*Лекция 13-15 (Продолжение)*

*Защита информации* на файловом уровне. Эти технологии позволяют скрыть конфиденциальную информацию пользователя на жестком диске компьютера или на сетевых дисках путем кодирования содержимого файлов, каталогов и дисков. *Доступ* к данной информации осуществляется по предъявлению ключа, который может вводиться с клавиатуры, храниться и предоставляться со смарт-карты, HASP-ключей или USB-ключей и прочих токенов.

Помимо вышеперечисленных функций указанные средства позволяют мгновенно "уничтожить" информацию при подаче сигнала "тревога" и при "входе под принуждением", а также блокировать *компьютер* в перерывах между сеансами работы.

Технологии токенов (смарт-карты, touch-memory, ключи для USB-портов, скрытые цифровые маркеры). Электронные ключи-жетоны (*Token*) являются средством повышения надежности защиты данных на основе гарантированной идентификации пользователя. Токены являются "контейнерами" для хранения персональных данных пользователя системы и некоторых его паролей.

Основным элементом токена является *микроконтроллер*, позволяющий создавать ключи с уникальным набором свойств. Благодаря микроконтроллеру усложняется логика работы ключа, которая делает ее более интеллектуальной ([рис. 7.6](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27507?page=2#image.7.6)).

Базовые возможности современных токенов:

* хранение паролей для доступа к системам, сетям и т.п.;
* хранение ключей шифрования для обеспечения секретности";
* хранение ключей для целей аутентификации;
* выполнение алгоритмов шифрования для аутентификации и обеспечения секретности информации;
* безопасное хранение информации.

Основное преимущество токена заключается в том, что персональная *информация* всегда находится на носителе (смарт-карте, ключе и т. д.) и предъявляется только во *время доступа* к системе или компьютеру.



**Рис. 7.6.**Архитектура смарт-карты

Технология интеллектуальных карт позволяет унифицировать правила доступа и поместить на одном персональном электронном носителе систему паролей для доступа на различные устройства и системы кодирования и декодирования информации.

В настоящее время получают распространение различного вида интеллектуальные карты с системой персональной аутентификации на базе биометрической информации, которая считывается с руки пользователя. Таким "ключом" может воспользоваться только тот *пользователь*, на которого настроен этот *ключ* ([рис. 7.7](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27507?page=2#image.7.7)).



**Рис. 7.7.**Классификация интеллектуальных карт

Скрытые цифровые маркеры (СЦМ) представляют собой специальный программы, которые встраиваются в защищаемый *объект*. Такие маркеры "индивидуализируют" *объект*, защищая тем самым от подмены или исправления, или выполняют общие защитные функции от несанкционированного чтения или копирования ([рис. 7.8](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27507?page=2#image.7.8)).



**Рис. 7.8.**Общие функции защиты на базе технологии скрытых цифровых маркеров

Межсетевые экраны. Использование технологии межсетевых экранов предлагается для решения таких задач как:

* безопасное взаимодействие пользователей и информационных ресурсов, расположенных в Extranet- и Intranet-сетях, с внешними сетями;
* создание технологически единого комплекса мер защиты для распределенных и сегментированных локальных сетей подразделений предприятия;
* построение иерархической системы защиты, предоставляющей адекватные средства обеспечения безопасности для различных по степени закрытости сегментов корпоративной сети.

В зависимости от масштабов организации и установленной политики безопасности рекомендуются межсетевые экраны (*Firewall*), отличающиеся по степени функциональности и по стоимости (межсетевые экраны CheckPoint *Firewall*-1, *Private* *Internet* *Exchange* (PIX) компании Cisco и другие). Устройства содержательной фильтрации (*Content* *Inspection*) устанавливаются, как правило, на входы почтовых серверов для отсечения большого объёма неопасной, но практически бесполезной информации, обычно рекламного характера (*Spam*), принудительно рассылаемой большому числу абонентов электронной почты.

Антивирусные средства. Лавинообразное распространением вирусов ("червей", "троянских коней"), как отмечалось выше, действительно стало большой проблемой для большинства компаний и государственных учреждений. Сложилось мнение, что основной *путь* "заражения" компьютеров происходит через *Internet*, поэтому наилучшее решение, по мнению многих руководителей — отключить корпоративную *сеть* от "Всемирной паутины" или запретить большинству сотрудников пользоваться ею. При этом не учитывается, что существует множество других путей проникновения вирусов на конкретный *компьютер*, например, использовании чужих флешек и дисков, пиратское *программное обеспечение* или персональные компьютеры "общего пользования" (например, опасность представляют домашние или студенческие компьютеры, если на них работает более одного человека). Системное применение соответствующих политик ИБ и лицензионных антивирусных средств (например, Лаборатории Касперского или Dr.*Web*) существенно уменьшает опасность "вирусного" заражения.

Защищенные *виртуальные частные сети*. Для защиты информации, передаваемой по открытым каналам связи, поддерживающим протоколы *TCP/IP*, существует ряд программных продуктов, предназначенных для построения защищенных виртуальных частных сетей (*VPN*) на основе международных стандартов *Internet* *Security Protocol*, ([рис. 7.9](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27507?page=2#image.7.9)).



**Рис. 7.9.**Компоновка VPN на основе международных стандартов и протоколов

Виртуальные сети создаются чаще всего на базе арендуемых и коммутируемых каналов связи в сетях общего пользования (*Internet*). Для небольших и средних компаний они являются хорошей альтернативой изолированным корпоративным сетям, так как обладают очевидными преимуществами: высокая гарантированная надёжность, изменяемая *топология*, простота конфигурирования, лёгкость масштабирования, *контроль* всех событий и действий в сети, относительно невысокая *стоимость* аренды каналов и коммуникационного оборудования.

Продукты работают в операционных системах *Windows* и Solaris и обеспечивают:

* защиту (конфиденциальность, подлинность и целостность) передаваемой по сетям информации;
* контроль доступа в защищаемый периметр сети;
* идентификацию и аутентификацию пользователей сетевых объектов;
* централизованное управление политикой корпоративной сетевой безопасности.

Системы шифрования с открытым криптографическим интерфейсом позволяют использовать различные реализации криптоалгоритмов. Это даёт возможность использования продуктов в любой стране мира в соответствии с принятыми национальными стандартами. Наличие разнообразных модификаций (линейка продуктов включает до десятка наименований для клиентских, серверных платформ, для сети масштаба офиса, для генерации ключевой информации) позволяет подбирать оптимальное по стоимости и надежности решение с возможностью постепенного наращивания мощности системы защиты.

Технологии обнаружения атак (*Intrusion* *Detection*). Постоянное изменение сети (появление новых рабочих станций, *реконфигурация* программных средств, и т.п.) может привести к появлению новых уязвимых мест, угроз и возможностей атак и информационные ресурсы, и на саму систему защиты. В связи с этим особенно важно своевременное их выявление и внесение изменений в соответствующие настройки информационного комплекса и его подсистем, и в том числе, в подсистему защиты. Это означает, что рабочее *место* администратора системы должно быть укомплектовано специализированными программными средствами обследования сетей и выявления уязвимых мест (наличия "дыр") для проведения атак "извне" и "снаружи", а также комплексной оценки степени защищенности от атак нарушителей. Например, в состав продуктов ЭЛВИС+, *Net* Pro *VPN* входят наиболее мощные среди обширного семейства коммерческих пакетов продукты компании *Internet* *Security* Systems (*Internet* *Scanner* и *System* *Security* *Scanner*), а также продукты компании Cisco: система обнаружения несанкционированного доступа NetRanger и *сканер* уязвимости системы безопасности NetSonar (<http://www.extrim.ru/instruments_vpn.asp>).

*Инфраструктура* открытых ключей (*PKI* — *Public* Key Infrastruture). Основными функциями *PKI* являются: *поддержка* жизненного *цикла* цифровых ключей и сертификатов (т.е. их генерация, распределение, отзыв и пр.), *поддержка* процесса идентификации и аутентификации пользователей, и реализация механизма интеграции существующих приложений и всех *компонент* подсистемы безопасности. Несмотря на существующие международные стандарты, определяющие функционирование системы *PKI* и способствующие ее взаимодействию с различными средствами защиты информации, к сожалению, не каждое средство информационной защиты, даже если его производитель декларирует соответствие стандартам, может работать с любой системой *PKI*. В настоящее время всё часще используются комплексные решения на базе IPSec и *PKI* ([рис. 7.9](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27507?page=2#image.7.9)).

В нашей стране только начинают появляться компании, предоставляющие услуги по анализу, проектированию и разработке *инфраструктуры открытых ключей*. Поскольку при возрастающих масштабах ведомственных и корпоративных сетей *VPN*-продукты не смогут работать без *PKI*, только у разработчиков и поставщиков *VPN* есть *опыт* работы в этой области.

В зависимости от масштаба деятельности компании методы и средства обеспечения ИБ могут различаться, но любой квалифицированный *CIO* или специалист IT-службы скажет, что любая проблема в области ИБ не решается односторонне — всегда требуется комплексный, интегральный подход.

Приходится с сожалением констатировать, что в российском бизнесе высшие менеджеры компаний и руководители крупных государственных организаций часто считают, что все проблемы в сфере ИБ можно решить, не прилагая особых организационных, технических и финансовых усилий. Во многих организацияхи руководители и даже специалисты пренебрегают международными стандартами и методами комплексного проектирования равнопрочных систем защиты, концентрируя свои усилия на применении отдельных, не связанных между собой технических средств, чему способствует отсутствие соответствующих отечественных стандартов и руководящих документов.

Нередко со стороны людей, позиционирующих себя в качестве IT-специалистов в российских компаниях, приходится слышать высказывания: "Проблемы информационной безопасности в нашей компании мы уже решили — установили *межсетевой экран* и купили лицензию на средства антивирусной защиты. Мы считаем, что этого достаточно".

Такой подход свидетельствует, что существование проблемы уже признается, но сильно недооценивается масштаб и сложность необходимых срочных мероприятий по ее решению. В тех компаниях, где руководство и специалисты всерьез задумались над тем, как обезопасить свой бизнес и избежать финансовых потерь, признано, что одними локальными мерами или радикальными "подручными" средствами уже не обойтись, а нужно применять именно системный *комплексный подход*.

Таким образом, защита должна быть ориентирована на комплексное обеспечение эффективного решения основных, функциональных задач всей информационной системы. Методологически решение этих задач следует осуществлять как проектирование сложной, достаточно автономной программно-аппаратной системы во и взаимодействии с окружающими ее функциональными задачами ИС. При этом следует определять и ранжировать функциональные компоненты ИС по степени необходимой защиты, оценивать серьезность различных внешних и внутренних угроз безопасности, выделять методы, средства и нормативные документы, адекватные видам угроз и требуемой защите, оценивать нужные для этого ресурсы различных видов. Планирование и комплексная разработка проекта системы программной защиты должны обеспечивать высокое качество последующего жизненного *цикла* всей ИС.

В заключение ещё раз отметим, что в условиях динамичного развития рынка и усложнения его инфраструктуры *информация* становится таким же стратегическим ресурсом, как и традиционные материальные и энергетические. Современные технологии, позволяющие находить, создавать, хранить, перерабатывать данные и обеспечивать эффективные способы представления информации, стали важным фактором конкурентоспособности и средством повышения эффективности управления всеми сферами общественной жизнедеятельности. Уровень информатизации является сегодня одним из главных факторов успешного развития всякого предприятия. В связи с этим в последнем десятилетии ХХ века и в начале века XXI чрезвычайную актуальность приобрели вопросы защиты конфиденциальной и служебной государственной и корпоративной информации, безопасности информационных систем и сетей.