**Лекция 6:**

**Обеспечение безопасности**

**Аннотация:**В лекции рассказывается о методологических аспектах защиты информационных систем.

**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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=1#image.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**

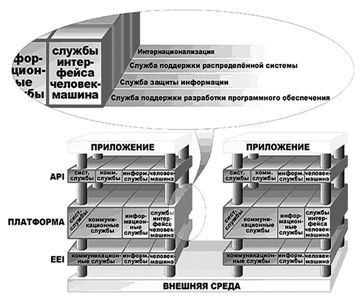
Специалистам в области ИБ сегодня практически невозможно обойтись без знаний соответствующих профилей защиты, стандартов и спецификаций. Формальная причина состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и "Руководящим документам" Гостехкомиссии РФ) закреплена 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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=1#image.6.2), [рис. 6.3](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=1#image.6.3)).



**Рис. 6.2.**Объекты стандартизации в открытой информационной системе



**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 [В. Липаев., <http://www.pcweek.ru/themes/detail.php?ID=55087>].

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 исполненияугроз, 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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=1#image.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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=1#image.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.



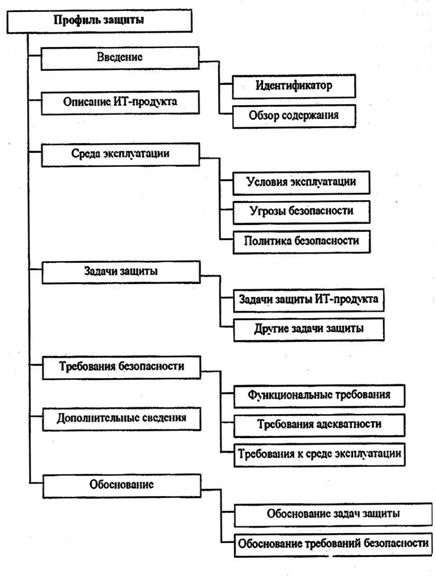
**Рис. 6.5.**Критерии адекватности средств защиты

*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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=1#image.6.6)).Ключевые средства контроля (*механизмы* управления ИБ), предлагаемые в *ISO 17799*, считаются особенно важными.



**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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=1#image.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**

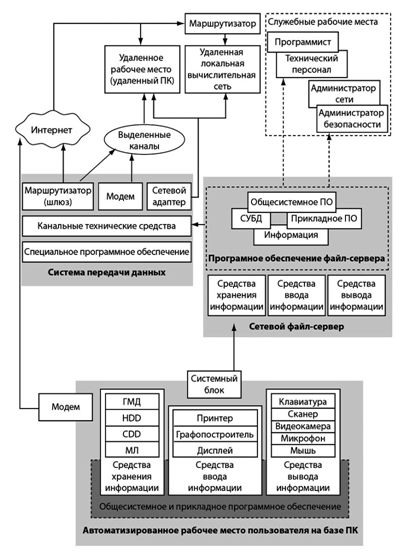
Современные распределенные корпорации, имеющие подразделения на разных континентах, имеют сложную техническую, инженерную и информационную инфраструктуру. Создание информационной сети такой корпорации и её эффективная защита является чрезвычайно сложной концептуальной и технологической задачей.

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.

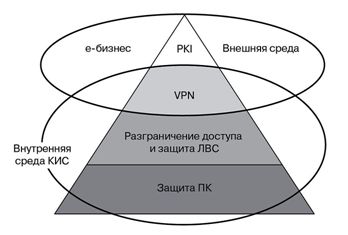
Целевое назначение любой корпоративной информационной системы состоит в обеспечении пользователей необходимой информацией в режиме "On Line" и адекватном информационном сопровождении деятельности предприятия.

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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=2#image.6.8)).



**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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=2#image.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.

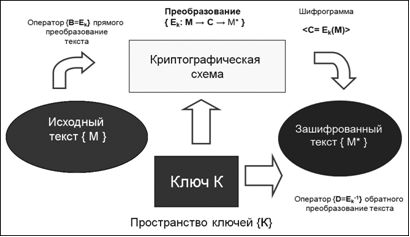
В соответствии с политиками безопасности используемые в компании технологии криптографии и специализированное программно-аппаратное обеспечение для защиты данных и документов, шифрования файлов и дисков реализуют следующие аспекты информационной защиты:

* 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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=2#image.6.10), а на [рис. 6.11](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=2#image.6.11) приведена схема симметричной криптосистемы с закрытым ключом [Соколов А. В., Шаньгин В. Ф., 2002].

Отправитель сообщения генерирует открытый текст сообщения <М> для передачи по незащищенному каналу связи. Для того чтобы передаваемый текст невозможно было прочитать, отправитель преобразует (шифрует) его с помощью алгоритма обратимого преобразования <Е_k>, формируя зашифрованный текст (криптограмму) <С= Е_k(М)>.

Адресат, получив криптограмму, применяет известное ему обратное преобразование <D=Е_k^{-1}> и получает исходный открытый текст М: <D_k(C) = Е_k^{-1}(Е_k(М)) = M>. Множество преобразований {Е_к}_i образуют семейства криптоалгоритмов {Е_к}^N. Параметр К, с помощью которого производится преобразование текста сообщения, называется ключом.

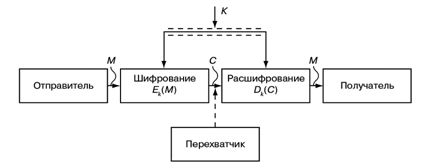


**Рис. 6.10.**Общая схема криптосистемы

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 {М} сообщений открытого текста в пространство {С} зашифрованных текстов. Параметр шифрования К (ключ) выбирается из конечного множества {К}, называемого пространством ключей.

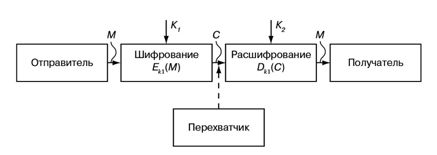
Существует два класса криптосистем — симметричные (с одним ключом) и асимметричные (с двумя ключами). Симметричные криптосистемы ([рис. 6.11](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=2#image.6.11)) используют один и тот же ключ в процедурах шифрования 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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=2#image.6.11), пунктирная линия), что является существенным недостатком симметричной системы шифрования.



**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.



**Рис. 6.12.**Схема асимметричной криптосистемы с открытым ключом

Асимметричные криптосистемы используют различные ключи ([рис. 6.12](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=2#image.6.12)):

* открытый ключ К_1 используется для шифрования данных и вычисляется по параметрам секретного ключа К_2;
* секретный ключ К_2 используется для расшифровки информации, зашифрованной с помощью парного ему открытого ключа К_1.

Открытый и секретный ключи и К_2 генерируются попарно, при этом ключ К_2 остается у его владельца и должен быть надежно защищен от НСД. Копии ключа К_1 распространяются среди пользователей сети, с которыми обменивается информацией обладатель секретного ключа К_2. Таким образом, в асимметричной криптосистеме ключ К1 свободно передается по открытым каналам связи, а секретный ключ К_2 хранится на месте его генерации.

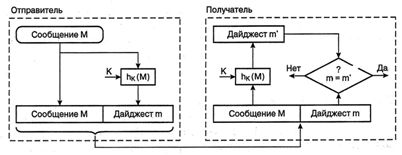
Система защиты информации называется криптостойкой, если в результате предпринятой злоумышленником атаки на зашифрованное послание невозможно расшифровать перехваченный зашифрованный текст С для получения открытого текста М или зашифровать текст злоумышленника М ' для передачи правдоподобного зашифрованного текста С ' 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 К_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 М, а выходом является строка фиксированной длины h(M) — дайджест сообщения ([рис. 6.13](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=2#image.6.13)).



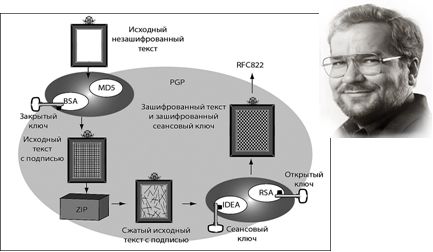
**Рис. 6.13.**Однонаправленной хэш-функции с параметром-ключом

Криптостойкость такого метода шифрования состоит в невозможности подобрать документ М  ', который обладал бы требуемым значением хэш-функции. Параметры вычисления хэш-функции h являются семейством ключей {К}^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 ЕСС 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].

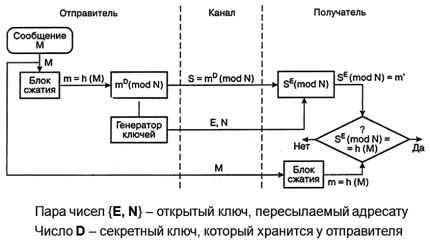
Наиболее известным программным продуктом, распространяемым свободно, является пакет PGP (Pretty Good Privacy). Пакет разработан Филом Циммерманом (Phil Zimmerman) в 1995 году, который использовал упомянутые алгоритмы RSA, IDEA, и MD5. PGP состоит из трёх частей — алгоритма IDEA, сигнатуры и цифровой 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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=2#image.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).



**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 34.11-94 — 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](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=2#image.6.15)).