте модель планирования

обеспечения безопасности целесообразно конкретизировать и использовать как фрагмент системного проекта разработки ИС.

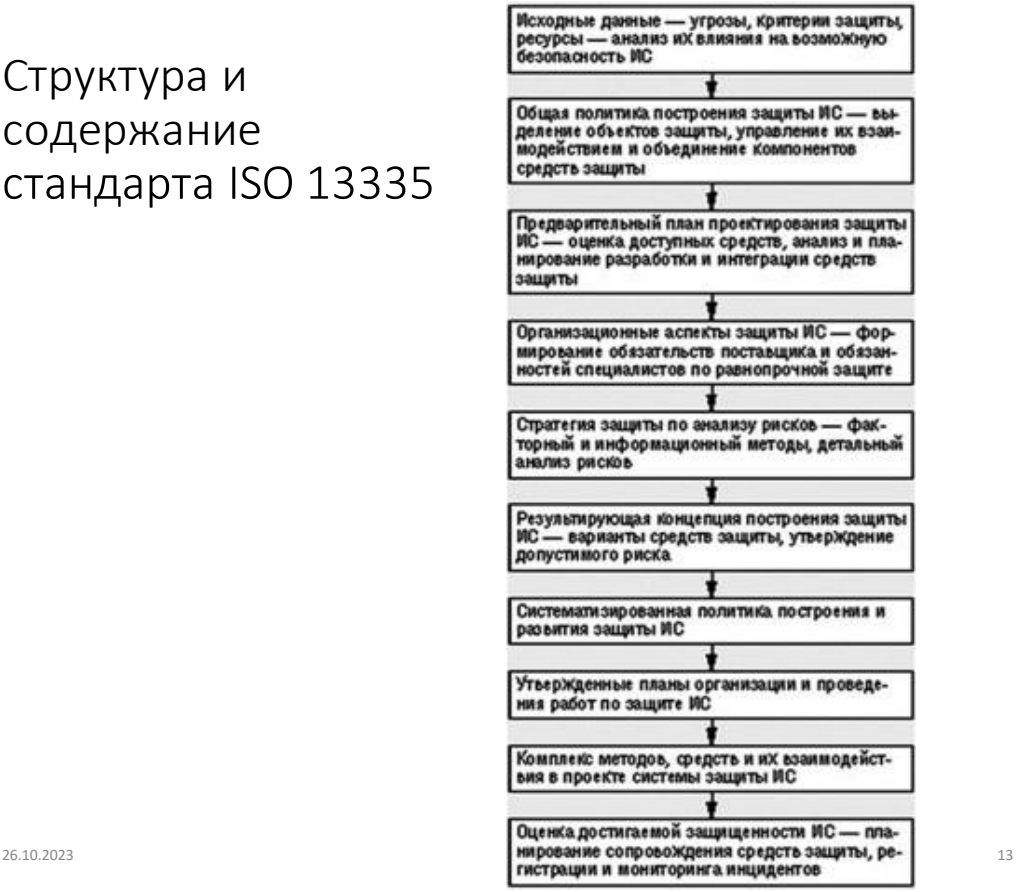


Рис. 6.4. Структура и содержание стандарта ISO 13335

Критерии оценки механизмов безопасности программно-технического уровня представлены в международном стандарте ISO 15408-1999 "Общие критерии оценки безопасности информационных технологий" ("The Common Criteria for Information Technology Security Evaluation"), принятом в 1999 году. Этот стандарт закрепил базовые основы стандартизации в области информационной защиты и получил дальнейшее развитие в серии стандартов, о которых будет сказано ниже.

В первой части стандарта представлены цели и концепция обеспечения безопасности, а также общая модель построения защиты ИС. Концепция базируется на типовой схеме жизненного цикла сложных систем, последовательной детализации требований и спецификаций компонентов. В ней выделены: окружающая среда; объекты; требования; спецификации функций; задачи инструментальных средств системы защиты. Изложены общие требования к критериям оценки результатов защиты, Профилю по безопасности, целям оценки требований и к использованию их результатов. Предложен проект комплекса общих целей, задач и критериев обеспечения безопасности ИС.

Во второй части представлена парадигма построения и реализации структурированных и детализированных функциональных требований к

компонентам защиты ИС. Выделены и классифицированы одиннадцать групп (классов) базовых задач обеспечения безопасности ИС. Каждый класс детализирован наборами требований, которые реализуют определенную часть целей обеспечения безопасности и, в свою очередь, состоят из набора более мелких компонентов решения частных задач.

В классы включены и подробно описаны принципы и методы реализации требований к функциям безопасности: криптографическая поддержка; защита коммуникаций и транспортировка (транзакции) информации; ввод, вывод и хранение пользовательских данных; идентификация и аутентификация пользователей; процессы управления функциями безопасности; защита данных о частной жизни; реализация ограничений по использованию вычислительных ресурсов; обеспечение надежности маршрутизации и связи между функциями безопасности, а также некоторые другие классы требований.

Для каждой группы задач приводятся рекомендации по применению набора наиболее эффективных компонентов и процедур обеспечения безопасности ИС. Для достижения целей безопасности ИС с определенным уровнем гарантии качества защиты компоненты функциональных требований и способов их реализации рекомендуется объединять в унифицированные "Профили защиты многократного применения".

Эти "Профили" могут служить базой для дальнейшей конкретизации функциональных требований в "Техническом задании по безопасности" для определенного проекта ИС и помогают избегать грубых ошибок при формировании таких требований. Обобщения оценок спецификации требований "Задания по безопасности" должны давать заказчикам, разработчикам и испытателям проекта возможность делать общий вывод об уровне его соответствия функциональным требованиям и требованиям гарантированности защиты ИС. В обширных приложениях изложены рекомендации по реализации средств для достижения основных функциональных целей и требований безопасности.

Третья часть стандарта посвящена целям, методам и уровням обеспечения гарантий качества процессов реализации требований к функциям обеспечения безопасности ИС. Определены методы и средства, которые целесообразно использовать для корректной реализации жизненного цикла компонентов защиты и эффективного их применения. Изложены детальные рекомендации по обеспечению гарантии качества создания и применения систем безопасности: функционирования конфигурационного управления средствами защиты; процессов поддержки жизненного цикла, разработки, поставки и эксплуатации компонентов, реализующих защиту ИС; корректности документов и руководств; тестирования и оценки уязвимости ИС. Выделена парадигма сопровождения и поддержки сохранения гарантий безопасности ИС, а также представлены методы ее реализации.

В целом, стандарт представляет собой детальное комплексное руководство, охватывающее требования к функциям и методам гарантирования качества современных методов и средств обеспечения безопасности ИС, которое целесообразно использовать при практическом проектировании систем защиты, а также как хорошее учебное пособие в этой области.

"Общие критерии" ("ОК") определяют функциональные требования безопасности (Security Functional Requirements) и требования к адекватности реализации функций безопасности (Security Assurance Requirements). "Общие критерии" содержат два основных вида требований безопасности (рис. 6.5):

1. функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям (сервисам) безопасности и реализующим их механизмам;

2. требования доверия, соответствующие пассивному аспекту; они предъявляются к технологии и процессу разработки и эксплуатации.

Рис. 6.5. Критерии адекватности средств защиты

Требования безопасности формулируются, и их выполнение проверяется для определенного объекта оценки - аппаратно-программного продукта или ИС. Безопасность в "ОК" рассматривается не статично, а в соответствии с жизненным циклом объекта оценки. Кроме того, обследуемый объект предстает не изолированно, а в "среде безопасности",

характеризующейся определенными уязвимостями и угрозами. "Общие критерии" целесообразно использовать для оценки уровня защищенности с точки зрения полноты реализованных в ней функций безопасности и надежности реализации этих функций. Хотя применимость "ОК" ограничивается механизмами безопасности программно-технического уровня, в них содержится определенный набор требований к механизмам безопасности организационного уровня и требований по физической защите, которые непосредственно связаны с описываемыми функциями безопасности.

Британский стандарт BS 7799 "Управление информационной безопасностью. Практические правила" почти без изменений отражен в международном стандарте ISO/IEC 17799:2000 "Практические правила управления информационной безопасностью" ("Code of practice for Information security management"). В этом стандарте обобщены правила по управлению ИБ, они могут быть использоваться в качестве критериев оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты. Практические правила разбиты на десять разделов.

1. Политика безопасности.
2. Организация защиты.
3. Классификация ресурсов и их контроль.
4. Безопасность персонала.
5. Физическая безопасность.
6. Администрирование компьютерных систем и сетей.
7. Управление доступом.
8. Разработка и сопровождение информационных систем.
9. Планирование бесперебойной работы организации.
10. Контроль выполнения требований политики безопасности.

В этих разделах содержится описание механизмов организационного уровня, реализуемых в настоящее время в государственных и коммерческих организациях во многих странах в виде соответствующих профилей защиты (рис. 6.6).Ключевые средства контроля (механизмы управления ИБ), предлагаемые в ISO 17799, считаются особенно важными.

Структура профиля защиты ИТ-продукта

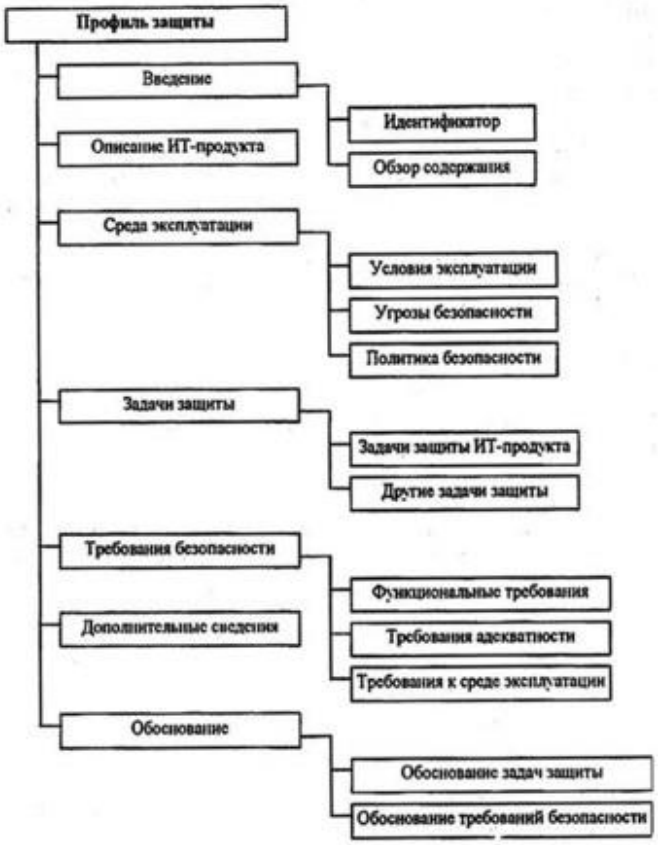


Рис. 6.6. Структура профиля защиты ИТ-продукта

При использовании некоторых из средств контроля, например шифрования, могут потребоваться советы специалистов по безопасности и оценка рисков. Для обеспечения защиты особенно ценных ресурсов или оказания противодействия особенно серьезным угрозам безопасности в ряде случаев могут потребоваться более сильные средства контроля, которые выходят за рамки ISO 17799.

Процедура аудита безопасности ИС по стандарту ISO 17799 включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту также является анализ и управление рисками. Семейство стандартов ISO 27000 по обеспечению безопасности и аудиту защиты, по управлению защитой и рисками в настоящее время активно развивается (рис. 6.7).

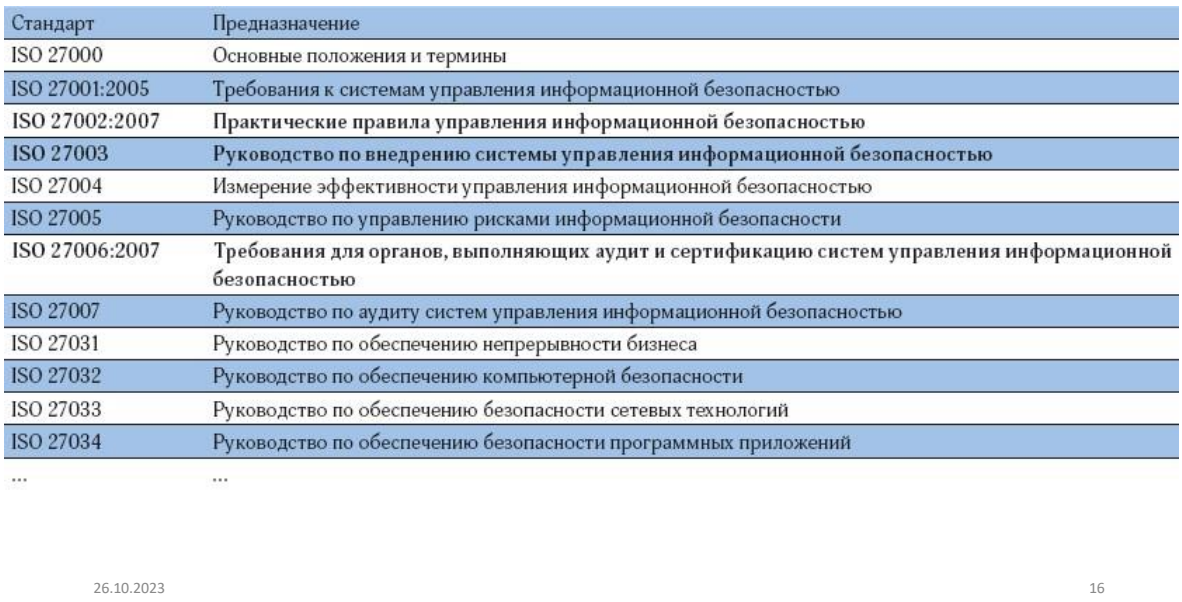


Рис. 6.7. Развитие семейства стандартов ISO 270...

На нижнем уровне разработаны в разных странах сотни отраслевых стандартов, нормативных документов и спецификаций по обеспечению ИБ, которые применяются национальными компаниями при разработке программных средств, ИС и обеспечении качества и безопасности их функционирования.

Технологии и инструменты обеспечения безопасности информации в системах и сетях

Основной особенностью любой сетевой структуры (системы) является то, что её компоненты распределены в пространстве и связь между ними осуществляется физически при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно, радиосвязь и т. п.) и программно — при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что, наряду с обычными (локальными) непреднамеренными действиями и атаками, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые (или удалённые) атаки (Remote Network Attacks). Они характеризуются, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых,

тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям.

С развитием локальных и глобальных сетей именно удалённые атаки становятся лидирующими как по количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных и информационных систем и сетей с точки зрения противостояния удалённым атакам приобретает первостепенное значение.

Современные сервисы безопасности функционируют в распределенной среде, поэтому необходимо учитывать наличие как локальных, так и сетевых угроз. В качестве общих можно выделить следующие угрозы:

- обход злоумышленником защитных средств;
- осуществление злоумышленником физического доступа к вычислительной установке, на которой функционирует сервис безопасности;
- ошибки администрирования, в частности, неправильная установка, ошибки при конфигурировании и т.п.;
- переход сервиса в небезопасное состояние в результате сбоя или отказа, при начальной загрузке, в процессе или после перезагрузки;
- маскарад пользователя (попытка злоумышленника выдать себя за уполномоченного пользователя, в частности, за администратора). В распределенной среде маскарад может реализовываться путем подмены исходного адреса или воспроизведения ранее перехваченных данных идентификации/аутентификации;
- маскарад сервера (попытка злоумышленника выдать свою систему за легальный сервер), следствием маскарада сервера может стать навязывание пользователю ложной информации или получение от пользователя конфиденциальной информации;
- использование злоумышленником чужого сетевого соединения или интерактивного сеанса (например, путем доступа к оставленному без присмотра терминалу);
- несанкционированное изменение злоумышленником конфигурации сервиса и/или конфигурационных данных;
- нарушение целостности программной конфигурации сервиса, в частности, внедрение троянских компонентов или получение контроля над сервисом;
- несанкционированный доступ к конфиденциальной (например, регистрационной) информации, в том числе несанкционированное расшифрование зашифрованных данных;
- несанкционированное изменение данных (например, регистрационной информации), в том числе таких, целостность которых защищена криптографическими методами;
- несанкционированный доступ к данным (на чтение и/или изменение) в процессе их передачи по сети;

- анализ потоков данных с целью получения конфиденциальной информации.
- перенаправление потоков данных (в частности, на системы, контролируемые злоумышленником);
- блокирование потоков данных;
- повреждение или утрата регистрационной, конфигурационной или иной информации, влияющей на безопасность функционирования сервиса (например, из-за повреждения носителей или переполнения регистрационного журнала);
- агрессивное потребление злоумышленником ресурсов, в частности, ресурсов протоколирования и аудита, а также полосы пропускания;
- сохранение остаточной информации в многократно используемых объектах.

Ввиду особой опасности таких атак — особенно для государственных предприятий и органов власти — к системам защиты информации предъявляются повышенные требования. Например, для защиты конфиденциальной информации в органах исполнительной власти следует удовлетворить следующие требования [Петренко С., Курбатов В., 2005].

1. Выбор конкретного способа подключения к сети Internet, в совокупности обеспечивающего межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры внутренней сети, проведение анализа защищенности узла Интернет, а также использование средств антивирусной защиты и централизованное управление средствами защиты должны производиться на основании рекомендаций документа Гостехкомиссии РФ СТР-К.
2. Автоматизированные системы защиты (АСЗ) организации должны обеспечивать защиту информации от несанкционированного доступа (НСД) по классу "1Г" в соответствии с "Руководящим документом" Гостехкомиссии РФ "РД. Автоматизированные системы. Защита от НСД к информации. Классификация АСЗ и требования по защите информации".
3. Средства вычислительной техники и программные средства АСЗ должны удовлетворять требованиям четвертого класса РД Гостехкомиссии России "РД. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации".
4. Программно-аппаратные средства межсетевого экранирования, применяемые для изоляции корпоративной сети от сетей общего пользования, должны удовлетворять требованиям "РД. Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации" по третьему классу защиты.

5. Информационные системы должны удовлетворять требованиям ГОСТ ИСО/ МЭК 15408 по защищенности информационных систем в рамках заданных профилей защиты.

6. Во исполнение приказа Госкомсвязи России от 25 декабря 1997 года №103 "Об организации работ по защите информации в отрасли связи и информатизации при использовании сети Internet" прямое подключение АРМ по управлению оборудованием сетей связи, мониторингу, обработки данных к сети Internet должно быть запрещено.

7. Программно-аппаратные средства криптографической защиты конфиденциальной информации, в том числе используемые для создания виртуальных защищенных сетей (VPN), должны иметь сертификаты ФАПСИ РФ.

8. Обязательным является использование средств ЭЦП для подтверждения подлинности документов.

9. Для введения использования персональных цифровых сертификатов и поддержки инфраструктуры открытых ключей для использования средств ЭЦП и шифрования необходимо создать легитимный удостоверяющий центр (систему удостоверяющих центров).

10. Политика информационной безопасности должна предусматривать обязательное включение в технические задания на создание коммуникационных и информационных систем требований информационной безопасности.

11. Должен быть регламентирован порядок ввода в эксплуатацию новых информационных систем, их аттестации по требованиям информационной безопасности.

Для выполнения перечисленных требований и надлежащей защиты конфиденциальной информации в государственных структурах принято использовать сертифицированные средства. Например, средства защиты от несанкционированного доступа (НСД), межсетевые экраны и средства построения VPN, средства защиты информации от утечки и прочие. В частности, для защиты информации от НСД рекомендуется использовать программно- аппаратные средства семейств Secret Net ("Информзащита"), Dallas Lock ("Конфидент"), "Аккорд" (ОКБ САПР), электронные замки "Соболь" ("Информзащита"), USB-токены ("Аладдин") и прочие. Для защиты информации, передаваемой по открытым каналам связи рекомендованы программно-аппаратные межсетевые экраны с функциями организации VPN, например, Firewall-1/VPN-1 (Check Point), "Застава" ("Элвис+"), VipNet ("Инфотекс"), "Континент" ("Информзащита"), ФПСН-IP ("АМИКОН") и другие.

Средства защиты информации для коммерческих структур более многообразны, среди них можно выделить следующие средства:

- управления обновлениями программных компонент АСЗ;
- межсетевого экранирования;

- построения VPN;
- контроля доступа;
- обнаружения вторжений и аномалий;
- резервного копирования и архивирования;
- централизованного управления безопасностью;
- предотвращения вторжений на уровне серверов;
- аудита и мониторинга средств безопасности;
- контроля деятельности сотрудников в сети Интернет;
- анализа содержимого почтовых сообщений;
- анализа защищенности информационных систем;
- защиты от спама;
- защиты от атак класса "Отказ в обслуживании" (DoS-атаки);
- контроля целостности;
- инфраструктура открытых ключей;
- усиленной аутентификации и прочие.

На основании политики информационной безопасности и указанных средств защиты информации (СЗИ) разрабатываются конкретные процедуры защиты, включающие распределение ответственности за их выполнение. Процедуры безопасности также важны, как и политики безопасности. Если политики безопасности определяют ЧТО должно быть защищено, то процедуры определяют КАК защитить информационные ресурсы компании и КТО конкретно должен разрабатывать, внедрять данные процедуры и контролировать их исполнение.

Технологическая модель подсистемы информационной безопасности

Современные распределенные корпорации, имеющие подразделения на разных континентах, имеют сложную техническую, инженерную и информационную инфраструктуру. Создание информационной сети такой корпорации и её эффективная защита является чрезвычайно сложной концептуальной и технологической задачей.

Первоначальное решение, характерное для последнего десятилетия прошлого века, использовать для формирования сети телефонные линии быстро привело к нагромождению коммуникаций и к невозможности эффективной защиты. Последующее создание и сопровождение собственных корпоративных сетей для обеспечения информационного обмена данными на базе таких линий связи стало обходиться в миллионы долларов.

Быстрое развитие технологий Internet, образование, рост и развитие "всемирной паутины" позволили создать достаточно дешевые и надежные коммуникации. Однако техническая надежность связи вовсе не означала безопасности корпоративных сетей, имеющих выходы в Интернет. Общие принципы построения Интернет и его использование как общедоступной сети с публичными сервисами привели к тому, что стало очень трудно обеспечить

надежную защиту от проникновения в корпоративные и государственные сети, построенные на базе протоколов TCP/IP и Internet -приложений — Web, FTP, e-mail и т.д.

Целевое назначение любой корпоративной информационной системы состоит в обеспечении пользователей необходимой информацией в режиме "On Line" и адекватном информационном сопровождении деятельности предприятия.

Базисом КИС является общесистемное программное обеспечение, которое включает операционную систему и программные оболочки, программы общего и прикладного назначения: автоматизированные рабочие места (АРМ) и Web-сервисы общего и специального назначения, СУБД и управление интегрированными вычислительными и мультимедийными приложениями, а также доступом в локальные и внешние сети (рис. 6.8).

Схема корпоративной информационной системы,
включающей локальные сети и выход в Internet

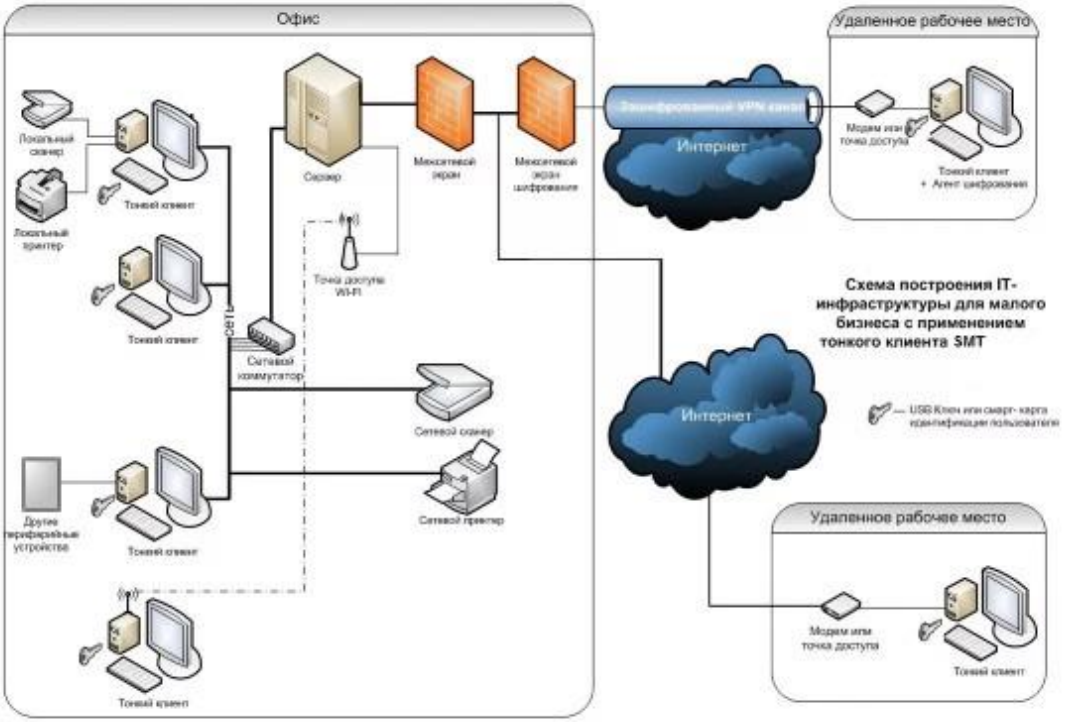


Рис. 6.8. Схема корпоративной информационной системы, включающей локальные сети и выход в Internet

Физически нижний уровень КИС базируется на серверах, рабочих станциях, персональных компьютерах различного назначения и коммуникационных устройствах, а также на программном обеспечении, реализующем работу перечисленных устройств. В связи с этим подсистема ИБ начинается с защиты именно этого программно-аппаратного оборудования. С этой целью можно использовать известные защитные средства операционных систем, антивирусные пакеты, средства и устройства аутентификации пользователя, средства криптографической защиты паролей и данных

прикладного уровня. Все эти средства образуют базу для реализации первого уровня технологической модели подсистемы ИБ (рис. 6.9) [Соколов А. В., Шаньгин В. Ф. 2002].

Рис. 6.9. Четырехуровневая технологическая модель подсистемы информационной безопасности

Второй физический уровень КИС — рабочие станции, серверы и персональные компьютеры объединятся в локальные сети, которые организуют внутреннее Intranet-пространство предприятия и могут быть иметь выходы во внешнее Internet-пространство. В этом случае речь идет о средствах информационной защиты (СЗИ) второго уровня — уровня защиты локальных сетей, который обычно включает:

- средства безопасности сетевых ОС;
- средства аутентификации пользователей (User Authentication Facilities — UAF);
- средства физического и программного разграничения доступа к распределенным и разделяемым информационным ресурсам;
- средства защиты домена локальной сети (Local Area Network Domain — LAND);
- средства промежуточного доступа (Proxy Server) и межсетевые экраны (Firewall);
- средства организации виртуальных локальных подсетей (Virtual Local Area Network — VLAN);

- средства обнаружения атаки и уязвимостей в системе защиты локальных сетей.

Следующий уровень реализации КИС — объединение нескольких локальных сетей географически распределенного предприятия в общую корпоративную Intranet-сеть через открытую сеть на базе современных технологий поддержки и сопровождения таких сетей (Quality of Service — QoS) с использованием открытой среды Internet в качестве коммутационной среды.

В этом случае на третьем уровне защиты КИС используются технологии защищенных виртуальных сетей (Virtual Private Networks — VPN). VPN-технологии часто интегрируются со средствами первого и второго уровней. Такой защищенный VPN-канал может простираться не только до маршрутизаторов доступа и пограничных Firewall'лов, но и до серверов и рабочих станций локальной сети.

Четвертый уровень защиты КИС — организация защищенного межкорпоративного обмена в среде электронного бизнеса (eBusiness). Методологической и технологической основой такой защиты являются методы и технологии управления публичными ключами и сертификатами криптографической защиты (Public Key Infrastructure — PKI). Суть этих технологий состоит в реализации двух глобальных функций: генерации и корректном распространении ключей и сертификатов и отслеживании их жизненного цикла. Базой для реализации средств защиты будут электронная цифровая подпись (Electronic Digital Signature — EDS) и VPN-технологии.

Отметим, что два нижних уровня защиты являются достаточно традиционными, так как они предназначены для обеспечения безопасности конкретной физически реализованной КИС. Верхние два уровня относятся к обеспечению безопасности передачи данных и электронного бизнеса, который осуществляется уже не в физическом, а в виртуальном пространстве, при этом VPN-технологии обеспечивают защищенный обмен данными в межкорпоративном пространстве, а PKI-технологии обеспечивают VPN-устройства ключами и сертификатами. В настоящее время на рынке имеется достаточное число технических и программных решений для защиты данных, информации, систем и сетей. Ниже рассмотрены некоторые базовые технологии на примере криптографической защиты данных, технологий межсетевых экранов, защищенных VPN-каналов связи, антивирусных и биометрических методов.

Технологии криптографической защиты информации

Криптография — это совокупность технических, математических, алгоритмических и программных методов преобразования данных (шифрование данных), которая делает их бесполезными для любого пользователя, у которого нет ключа для расшифровки. Криптографические преобразования обеспечивают решение следующих базовых задач защиты -

конфиденциальности (невозможности прочитать данные и извлечь полезную информацию) и целостности (невозможность модифицировать данные для изменения смысла или внесения ложной информации).

Технологии криптографии позволяют реализовать следующие процессы информационной защиты:

- идентификация (отождествление) объекта или субъекта сети или информационной системы;
- аутентификация (проверка подлинности) объекта или субъекта сети;
- контроль/разграничение доступа к ресурсам локальной сети или внесетевым сервисам;
- обеспечение и контроль целостности данных.

В соответствии с политиками безопасности используемые в компании технологии криптографии и специализированное программно-аппаратное обеспечение для защиты данных и документов, шифрования файлов и дисков реализуют следующие аспекты информационной защиты:

- шифруемые электронные письма и соединения VPN скрывают передаваемые данные от вирусов и сканеров содержимого;
- шифрование дисков не должно затруднять автоматическое резервное сохранение данных или управление файлами;
- сетевой администратор может не иметь права доступа к защищаемым файлам, содержащим конфиденциальную информацию, если это вызвано производственной необходимостью;
- когда сотрудник покидает предприятие, у его работодателя должна быть возможность доступа к зашифрованным данным, связанным с производственной деятельностью этого сотрудника;
- надежность шифрования и доступа должна быть обеспечена на длительное время;
- если при шифровании применяется метод открытого ключа, то помимо программного обеспечения необходимо построение инфраструктуры управления ключами или сертификатами;
- в случае попытки взлома системы или утечки секретной информации систему можно быстро перенастроить;
- широкое применение шифрования возможно лишь при условии простоты его обслуживания.

Общая схема простой криптосистемы показана на рис. 6.10, а на рис. 6.11 приведена схема симметричной криптосистемы с закрытым ключом [Соколов А. В., Шаньгин В. Ф., 2002].

Отправитель сообщения генерирует открытый текст сообщения $< M >$ для передачи по незащищенному каналу связи. Для того чтобы передаваемый текст невозможно было прочитать, отправитель преобразует

(шифрует) его с помощью алгоритма обратимого преобразования $< \mathrm{E}_k >$, формируя зашифрованный текст (криптограмму) $< \mathrm{C} = \mathrm{E}_k(\mathrm{M}) >$.

Адресат, получив криптограмму, применяет известное ему обратное преобразование $< D = \mathrm{E}_k^{-1} >$ и получает исходный открытый текст $\mathrm{M} :< D_k(C) = \mathrm{E}_k^{-1}(\mathrm{E}_k(\mathrm{M})) = M >$. Множество преобразований $\mathrm{E}_{\mathrm{к}i}$ образуют семейства криптоалгоритмов $\mathrm{E}_{\mathrm{к}}{}^N$. Параметр K, с помощью которого производится преобразование текста сообщения, называется ключом.

Общая схема криптосистемы

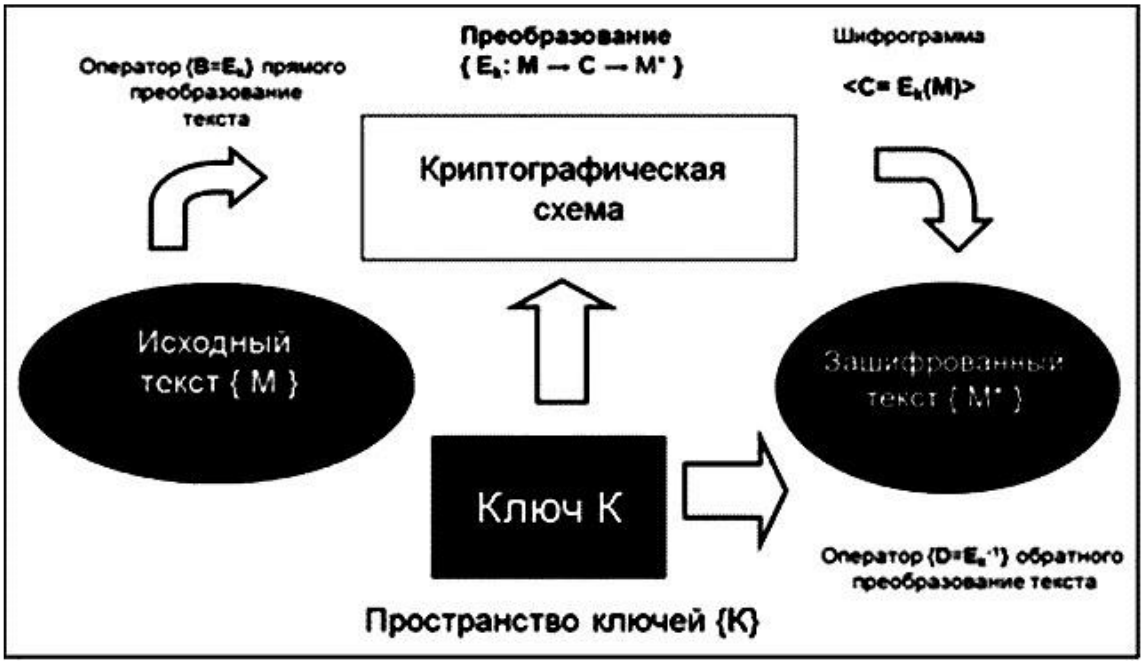


Рис. 6.10. Общая схема криптосистемы

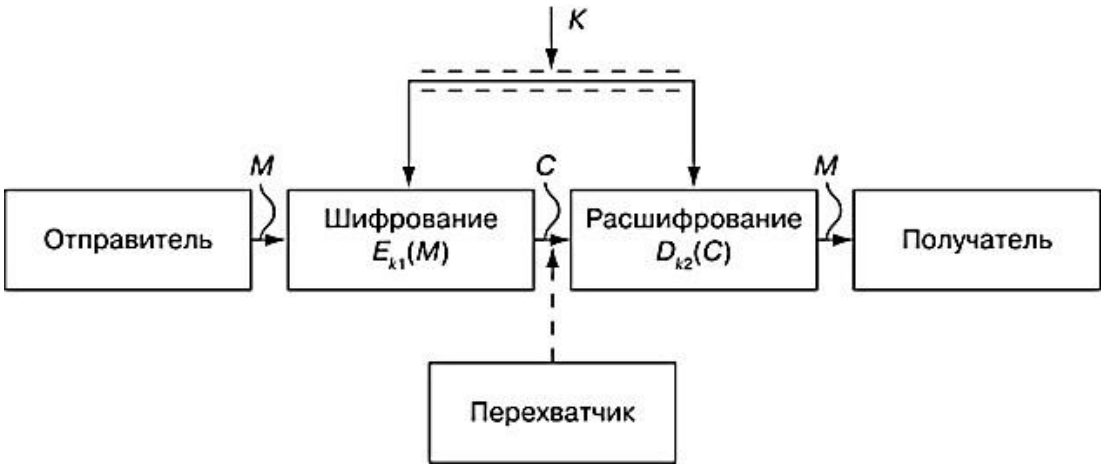
Такой ключ, по сути, является уникальным параметром — только его владелец (группа владельцев) может использовать этот ключ. Таким образом, криптографическая система по определению — это однопараметрическое семейство $E_k k \in K$ обратимых преобразований $< E_k : M \to C >$ из пространства M сообщений открытого текста в пространство C зашифрованных текстов. Параметр шифрования K (ключ) выбирается из конечного множества {K}, называемого пространством ключей.

Существует два класса криптосистем — симметричные (с одним ключом) и асимметричные (с двумя ключами). Симметричные криптосистемы (рис. 6.11) используют один и тот же ключ в процедурах шифрования и

расшифровки текста — и поэтому такие системы называются системами с секретным закрытым ключом.

Ключ должен быть известен только тем, кто занимается отправкой и получением сообщений. Таким образом, задача обеспечения конфиденциальности сводится к обеспечению конфиденциальности ключа. Передача такого ключа от адресата пользователю может быть выполнена только по защищенному каналу связи (рис. 6.11, пунктирная линия), что является существенным недостатком симметричной системы шифрования.

Схема симметричной криптосистемы с закрытым ключом

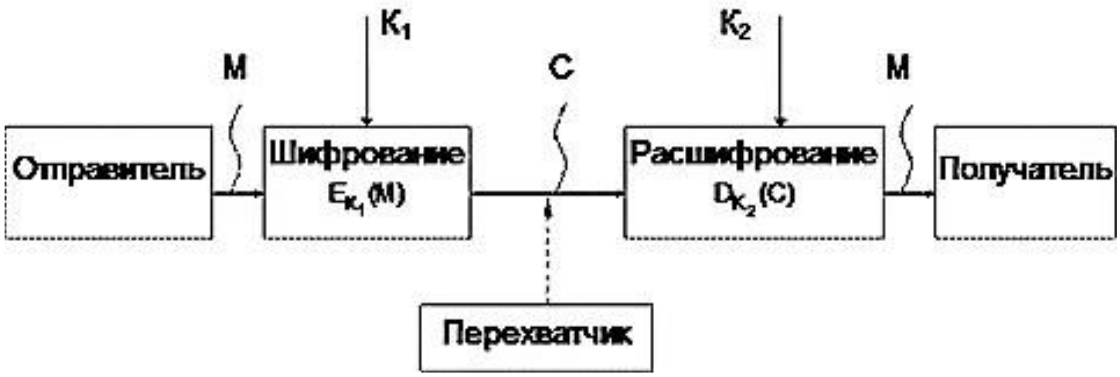


27.10.2023 20

Рис. 6.11. Схема симметричной криптосистемы с закрытым ключом

Такой вид шифрования наиболее часто используется в закрытых локальных сетях, в том числе входящих в КИС, для предотвращения НСД в отсутствие владельца ресурса. Таким способом можно шифровать как отдельные тексты и файлы, так и логические и физические диски.

Схема асимметричной криптосистемы с открытым ключом



27.10.2023 21

Рис. 6.12. Схема асимметричной криптосистемы с открытым ключом

Асимметричные криптосистемы используют различные ключи (рис. 6.12):

- открытый ключ K_1 используется для шифрования данных и вычисляется по параметрам секретного ключа K_2;
- секретный ключ K_2 используется для расшифровки информации, зашифрованной с помощью парного ему открытого ключа K_1.

Открытый и секретный ключи и K_2 генерируются попарно, при этом ключ K_2 остается у его владельца и должен быть надежно защищен от НСД. Копии ключа K_1 распространяются среди пользователей сети, с которыми обменивается информацией обладатель секретного ключа K_2. Таким образом, в асимметричной криптосистеме ключ $K1$ свободно передается по открытым каналам связи, а секретный ключ K_2 хранится на месте его генерации.

Система защиты информации называется криптостойкой, если в результате предпринятой злоумышленником атаки на зашифрованное послание невозможно расшифровать перехваченный зашифрованный текст C для получения открытого текста M или зашифровать текст злоумышленника M' для передачи правдоподобного зашифрованного текста C' с искаженными данными.

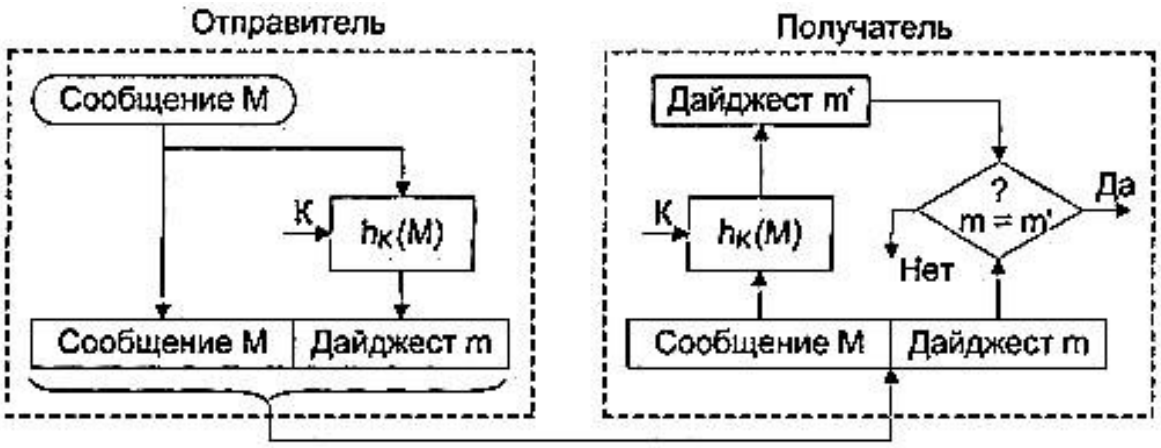
В настоящее время используется следующий подход реализации криптозащиты — криптосистема, реализующая семейство криптографических преобразований $E_k k \in K$, является открытой системой. Это очень важный принцип криптозащиты, так как защищенность системы не должна зависеть от того, чего нельзя было бы быстро перенастроить в случае необходимости, если произошла утечка секретной информации. Изменение программно-аппаратой части системы защиты информации требует значительных финансовых и временных затрат, а изменение ключей является несложным делом. Именно поэтому стойкость криптосистемы определяется, в основном, секретностью ключа K_2.

Формальные математические методы криптографии были разработаны Клодом Шенноном ("Математическая теория криптографии", 1945 г.). Он доказал теорему о существовании и единственности абсолютно стойкого шифра — это такая система шифрования, когда текст однократно зашифровывается с помощью случайного открытого ключа такой же длины.

В 1976 году американские математики У.Диффи и М.Хеллман обосновали методологию асимметричного шифрования с применением открытой однонаправленной функции (это такая функция, когда по её значению нельзя восстановить значение аргумента) и открытой однонаправленной функции с секретом.

В 90-е годы XX века профессор Массачусетского технологического института (MIT, USA) Рональд Ривест разработал метод шифрования с помощью особого класса функций — хэш-функций (Hash Function). Это был алгоритм шифрования MD6 хэширования переменной разрядности. Хэш-функция (дайджест-функция) — это отображение, на вход которого подается сообщение переменной длины M, а выходом является строка фиксированной длины $h(M)$ — дайджест сообщения (рис. 6.13).

Схема однонаправленной хэш-функции с параметром-ключом



27.10.2023 22

Рис. 6.13. Однонаправленной хэш-функции с параметром-ключом

Криптостойкость такого метода шифрования состоит в невозможности подобрать документ M', который обладал бы требуемым значением хэш-функции. Параметры вычисления хэш-функции h являются семейством ключей K^N. В настоящее время на этих принципах строятся алгоритмы формирования электронной цифровой подписи (ЭЦП).

Наиболее известными симметричными алгоритмами шифрования в настоящее время являются DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), RC2, RC5, CAST, Blowfish. Асимметричные алгоритмы — RSA (R.Rivest, A.Shamir, L.Adleman), алгоритм Эль Гамаля (ElGamal), криптосистема ECC на эллиптических кривых, алгоритм открытого распределения ключей Диффи-Хеллмана.

Алгоритмы, основанные на применении хэш-функций — MD4 (Message Digest 4), MD5 (Message Digest 5), SHA (Secure Hash Algorithm) [Соколов А.В., Шаньгин В.Ф., 2002].

Наиболее известным программным продуктом, распространяемым свободно, является пакет PGP (Pretty Good Privacy). Пакет разработан Филом Циммерманом (Phil Zimmerman) в 1995 году, который использовал упомянутые алгоритмы RSA, IDEA, и MD5. PGP состоит из трёх частей — алгоритма IDEA, сигнатуры и цифровой подписи. PGP использует три ключа — открытый ключ адресата, секретный ключ владельца и сеансовый ключ,

генерируемый при помощи RSA и открытого ключа случайным образом при шифровании сообщения (рис. 6.14). Информацию об этом продукте можно получить по адресу: http://www.mit.edu/network/pgp-form.html.

Рис. 6.14. Схема формирования защищенного сообщения с помощью пакета PGP

Выбор алгоритма шифрования, кроме обязательного DES, зависит от разработчика. Это создает дополнительное преимущество, так как злоумышленник должен определить, какой шифр следует вскрыть. Если добавить необходимость подбора ключей, то шансы расшифровки существенно уменьшаются.

Примером простого и эффективного протокола управления криптографическими ключами в сетях является протокол SKIP (Simple Key management for Internet Protocol), представленный в 1994 году компанией Sun Microsystems (США). Это открытая спецификация, её свободно можно использовать для разработки средств защиты информации в Internet-сетях. Ряд компаний успешно применяет этот протокол для коммерческих разработок СЗИ: Swiss Institute of Technology (Швейцария), Check Point Software Inc. (США, Израиль), Toshiba (Япония), ЭЛВИС+ (Россия), VPNet (США).

Схема формирования ЭЦП

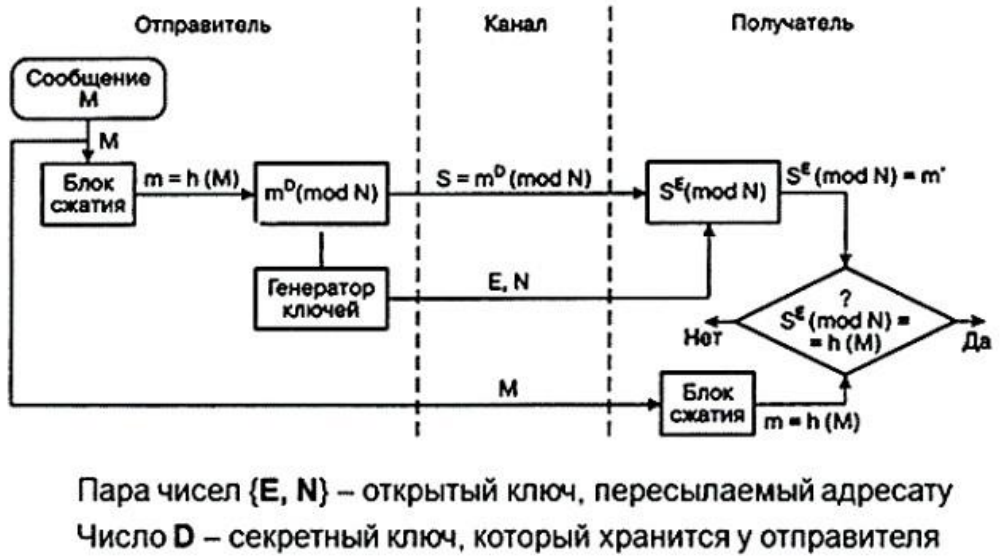


Рис. 6.15. Схема формирования ЭЦП

В России установлен единый алгоритм криптографических преобразований данных для систем обработки и передачи данных в сетях, который установлен стандартом ГОСТ 28147-89. Другой российский стандарт — ГОСТ Р 34.11-2012 — определяет алгоритм и процедуру вычисления хэш-функций для любых последовательностей двоичных символов, используемых в криптографических методах защиты информации. Отечественный стандарт ГОСТ Р 34.10-94 является стандартом, определяющим алгоритм формирования ЭЦП (рис. 6.15).

Технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны

Межсетевой экран (брандмауэр, Firewall) — программно-аппаратная система межсетевой защиты, которая отделяет одну часть сети от другой и реализует набор правил для прохождения данных из одной части в другую. Границей является раздел между локальной корпоративной сетью и внешними Internet-сетями или различными частями локальной распределенной сети. Экран фильтрует текущий трафик, пропуская одни пакеты информации и отсеивая другие.

Межсетевой экран (МЭ) является одним из основных компонентов защиты сетей. Наряду с Internet-протоколом межсетевого обмена (Internet Security Protocol — IPSec) МЭ является одним из важнейших средств защиты, осуществляя надежную аутентификацию пользователей и защиту от НСД.

Отметим, что большая часть проблем с информационной безопасностью сетей связана с "прародительской" зависимостью коммуникационных решений от ОС UNIX — особенности открытой платформы и среды программирования UNIX сказались на реализации протоколов обмена данными и политики информационной безопасности. Вследствие этого ряд Internet-служб и совокупность сетевых протоколов (Transmission Control Protocol/Internet Protocol — TCP/IP) имеет "бреши" в защите [Левин М., 2001].

К числу таких служб и протоколов относятся:

- служба сетевых имен (Domain Name Server — DNS);
- доступ к всемирной паутине WWW;
- программа электронной почты Send Mail;
- служба эмуляции удаленного терминала Telnet;
- простой протокол передачи электронной почты (Simple Mail Transfer Protocol — SMTP);
- протокол передачи файлов (File Transfer Protocol);
- графическая оконная система X Windows.

Настройки МЭ, т.е. решение пропускать или отсеивать пакеты информации, зависят от топологии распределенной сети и принятой политики информационной безопасности. В связи с этим политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Эти правила базируются на двух общих принципах — запрещать всё, что не разрешено в явной форме, и разрешать всё, что не запрещено в явной форме. Использование первого принципа дает меньше возможностей пользователям и охватывает жёстко очерченную область сетевого взаимодействия. Политика, основанная на втором принципе, является более мягкой, но во многих случаях она менее желательна, так как она предоставляет пользователям больше возможностей "обойти" МЭ и использовать запрещенные сервисы через нестандартные порты (User Data Protocol — UDP), которые не запрещены политикой безопасности.

Функциональные возможности МЭ охватывают следующие разделы реализации информационной безопасности:

- настройку правил фильтрации;
- администрирование доступа во внутренние сети;
- фильтрацию на сетевом уровне;
- фильтрацию на прикладном уровне;
- средства сетевой аутентификации;
- ведение журналов и учет.

Программно-аппаратные компоненты МЭ можно отнести к одной из трёх категорий: фильтрующие маршрутизаторы, шлюзы сеансового уровня и шлюзы уровня приложений. Эти компоненты МЭ — каждый отдельно и в

различных комбинациях — отражают базовые возможности МЭ и отличают их один от другого.

Фильтрующий маршрутизатор (Filter Router — FR) фильтрует IP-пакеты по параметрам полей заголовка пакета: IP-адрес отправителя, IP-адрес адресата, TCP/UDP-порт отправителя и TCP/UDP-порт адресата. Фильтрация направлена на безусловное блокирование соединений с определенными хостами и/или портами — в этом случае реализуется политика первого типа.

Формирование правил фильтрации является достаточно сложным делом, к тому же обычно отсутствуют стандартизированные средства тестирования правил и корректности их исполнения. Возможности FR по реализации эффективной защиты ограничены, так как на сетевом уровне эталонной модели OSI обычно он проверяет только IP-заголовки пакетов. К достоинствам применения FR можно отнести невысокую стоимость, гибкость формирования правил, незначительную задержку при передаче пакетов. Недостатки FR достаточно серьезны, о них следует сказать более подробно:

- отсутствует аутентификация конкретного пользователя;
- указанную выше аутентификацию по IP-адресу можно "обойти" путем замещения информации пользователя информацией злоумышленника, использующего нужный IP-адрес;
- внутренняя сеть "видна" из внешней сети;
- правила фильтрации сложны в описании и верификации, они требуют высокой квалификации администратора и хорошего знания протоколов TCP/UDP;
- нарушение работы ФМ приводит к полной незащищенности всех компьютеров, которые находятся за этим МЭ.

Шлюз сеансового уровня (Session Level Gateway — SLG) —активный транслятор TCP соединения. Шлюз принимает запрос авторизованного клиента на предоставление услуг, проверяет допустимость запрошенного сеанса (Handshaking), устанавливает нужное соединение с адресом назначения внешней сети и формирует статистику по данному сеансу связи. После установления факта, что доверенный клиент и внешний хост являются "законными" (авторизованными) участниками сеанса, шлюз транслирует пакеты в обоих направлениях без фильтрации. При этом часто пункт назначения оговаривается заранее, а источников информации может быть много (соединение "один-ко-многим") — это, например, типичный случай использования внешнего Web-ресурса.

Используя различные порты, можно создавать различные конфигурации соединений, обслуживая одновременно всех пользователей, имеющих право на доступ к ресурсам сети. Существенным недостатком SLG является то, что после установления связи пакеты фильтруются только на сеансовом уровне модели OSI без проверки их содержимого на уровне прикладных программ. Авторизованный злоумышленник может спокойно транслировать

вредоносные программы через такой шлюз. Таким образом, реализация защиты осуществляется, в основном, на уровне квитирования (Handshaking).

Шлюз уровня приложений (Application Layer Gateway — ALG). Для компенсации недостатков FR и SLG шлюзов в межсетевые экраны встраивают прикладные программы для фильтрации пакетов при соединениях с такими сервисами, как Telnet и FTP и пр. Эти приложения называются Proxy-службами, а устройство (хост), на котором работает служба, называется шлюзом уровня приложений. Шлюз исключает прямое взаимодействие между авторизованным пользователем и внешним хостом. Зафиксировав сетевой сеанс, шлюз останавливает его и вызывает уполномоченное приложение для реализации запрашиваемой услуги — Telnet, FTP, WWW или E-mail. Внешний пользователь, который хочет получить услугу соединения в сети, соединяется вначале с ALG, а затем, пройдя предусмотренные политикой безопасности процедуры, получает доступ к нужному внутреннему узлу (хосту). Отметим явные преимущества такой технологии:

- уполномоченные приложения вызывают только те службы, которые прописаны в сфере их действия, исключая все остальные, которые не отвечают требованиям информационной безопасности в контексте запрашиваемой услуги;
- уполномоченные приложения обеспечивают фильтрацию протокола — например, некоторые ALG могут быть настроены на фильтрацию FTP соединения и запрещают при этом выполнение команды <FTP put>, что однозначно не позволяет передавать информацию на анонимный FTP-сервер;
- шлюзы прикладного уровня, как правило, фиксируют в специальном журнале выполняемые сервером действия и в случае необходимости сообщают сетевому администратору о возможных коллизиях и попытках проникновения;
- структура внутренней сети не видна из Internet-сети, шлюз осуществляет надежную аутентификацию и регистрацию, правила фильтрации просты, так как экран пропускает прикладной трафик, предназначенный только для шлюза прикладного уровня, блокируя весь остальной.

Как показывает практика, защита на уровне приложений позволяет дополнительно осуществлять другие проверки в системе защиты информации — а это снижает опасность "взлома" системы, имеющей "прорехи" в системе безопасности.

Межсетевые экраны можно разделить по следующим основным признакам:

- по исполнению: программный и программно-аппаратный;

- по используемой технологии: контроль состояния протокола (Stateful Inspection Protocol) или с использованием модулей посредников (Proxy Server);
- по функционированию на уровнях эталонной модели OSI (Open System Interconnection): шлюзы экспертного, прикладного, сеансового уровней, пакетный фильтр;
- по схеме подключения: схема единой защиты сети; схема с закрытым и не защищаемым открытым сегментами сети; схема с раздельной защитой закрытого и открытого сегментов сети.

На рис. 6.16 показан вариант защиты локальной сети на базе программно-аппаратного решения — межсетевого экрана Cisco 2610 & PIX Firewall 520 компании Cisco Systems [Соколов А. В., Шаньгин В. Ф., 2002]. Отличительной особенностью этой модели является специальная ОС реального времени, а высокая производительность реализуется на базе алгоритма адаптивной безопасности (Adaptive Security Algorithm — ASA).

Рис. 6.16. Использование комплекса "маршрутизатор-файервол" в системах защиты информации при подключении к Internet

Приведенное решение имеет несомненные достоинства: высокая производительность и пропускная способность до 4 Гб/сек; возможность поддержки до 256 тысяч одновременных сессий; объединение преимуществ пакетного и прикладного шлюзов, простота и надежность в установке и эксплуатации, возможность сертификации в Государственной технической комиссии РФ.

В заключение отметим, что межсетевые экраны, естественно, не решают всех вопросов информационной безопасности распределенных КИС и локальных сетей — существует ряд ограничений на их применение и ряд угроз, от которых МЭ не могут защитить. Отсюда следует, что технологии МЭ следует применять комплексно — с другими технологиями и средствами защиты.

Концепция защищенных виртуальных частных сетей

При выходе локальной сети в открытое Internet-пространство возникают угрозы двух основных типов: несанкционированный доступ (НСД) к данным в процессе их передачи по открытой сети и НСД к внутренним ресурсам КИС.

Информационная защита при передаче данных по открытым каналам реализуется следующими мерами:

- взаимная аутентификация сторон;
- прямое и обратное криптографическое преобразование данных;
- проверка достоверности и целостности полученных данных.

Организация защиты с использованием технологии виртуальных частных сетей (Virtual Private Network — VPN) подразумевает формирование защищенного "виртуального туннеля" между узлами открытой сети, доступ в который невозможен потенциальному злоумышленнику. Преимущества этой технологии очевидны: аппаратная реализация довольно проста, нет необходимости создавать или арендовать дорогие выделенные физические сети, можно использовать открытый дешевый Internet, скорость передачи данных по туннелю такая же, как по выделенному каналу.

В настоящее время существует четыре вида архитектуры организации защиты информации на базе применения технологии VPN [Соколов А. В., Шаньгин В. Ф., 2002].

Локальная сеть VPN (Local Area Network-VPN). Обеспечивает защиту потоков данных и информации от НСД внутри сети компании, а также информационную безопасность на уровне разграничения доступа, системных и персональных паролей, безопасности функционирования ОС, ведение журнала коллизий, шифрование конфиденциальной информации.

Внутрикорпоративная сеть VPN (Intranet-VPN). Обеспечивает безопасные соединения между внутренними подразделениями распределенной компании.

Для такой сети подразумевается:

- использование мощных криптографических средств шифрования данных;
- обеспечение надежности работы критически важных транзакционных приложений, СУБД, электронной почты, Telnet, FTP;
- скорость и производительность передачи, приема и использования данных;
- гибкость управления средствами подключения новых пользователей и приложений.

Сети VPN с удаленным доступом (Internet-VPN). Обеспечивает защищенный удаленный доступ удаленных подразделений распределённой компании и мобильных сотрудников и отделов через открытое пространство Internet (рис. 6.17).

Такая сеть организует:

- адекватную систему идентификации и аутентификации удалённых и мобильных пользователей;

- эффективную систему управления ресурсами защиты, находящимися в географически распределенной информационной системе.

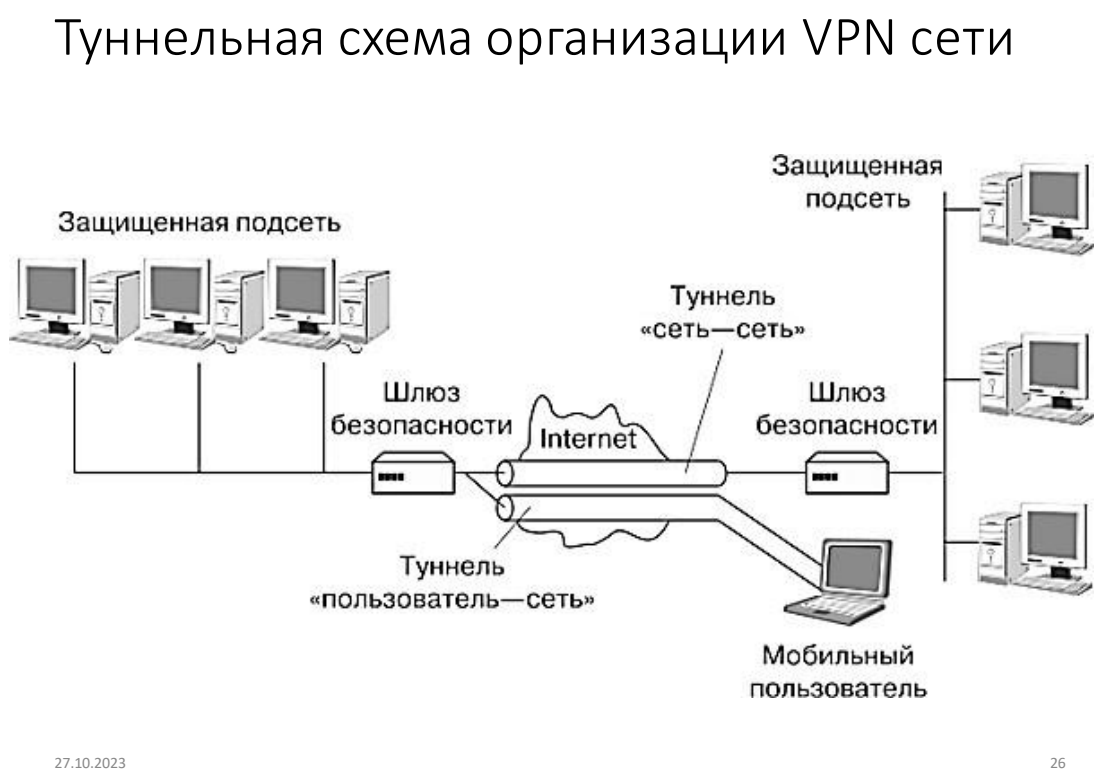


Рис. 6.17. Туннельная схема организации VPN сети

Межкорпоративная сеть VPN (Extranet-VPN). Обеспечивает эффективный защищённый обмен информацией с поставщиками, партнёрами, филиалами корпорации в других странах. Такая сеть предусматривает использование стандартизированных и надёжных VPN-продуктов, работающих в открытых гетерогенных средах и обеспечивающих максимальную защищенность конфиденциального трафика, включающего аудио и видео потоки информации — конфиденциальные телефонные переговоры и телеконференции с клиентами.

Можно выделить два основных способа технической реализации виртуальных туннелей:

- построение совокупности соединений (Frame Relay или Asynchronous Transfer Mode) между двумя нужными точками единой сетевой инфраструктуры, надежно изолированной от других пользователей механизмом организации встроенных виртуальных каналов;
- построение виртуального IP-туннеля между двумя узлами сети на базе использования технологии туннелирования, когда каждый пакет информации шифруется и "вкладывается" в поле нового пакета специального вида (конверт), который и передается по IP-туннелю — при этом пакет

протокола более низкого уровня помещается в поле данных пакета более высокого уровня (рис. 6.18).

Схема пакета, подготовленного к отправке по туннелю

27.10.2023 27

Рис. 6.18. Схема пакета, подготовленного к отправке по туннелю

VPN-туннель обладает всеми свойствами защищенной выделенной линии, проходящей через открытое пространство Internet. Особенность технологии туннелирования состоит в том, что она позволяет зашифровать не только поле данных, а весь исходный пакет, включая заголовки. Это важная деталь, так как из заголовка исходного пакета злоумышленник может извлечь данные о внутренней структуре сети — например, информацию о количестве локальных сетей и узлов и их IP-адресах.

Зашифрованный пакет, называемый SKIP-пакетом, инкапсулируется в другой пакет с открытым заголовком, который транспортируется по соответствующему туннелю (рис. 6.19).

При достижении конечной точки туннеля из внешнего пакета извлекается внутренний, расшифровывается, и его заголовок используется для дальнейшей передачи во внутренней сети или подключенному к локальной сети мобильному пользователю. Туннелирование применяется не только для обеспечения конфиденциальности внутреннего пакета данных, но и для его целостности и аутентичности, механизм туннелирования часто применяется в различных протоколах формирования защищенного канала связи. Технология позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол.

Таким образом, можно реализовать взаимодействие нескольких разнотипных сетей, преодолевая несоответствие внешних протоколов и схем адресации.

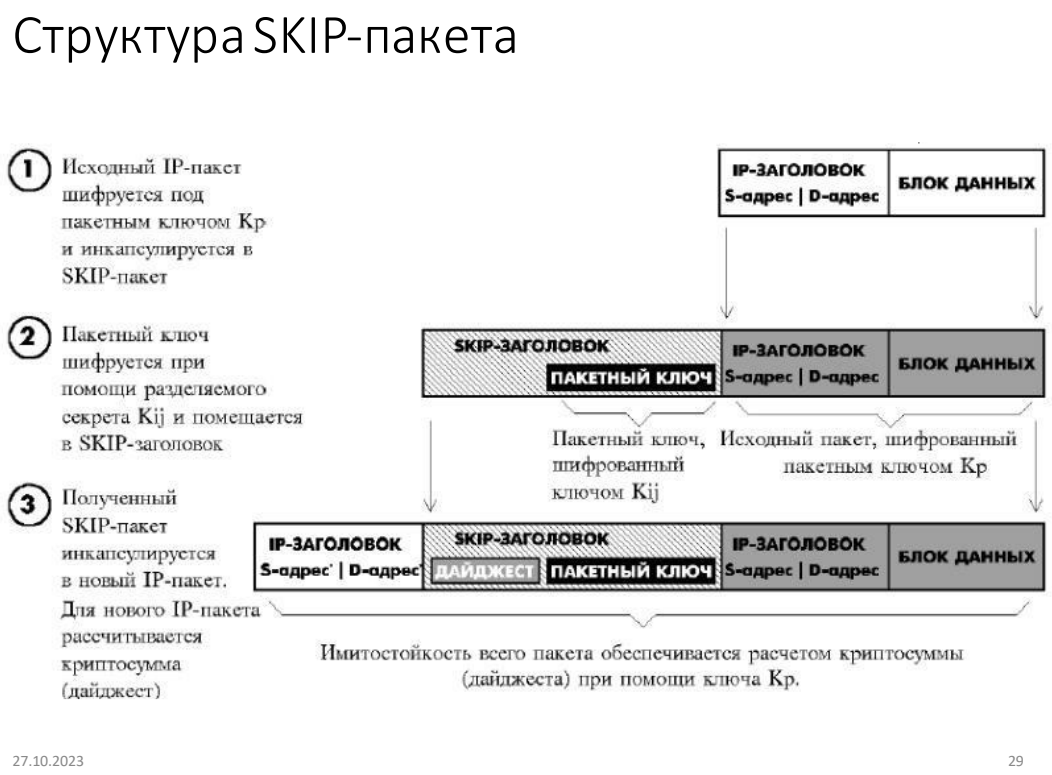


Рис. 6.19. Структура SKIP-пакета

Средства построения защищенной VPN достаточно разнообразны — они могут включать маршрутизаторы с механизмом фильтрации пакетов (Filtering Router), многофункциональные межсетевые экраны (Multifunction Firewall), промежуточные устройства доступа в сеть (Proxy Server), программно-аппаратные шифраторы (Firmware Cryptograph). По технической реализации можно выделить следующие основные виды средств формирования VPN:

- специализированные программные решения, дополняющие стандартную операционную систему функциями VPN;
- программно-аппаратное устройство на базе специализированной ОС реального времени, имеющее два или несколько сетевых интерфейсов и аппаратную криптографическую поддержку;
- средства VPN, встроенные в стандартный маршрутизатор или коммутатор;
- расширение охвата защищаемой зоны канала передачи и приёма данных за счет дополнительных функций межсетевого экрана.

Туннели VPN создаются для различных типов конечных пользователей: это может быть локальная сеть (Local Area Network — LAN) со шлюзом безопасности (Security Gateway) или отдельные компьютеры удаленных или мобильных пользователей с сетевым программным обеспечением для шифрования и аутентификации трафика — клиенты VPN (рис. 6.17). Через шлюз безопасности проходит весь трафик для внутренней корпоративной сети. Адрес шлюза VPN указывается как внешний адрес входящего туннелируемого пакета, а расшифрованный внутренний адрес пакета является адресом конкретного хоста за шлюзом.

Наиболее простым и относительно недорогим способом организации VPN-канала является схема, в соответствии с которой защищенный туннель прокладывается только в открытой сети для транспортировки зашифрованных пакетов. В качестве конечных точек туннеля выступают провайдеры Internet-сети или пограничные межсетевые экраны (маршрутизаторы) локальной сети. Защищенный туннель формируется компонентами виртуальной сети, функционирующим на узлах, между которыми он создается. В настоящее время активно функционирует рынок VPN-средств — приведем некоторые примеры популярных и широко используемых решений для каждого класса продуктов.

VPN на базе сетевых операционных систем. Для формирования виртуальных защищённых туннелей в IP сетях сетевая операционная система Windows NT использует протокол PPTP (Point-to-Point Transfer Protocol). Туннелирование информационных пакетов производится инкапсулированием и шифрованием (криптоалгоритм RSA RC4) стандартных блоков данных фиксированного формата (PPP Data Frames) в IP-дейтаграммы, которые и передаются в открытых IP-сетях. Данное решение является недорогим, и его можно эффективно использовать для формирования VPN-каналов внутри локальных сетей, домена Windows NT или для построения Internet- и Extranet-VPN для небольших компаний малого и среднего бизнеса для защиты не критичных приложений.

VPN на базе маршрутизаторов. В России лидером на рынке VPN-продуктов является компания Cisco Systems. Построение каналов VPN на базе маршрутизаторов Cisco осуществляется средствами ОС версии Cisco IOS 12.x. Для организации туннеля маршрутизаторы Cisco используют протокол L2TP канального уровня эталонной модели OSI, разработанного на базе "фирменных" протоколов Cisco L2F и Microsoft PPTP, и протокол сетевого уровня IPSec, созданного ассоциацией "Проблемная группа проектирования Internet (Internet Engineering Task Force — IETF). Эффективно применяется Cisco VPN Client, который предназначен для создания защищенных соединений Point-to Point между удаленными рабочими станциями и маршрутизаторами Cisco — это позволяет построить практически все виды VPN-соединений в сетях.

VPN на базе межсетевых экранов. Эта технология считается наиболее сбалансированной и оптимальной с точки обеспечения комплексной безопасности КИС и её защиты от атак из внешней открытой сети. В России нашел широкое применение программный продукт Check Point Firewall-1/VPN-1 компании Check Point Software Technologies. Это решение позволяет построить глубоко комплексную эшелонированную систему защиты КИС.

В состав продукта входят: Check Point Firewall-1, набор средств для формирования корпоративной виртуальной частной сети Check Point VPN-1, средства обнаружения атак и вторжений Real Secure, средства управления полосой пропускания информационных пакетов Flood Gate, средства VPN-1 Secure Remote, VPN-1 Appliance и VPN-1 Secure Client для построения Localnet/Intranet/Internet/Extranet VPN-каналов. Весь набор продуктов Check Point VPN-1 построен на базе открытых стандартов IPSec, имеет развитую систему идентификации и аутентификации пользователей, взаимодействует с внешней системой распределения открытых ключей PKI, поддерживает централизованную систему управления и аудита.

На российском рынке можно указать два продукта, получивших достаточно широкую известность — это криптографический комплекс "Шифратор IP пакетов" производства объединения МО ПН ИЭИ (http://www.security.ru) и ряд программных продуктов ЗАСТАВА компании ЭЛВИС+ (http://www.elvis.ru). Самым быстрорастущим сегментом рынка систем информационной безопасности по исследованиям IDC, Price Waterhouse Cooper и Gartner Group являются системы блокировки корпоративных каналов связи. Быстрее всего растут продажи систем защиты от утечек внутренней информации (Intrusion Detection and Prevention — IDP), которые позволяют контролировать трафик электронной почты и доступ к внешним Internet-ресурсам.

Антивирусная защита

История появления вирусописательства чрезвычайно интересна — она ещё ждёт своего дотошного исследователя! До сих пор нет единого мнения относительно момента, который можно было бы считать официальным днём появления вируса, как не существовало и критериев, под которые можно было бы подвести то или иное ПО и отличить исследовательские эксперименты от целенаправленно написанной программы с вредоносными функциями.

В 1949 году Джон фон Нейман (John von Naumann), выдающийся американский математик венгерского происхождения, сделавший важный вклад в квантовую физику, квантовую логику, функциональный анализ, теорию множеств, информатику, экономику и другие отрасли науки, разработал математическую теорию создания самовоспроизводящихся программ. Это была первая попытка создать теорию такого явления, но она не вызвала большого интереса у научного сообщества, так как не имела видимого прикладного значения.

Нет согласия и по поводу происхождения названия "компьютерный вирус". По одной из версий это случилось 10 ноября 1983 года, когда аспирант Университета Южной Калифорнии (University of Southern California) Фред Коэн (Fred Cohen) во время семинара по безопасности в Лехайском университете (Пенсильвания, США) продемонстрировал на системе VAX 11/750 программу, способную внедряться в другие программные объекты. Эту программу можно с полным правом считать одним из первых прототипов компьютерного вируса.

Коэн внедрил написанный им код в одну из Unix-команд, и в течение пяти минут после запуска её на вычислительной машине получил контроль над системой. В четырёх других демонстрациях полного доступа удавалось добиться за полчаса, оставив поверженными все существовавшие в то время защитные механизмы.

Существует версия, что термином "вирус" назвал копирующую саму себя программу научный руководитель Фреда, один из создателей криптографического алгоритма RSA Леонард Эдлеман (Leonard Adleman).

Годом позже, на 7-й конференции по безопасности информации, Ф.Коэн дает научное определение термину "компьютерный вирус", как программе, способной "заражать" другие программы при помощи их модификации с целью внедрения своих копий и выполнения заданных действий. Отметим, что Ф.Коэн определённо не был новатором в этой области. Теоретические рассуждения о распространяющихся копированием с компьютера на компьютер программах и практическая реализация успешно осуществлялись и раньше. Однако именно презентация Ф.Коэна заставила специалистов серьёзно заговорить о потенциальном ущербе от преднамеренных атак. Всего через пятнадцать лет распространение вредоносного программного обеспечения приобрело угрожающие масштабы, радикально снизить которые не представляется возможным.

В некотором смысле опередил Ф. Коэна 15-летний школьник из Пенсильвании Рик Скрента (Rich Skrenta). Его излюбленным занятием было подшучивание над товарищами путём модификаций кода игр для Apple II, которые приводили к внезапному выключению компьютеров или выполняли другие действия. В 1982 году он написал Elk Cloner — самовоспроизводящийся загрузочный вирус, инфицировавший Apple II через гибкий магнитный диск. Во время каждой 50-й перезагрузки ПК появлялось сообщение со словами: "Он завладеет вашими дисками, он завладеет вашими чипами. Да, это Cloner! Он прилипнет к вам как клей, он внедрится в память. Cloner приветствует вас!"

Программа Р.Скрента не вышла далеко за пределы круга его друзей. Лавры достались "шедевру" программистской мысли, появившемуся несколькими годами позже. Программу Brain ("Мозг") создали в 1988 году двое братьев — выходцев из Пакистана, которым приписывается инфицирование ПК через созданные ими нелегальные копии программы для

мониторинга работы сердца. Вирус содержал уведомление об авторском праве с именами и телефонами братьев, поэтому пользователи заражённых машин могли обратиться к напрямую к вирусописателям за "вакциной". За первой версией Brain последовало множество модификаций, преследовавших сугубо коммерческий интерес.

В 1988 году аспирант Корнельского университета (Cornell University) Роберт Теппен Моррис младший (Robert Tappan Morris Jr.), приходившийся сыном главному научному сотруднику Агентства национальной безопасности США (National Security Agency), выпустил в свет первый широко распространившийся компьютерный червь, хотя экспериментальные работы в этой области проводились с конца 1970-х годов. Этот тип программ чаще всего не производит никаких деструктивных манипуляций с файлами пользователя и ставит целью как можно более быстрое и широкое распространение, снижая эффективность работы сетей.

По некоторым оценкам, от 5% до 10% подключённых в то время к Сети машин, по большей части принадлежавших университетам и исследовательским организациям, были атакованы им. Червь использовал уязвимости нескольких программах, в том числе Sendmail. Р.Т.Моррис стал первым человеком, осуждённым по обвинению в преступлениях в компьютерной сфере, и получил 3 года условно. Однако это не помешало ему впоследствии стать профессором Массачусетского технологического института (MIT).

Следующий большой шаг вредоносное ПО совершило в 90-х годах с ростом спроса на персональные компьютеры и количества пользователей электронной почты. Электронные коммуникации предоставили гораздо более эффективный путь инфицирования ПК, чем через носители информации. Образцом скорости распростанения стал вирус Melissa в 1999 году, внедрившийся в 250 тыс. систем. Однако он был безвреден, за исключением того, что каждый раз при совпадении времени и даты — например, 5:20 и 20 мая — на экране возникала цитата из The Simpsons.

Годом позже появился Love Bug, известный также как LoveLetter. За короткое время вирус облетел весь мир! Он был написан филиппинским студентом и приходил в электронном сообщении с темой "I Love You". Как только пользователь пытался открыть вложение, вирус через Microsoft Outlook пересылал себя по всем адресам в списке контактов. Затем скачивал троянскую программу для сбора интересующей филиппинца информации. LoveLetter атаковал около 55 миллионов ПК и заразил от 2,5 до 3 миллионов. Размер причинённого им ущерба оценивался в 10 миллиардов, но студент избежал наказания, поскольку Филиппины не имели в то время законодательной базы для борьбы с киберпреступниками [Борн Денис, http://www.wired.com].

Лавинообразное распространением вирусов стало большой проблемой для большинства компаний и государственных учреждений. В настоящее

время известно более миллиона компьютерных вирусов и каждый месяц появляется более 3000 новых разновидностей ["Энциклопедия Вирусов", http://www.viruslist.com/ru/viruses/encyclopedia.].

Компьютерный вирус — это специально написанная программа, которая может "приписывать" себя к другим программам, т.е. "заражать их", с целью выполнения различных нежелательных действий на компьютере, в вычислительной или информационной системе и в сети.

Когда такая программа начинает работу, то сначала, как правило, управление получает вирус. Вирус может действовать самостоятельно, выполняя определенные вредоносные действия (изменяет файлы или таблицу размещения файлов на диске, засоряет оперативную память, изменяет адресацию обращений к внешним устройствам, генерирует вредоносное приложение, крадет пароли и данные и т.д.), или "заражает" другие программы. Зараженные программы могут быть перенесены на другой компьютер с помощью дискет или локальной сети.

Формы организации вирусных атак весьма разнообразны, но в целом практически их можно "разбросать" по следующим категориям:

- удаленное проникновение в компьютер — программы, которые получают неавторизованный доступ к другому компьютеру через Internet (или локальную сеть);
- локальное проникновение в компьютер — программы, которые получают неавторизованный доступ к компьютеру, на котором они впоследствии работают;
- удаленное блокирование компьютера — программы, которые через Internet (или сеть) блокируют работу всего удаленного компьютера или отдельной программы на нем;
- локальное блокирование компьютера — программы, которые блокируют работу компьютера, на котором они работают;
- сетевые сканеры — программы, которые осуществляют сбор информации о сети, чтобы определить, какие из компьютеров и программ, работающих на них, потенциально уязвимы к атакам;
- сканеры уязвимых мест программ — программы, проверяют большие группы компьютеров в Интернет в поисках компьютеров, уязвимых к тому или иному конкретному виду атаки;
- "вскрыватели" паролей — программы, которые обнаруживают легко угадываемые пароли в зашифрованных файлах паролей;
- сетевые анализаторы (sniffers) — программы, которые слушают сетевой трафик; часто в них имеются возможности автоматического выделения имен пользователей, паролей и номеров кредитных карт из трафика;
- модификация передаваемых данных или подмена информации;

- подмена доверенного объекта распределённой вычислительной сети (работа от его имени) или ложный объект распределённой ВС (РВС).
- "социальная инженерия" — несанкционированный доступ к информации иначе, чем взлом программного обеспечения. Цель — ввести в заблуждение сотрудников (сетевых или системных администраторов, пользователей, менеджеров) для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы.

К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Сетевые черви

Основным признаком, по которому типы червей различаются между собой, является способ распространения червя — каким способом он передает свою копию на удаленные компьютеры. Другими признаками различия КЧ между собой являются способы запуска копии червя на заражаемом компьютере, методы внедрения в систему, а также полиморфизм, "стелс" и прочие характеристики, присущие и другим типам вредоносного программного обеспечения (вирусам и троянским программам).

Пример — E-mail-Worm — почтовые черви. К данной категории червей относятся те из них, которые для своего распространения используют электронную почту. При этом червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, URL на зараженный файл, расположенный на взломанном или хакерском веб-сайте). В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором — при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков — активизируется код червя.

Для отправки зараженных сообщений почтовые черви используют различные способы. Наиболее распространены:

- прямое подключение к SMTP-серверу, используя встроенную в код червя почтовую библиотеку;
- использование сервисов MS Outlook;
- использование функций Windows MAPI.

Различные методы используются почтовыми червями для поиска почтовых адресов, на которые будут рассылаться зараженные письма. Почтовые черви:

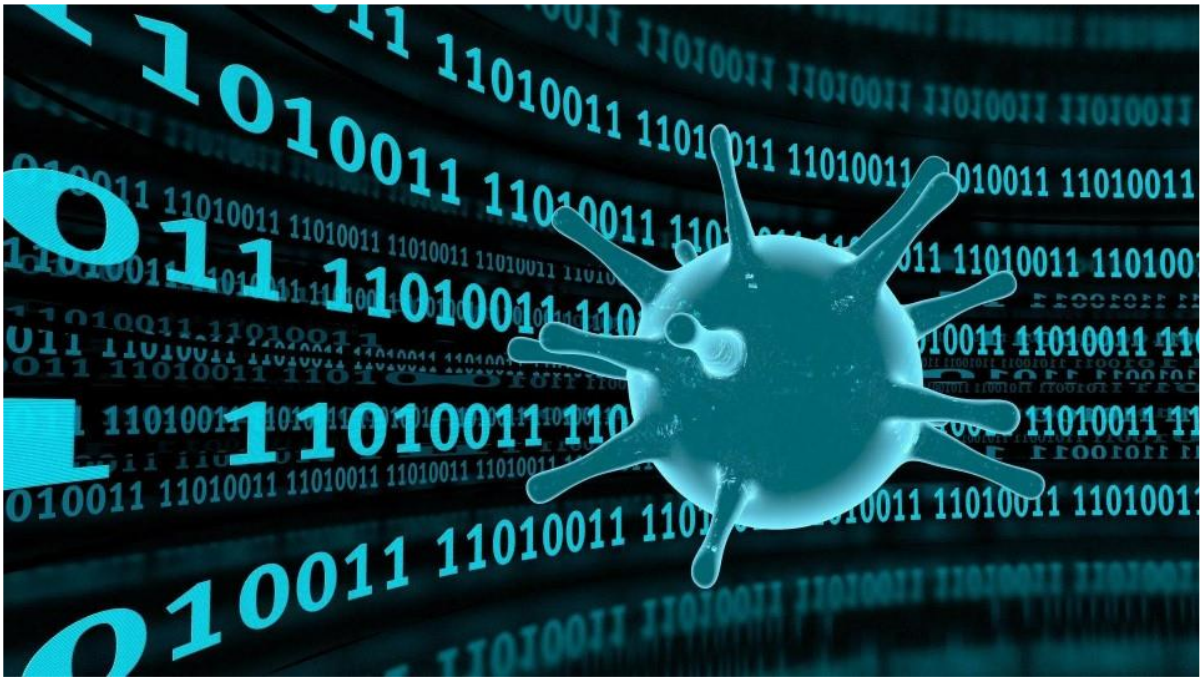
- рассылают себя по всем адресам, обнаруженным в адресной книге MS Outlook;
- считывает адреса из адресной базы WAB;

- сканируют "подходящие" файлы на диске и выделяет в них строки, являющиеся адресами электронной почты;
- отсылают себя по всем адресам, обнаруженным в письмах в почтовом ящике (при этом некоторые почтовые черви "отвечают" на обнаруженные в ящике письма).

Многие черви используют сразу несколько из перечисленных методов. Встречаются также и другие способы поиска адресов электронной почты. Другие виды червей: IM-Worm — черви, использующие Internet-пейджеры, IRC-Worm — черви в IRC-каналах, Net-Worm — прочие сетевые черви.

Классические компьютерные вирусы

Классические компьютерные вирусы



27.10.2023 32

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью: последующего запуска своего кода при каких-либо действиях пользователя или дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;

- вирус скопировал себя на съёмный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например бэкдор-процедуру или троянскую компоненту уничтожения информации на диске.

Многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макроязыки (макросы) для автоматизации выполнения повторяющихся действий. Эти макроязыки часто имеют сложную структуру и развитый набор команд. Макро-вирусы являются программами на макроязыках, встроенных в такие системы обработки данных. Для своего размножения вирусы этого класса используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Скрипт-вирусы

Следует отметить также скрипт-вирусы, являющиеся подгруппой файловых вирусов. Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы (командные и служебные файлы MS Windows или Linux), либо являются частями многокомпонентных вирусов. Также, данные вирусы могут заражать файлы других форматов (например, HTML), если в них возможно выполнение скриптов.

Троянские программы

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и её передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях. Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

Троянские программы многообразны и различаются между собой по тем действиям, которые они производят на зараженном компьютере:

- Backdoor — троянские утилиты удаленного администрирования.
- Trojan-PSW — воровство паролей.
- Trojan-AOL — семейство троянских программ, "ворующих" коды доступа к сети AOL (America Online). Выделены в особую группу по причине своей многочисленности.
- Trojan-Clicker — Internet-кликеры. Семейство троянских программ, основная функция которых — организация несанкционированных

обращений к Internet-ресурсам (обычно к Web-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных файлов, в которых указаны "стандартные" адреса Internet-ресурсов (например, файл hosts в MS Windows).

- Trojan-Downloader — доставка прочих вредоносных программ.
- Trojan-Dropper — инсталляторы прочих вредоносных программ. Троянские программы этого класса написаны в целях скрытной инсталляции других программ и практически всегда используются для "подсовывания" на компьютер-жертву вирусов или других троянских программ.
- Trojan-Proxy — троянские прокси-сервера. Семейство троянских программ, скрытно осуществляющих анонимный доступ к различным интернет-ресурсам. Обычно используются для рассылки спама.
- Trojan-Spy — шпионские программы. Данные троянцы осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в какой-либо файл на диске и периодически отправляются злоумышленнику. Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.
- Trojan — прочие троянские программы. В данной категории также присутствуют "многоцелевые" троянские программы, например, те из них, которые одновременно шпионят за пользователем и предоставляют proxy-сервис удаленному злоумышленнику.
- Trojan ArcBomb — "бомбы" в архивах. Представляют собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные — зависание или существенное замедление работы компьютера или заполнение диска большим количеством "пустых" данных. Особенно опасны "архивные бомбы" для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации — "архивная бомба" может просто остановить работу сервера.
- Trojan-Notifier — оповещение об успешной атаке. Троянцы данного типа предназначены для сообщения своему "хозяину" о зараженном компьютере. При этом на адрес "хозяина" отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т. п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к веб-странице "хозяина", ICQ-сообщением. Данные троянские программы используются в многокомпонентных троянских наборах для извещения своего "хозяина" об успешной инсталляции троянских компонент в атакуемую систему.

Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- "злые шутки", затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб конкретному или некоторым удалённым компьютерам.

К прочим вредоносным относятся разнообразные программы, которые не представляют угрозы непосредственно компьютеру, на котором исполняются, а разработаны для создания других вирусов или троянских программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т. п.

К таким программам можно отнести известные:

- DoS, DdoS — сетевые атаки;
- Exploit, HackTool — взломщики удаленных компьютеров. Хакерские утилиты данного класса предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа "backdoor") или для внедрения во взломанную систему других вредоносных программ.
- Flooder — "замусоривание" сети. Данные хакерские утилиты используются для "забивания мусором" (бесполезными сообщениями) каналов интернета — IRC-каналов, компьютерных пейджинговых сетей, электронной почты и т. д.
- Constructor — конструкторы вирусов и троянских программ. Конструкторы вирусов и троянских программ — это утилиты, предназначенные для изготовления новых компьютерных вирусов и "троянцев". Известны конструкторы вирусов для DOS, Windows и макро-вирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы.
- Nuker — фатальные сетевые атаки. Утилиты, отправляющие специально оформленные запросы на атакуемые компьютеры в сети, в результате чего атакуемая система прекращает работу. Используют уязвимости в программном обеспечении и операционных системах, в результате чего сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении.
- Bad-Joke, Hoax — злые шутки, введение пользователя в заблуждение. К ним относятся программы, которые не причиняют

компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К "злым шуткам" относятся, например, программы, которые "пугают" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т. д. — в зависимости от чувства юмора автора такой программы.

- FileCryptor, PolyCryptor — скрытие от антивирусных программ. Хакерские утилиты, использующиеся для шифрования других вредоносных программ с целью скрытия их содержимого от антивирусной проверки.
- PolyEngine — полиморфные генераторы. Полиморфные генераторы не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.
- VirTool — утилиты, предназначенные для облегчения написания компьютерных вирусов и для их изучения в хакерских целях.

От чего надо защищаться в первую очередь?

Во-первых, это вирусы (Virus, Worm) и всевозможные виды практически бесполезной информации (обычно рекламы), принудительно рассылаемой абонентам электронной почты (Spam). По различным данным в 2013 году вирусным атакам было подвержено от 80 до 85 процентов компаний во всем мире. И эта цифра продолжает расти.

Далее следует назвать вредоносные программы типа "троянский конь" (Trojan Horse), которые могут быть незаметно для владельца установлены на его компьютер и также незаметно функционировать на нем. Простые варианты "троянского коня" выполняют какую-либо одну функцию — например, кражу паролей, но есть и более "продвинутые" экземпляры, которые реализуют широкий спектр функций для удаленного управления компьютером, включая просмотр содержимого каталогов, перехват всех вводимых с клавиатуры команд, кражу или искажение данных и информации, изменение файлов и содержания полей баз данных.

Другим распространенным типом атак являются действия, направленные на выведение из строя того или иного узла сети. Эти атаки получили название "отказ в обслуживании" (Denial of Service — DoS), и на сегодняшний день известно более сотни различных вариантов этих действий. Выше отмечалось, что выведение из строя узла сети на несколько часов может привести к очень серьезным последствиям. Например, выведение из строя сервера платежной системы банка приведет к невозможности осуществления платежей и, как следствие, к большим прямым и косвенным финансовым и рейтинговым потерям.

Атаки и угрозы такого типа являются наиболее частыми, однако существуют и другие угрозы, которые могут привести к серьезным последствиям. Например, система обнаружения атак RealSecure обнаруживает более 1000 различных событий, влияющих на безопасность и относящихся к внешним атакам. Американская организация US-CERT (http://www.vnunet.com/vnunet/news/2143314/security-industry-gathers), занимающаяся проблемами в области компьютерной безопасности, предложила использовать стандартные названия для интернет-червей и других вредоносных программ. Члены US-CERT назвали свою программу "Общая классификация вредоносных программ" (CME). Цель программы — не вводить пользователей в заблуждение, используя разные названия для одних и тех же вирусов. Например, червь W32.Zotob.E по классификации Symantec в классификации McAfee называется W32/IRCbot.worm!MS05-039, а Trend Micro называет эту программу WORM_RBOT.CBQ.

Сейчас многие вирусы получают свои названия на основании описания или информации, включенной в код программы их создателями. В новой системе вирусы будут использовать номера CME. Первый вирус получит название CME-1.

Подобная система классификации уже существует для описания уязвимостей в программном обеспечении. Общий идентификатор уязвимостей включает себя порядковый номер и год, в котором уязвимость была выявлена. В идентификатор вирусов не включат дату, потому что пользователи часто неправильно воспринимают эту информацию. Они считают, что уязвимость с ранней датой менее опасна, чем уязвимость, выявленная позже.

Инициаторы предложения о CME допускают использование и старых вирусных имен, но надеются, что их система улучшит обмен информацией между антивирусными разработчиками и антивирусным сообществом в целом. Проект уже поддержали Computer Associates, McAfee, Microsoft, Symantec и F-Secure.

Как надо защищаться?

Общие методики защиты от вирусов в обязательном порядке являются обязательной составной частью политики информационной безопасности предприятия. В соответствующих разделах политики следует обязательно прописывать принципы антивирусной защиты, применяемые стандарты и нормативные документы, определяющие порядок действий пользователя при работе в локальной и внешних сетях, его полномочия, применяемые антивирусные средства. Наборы обязательных правил могут быть достаточно разнообразны, однако можно сформулировать в общем виде следующие правила для пользователей:

- проверять на вирусы все диски CD-RW, ZIP-диски, побывавшие на другом компьютере, все приобретенные не в фирменных магазинах CD и флешки;

- использовать антивирусные программы известных проверенных фирм, регулярно (в идеале — ежедневно) обновлять их базы;
- не выгружать резидентную часть (монитор) антивирусной программы из оперативной памяти компьютера;
- использовать только программы и данные, полученные из надежных источников — чаще всего вирусами бывают заражены пиратские копии программ;
- никогда не открывать файлы, прикрепленные к электронным письмам, пришедшим от неизвестных отправителей, и не заходить на сайты, рекламируемые через спам-рассылки (по данным Лаборатории Касперского, в настоящее время около 90% вирусов распространяются именно таким образом).

Аналогично можно сформулировать несколько общих требований к хорошей антивирусной программе. Такая программа должна:

- обеспечивать эффективную защиту в режиме реального времени — резидентная часть (монитор) программы должна постоянно находиться в оперативной памяти компьютера и производить проверку всех файловых операций (при создании, редактировании, копировании файлов, запуске их на исполнение), сообщений электронной почты, данных и программ, получаемых из Internet;
- позволять проверять все содержимое локальных дисков "по требованию", запуская проверку вручную или автоматически по расписанию или привключении компьютера;
- защищать компьютер даже от неизвестных вирусов — программа должна включать в себя технологии поиска неизвестных вирусов, основанные на принципах эвристического анализа;
- уметь проверять и лечить архивированные файлы;
- давать возможность регулярно (желательно ежедневно) обновлять антивирусные базы (через Internet, с дискет или CD).

Антивирусное программное обеспечение активно разрабатывается во многих странах. Так например, ученые из Национальной лаборатории Sandia (Sandia Corporation) в Ливерморе, Калифорния, запустили более миллиона ядер (kernel) операционной системы Linux в виртуальной среде.

Эксперимент должен помочь в исследовании поведения ботнетов — сетей из миллионов зараженных вредоносным программным обеспечением компьютеров, используемых для разнообразных атак, например, спам-рассылок или DDoS-атак (Distributed Denial of Service). Один из участников проекта Рон Минник (Ron Minnich) объясняет, что реальные сети трудно поддаются анализу из-за географического распределения входящих в них узлов по всему миру. Однако, используя технологию виртуальных машин на суперкомпьютерном кластере Thunderbird, команде ученых удалось запустить виртуальную систему, сравнимую по масштабам с современными ботнетами.

Минник с коллегами рассчитывают, что этот исследовательский проект поможет не только понять принципы работы вредоносных сетей, составленных из множества ПК, но попытаться разработать методики их обезвреживания.

В настоящее время в России используются главным образом два проверенных качественных антивирусных пакета: Dr.WEB и "Антивирус Касперского". Каждая из этих продуктов имеет свою линейку, ориентированную на разные сферы применения — для использования на локальных компьютерах, для малого и среднего бизнеса, для крупных корпоративных клиентов, для защиты локальных сетей, для почтовых, файловых серверов, серверов приложений. Оба продукта, безусловно, отвечают всем вышеперечисленным требованиям. Материалы по этим пакетам можно найти на сайтах указанных компаний.

Современные средства биометрической идентификации

В настоящее время наряду с указанными выше средствами защиты информации в системах и сетях шире применяются биометрические системы безопасности. По данным аналитической компании Frost&Sullivan, общий объем продаж биометрического оборудования в Америке в 2000 году не превысил 86,8 млн. долларов, вырос в 2001 году до 160,3 млн. долларов и превысил в 2012 году 9 миллиардов долларов. В настоящее время рынок таких устройств перевалил за десятки миллиардов долларов в год.

Биометрические технологии идентификации имеют ряд преимуществ перед традиционными средствами. Под биометрией понимают методы автоматической идентификации человека и подтверждения личности, основанные на физиологических или поведенческих характеристиках (рис. 6.20).

Наиболее часто применяются три основных биометрических метода — это распознавание человека по отпечаткам пальцев, по радужной оболочке глаза и по изображению лица. По информации консалтинговой компании International Biometric Group из Нью-Йорка, наиболее распространенной технологией стало сканирование отпечатков пальцев.

Отмечается, что из 127 млн. долларов, вырученных от продажи биометрических устройств, 44% приходится на дактилоскопические сканеры. Системы распознавания черт лица занимают второе место по уровню спроса, который составляет 14%, далее следуют устройства распознавания по форме ладони (13%), по голосу (10%) и радужной оболочке глаза (8%). Устройства верификации подписи в этом списке составляют 2%.

Система биометрических параметров для идентификации личности

Рис. 6.20. Система биометрических параметров для идентификации личности

Преимущества биометрических систем безопасности очевидны. Уникальные человеческие качества хороши тем, что их трудно подделать, трудно оставить фальшивый отпечаток пальца при помощи своего собственного или сделать радужную оболочку своего глаза похожей на чью-то другую.

В отличие от бумажных идентификаторов (паспорт, водительское удостоверение или иное удостоверение личности), от пароля или персонального идентификационного номера (ПИН), биометрические характеристики невозможно забыть или потерять. Кроме того, в силу своей уникальности они используются для предотвращения воровства или мошенничества.

Методы распознавания по изображению лица могут работать с двухмерным или с трехмерным изображением (так называемые 2D- и 3D-фото). Стоит отметить, что идентификация человека по чертам лица — одно из самых динамично развивающихся направлений в биометрической индустрии. Привлекательность данного метода основана на том, что он наиболее близок к тому, как люди обычно идентифицируют друг друга. Распространение мультимедийных технологий, благодаря которому все чаще можно встретить видеокамеры, установленные на городских улицах и площадях, на вокзалах, в аэропортах и других местах скопления людей, определило развитие этого направления.

Распознавание лица предусматривает выполнение любой из следующих функций: аутентификация (установление подлинности "один в один") или идентификация (поиск соответствия "один из многих"). Система автоматически оценивает качество изображения для опознания лица и, если необходимо, способна его улучшить. Она также создает изображение лица из сегментов данных, генерирует цифровой код или внутренний шаблон, уникальный для каждого индивидуума (рис. 6.21).

Рис. 6.21. Трёхмерное изображение лица в системе идентификации человека

Трехмерная фотография — новейшая биометрическая технология, созданная отечественными разработчиками около пяти лет назад. Трехмерное фото, занимая всего 5 Кбайт, может быть записано в биометрический паспорт; оно увеличивает точность идентификации личности и повышает надежность автоматической сверки документов. Эксперты отмечают, что уровень распознавания трехмерной фотографии составляет более 90%, тогда как у двухмерного изображения этот показатель редко превышает 50%.

Биометрические технологии призваны обеспечить повышение надежности и эффективности сверки документов, предназначены для электронного документирования (логирования) всех сверок, а также для эффективной и надежной идентификации личности человека в широком спектре ситуаций (рис. 6.22).

Рис. 6.22. биометрический контроль

При решении этой задачи возможны два сценария: двойная или тройная верификация. Двойная верификация подразумевает сверку биометрического шаблона, записанного в электронном паспорте или визе, с биометрическими характеристиками проверяемого субъекта.

Тройная верификация, в свою очередь, предполагает дополнительную сверку двух указанных характеристик с шаблоном, хранящимся в общегосударственном регистре биометрических данных. При этом сценарии любая попытка подделки документа становится бессмысленной, поскольку тройная верификация выявит несоответствие с шаблоном, записанным в государственный регистр при выдаче документа.

Еще одна задача, связанная в основном с выдачей паспорта или визы, заключается в проверке того факта, что аналогичный документ не выдавался ранее гражданину с теми же биометрическими данными, но проходившему под другим именем, а также в сверке биометрических данных гражданина с базами данных оперативных и специальных служб. И в том и в другом случае решение задачи предполагает использование биометрических методов в режиме идентификации, при этом размер баз данных может быть очень большим.

Для решения первой задачи (двойной и тройной верификации) допускается использовать любой из трех методов (по фотографии лица, по отпечаткам пальцев или радужной оболочке), которые дают приемлемую

точность. Для решения второй задачи (идентификации гражданина по большой базе данных) необходимы комбинированные методы.

По мнению экспертов, наиболее обоснованное решение при внедрении биометрических методов — это первичный сбор и занесение в единый государственный регистр, а также в электронные идентификационные документы как дактилоскопической информации (с двух пальцев), так и двух изображений лица (двухмерного и трехмерного). При этом для решения задачи верификации, подразумевающей сверку документов при пересечении гражданами границ, достаточно комбинированного (2D + 3D) метода распознавания лица. Этот бесконтактный метод обеспечивает максимальную измеряемость биометрической характеристики (иными словами, максимальную скорость верификации и прохода), следовательно, он не замедлит, а ускорит прохождение пассажиропотока через точки контроля.

Точность 3D- и тем более комбинированного метода высока и отвечает всем требованиям в режиме верификации, а также в режиме идентификации с не очень большими (до 10 тыс. человек) оперативными базами данных (пример - список лиц, объявленных в розыск). Кроме того, использование обычной двухмерной фотографии — во-первых, общепринятая практика, во-вторых, позволяет оператору принять окончательное решение или провести визуальное сравнение с несколькими наиболее похожими индивидуумами из базы данных. Благодаря этому можно увеличить размер базы данных для оперативной идентификации до нескольких сотен тысяч человек.

Использование дактилоскопической информации предполагается только в момент проверки личности, до выдачи документа, а также при необходимости задержания гражданина и предъявлении обвинений. Это позволяет повысить уровень защиты данных, ограничив круг лиц, имеющих право доступа к записанной в паспорте дактилоскопической информации, только сотрудниками соответствующих правоохранительных служб.

В июле 2005 году Федеральное агентство по техническому регулированию и метрологии РФ направило в Международный подкомитет по стандартизации в области биометрии при ISO официальное предложение, касающееся изменения международного стандарта в области биометрии. Суть предлагаемой поправки заключается во включении трехмерного цифрового изображения лица, наряду с обычной двухмерной фотографией, в формат данных, предназначаемый для хранения, обмена и использования при автоматическом распознавании личности. После утверждения проекта, под цифровым изображением лица будут понимать формат данных, включающий как обычную двухмерную, так и трехмерную фотографию. Немного ранее, в феврале 2005 года, по инициативе компании A4Vision, поддержанной, в частности, Oracle, Motorola, Unisys, Logitech, аналогичная поправка к национальному стандарту была одобрена в США. Заметим, что компания A4Vision (http://www.a4vision.com), основанная нашими соотечественниками,

первой разработала технологию трехмерного распознавания лиц и, выйдя на рынок США, инициировала процедуру изменения американского стандарта.