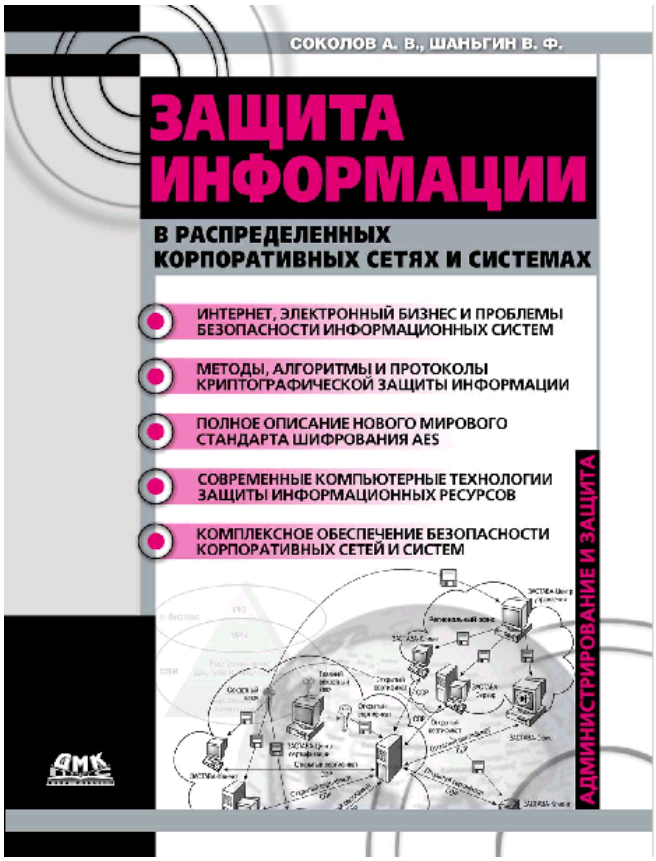
ОБЗОР СОДЕРЖАНИЯ МОНОГРАФИИ СОКОЛОВА А.В. И ШАНЬГИНА В.Ф.
"ЗАЩИТА ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ КОРПОРАТИВНЫХ СЕТЯХ И СИСТЕМАХ"

- М.: ДМК Пресс, 2002. - 656 с.: ил.



Стремительное развитие информационных технологий привело к созданию и быстрому росту глобальной сети Internet, формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. К числу наиболее перспективных направлений применения современных информационных технологий относится бизнес. Новые технологические возможности облегчают распространение информации, повышают эффективность производственных процессов, способствуют расширению деловых операций в процессе бизнеса.
Эффективность бизнеса компании напрямую зависит от качества и оперативности управления бизнес-процессами. Одним из главных инструментов управления бизнесом являются корпоративные информационные системы. Предприятия нового типа - это разветвленная сеть распределенных подразделений, филиалов и групп, взаимодействующих друг с другом. Распределенные корпоративные информационные системы становятся сегодня важнейшим средством производства современной компании, они позволяют преобразовать традиционные формы бизнеса в электронный бизнес.

Электронный бизнес - это новый способ взаимодействия деловых партнеров, сотрудников и клиентов. Он является исключительно перспективным и потенциально может принести большие доходы. Электронный бизнес использует глобальную сеть Internet и современные информационные технологии для повышения эффективности всех сторон деловых отношений, включая продажи, маркетинг, платежи, финансовый анализ, поиск сотрудников, поддержку клиентов и партнерских отношений.

Важнейшим условием существования электронного бизнеса является информационная безопасность, под которой понимается защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий, которые могут нанести ущерб владельцам или пользователям информации. Ущерб от нарушения информационной безопасности может привести не только к крупным финансовым потерям, но и к полному закрытию компании.

Обеспечение безопасности корпоративной информационной системы является приоритетной задачей для руководства компании, поскольку от сохранения конфиденциальности, целостности и доступности корпоративных информационных ресурсов во многом зависит оперативность принятия решений и эффективность работы компании.

Несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей, к сожалению, не уменьшается. Поэтому проблемы обеспечения информационной безопасности привлекают пристальное внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей, включая компании, работающие в сфере электронного бизнеса.

Задача обеспечения безопасности корпоративных информационной систем (КИС) традиционно решается путем построения подсистемы информационной безопасности (ПИБ) КИС. Определяющим требованием к

ПИБ является сохранение вложенных в построение КИС инвестиций. Другими словами, ПИБ должна функционировать абсолютно прозрачно для уже существующих в КИС приложений и быть полностью совместимой с используемыми в КИС сетевыми технологиями.

Подсистема информационной безопасности предприятия должна учитывать появление новых технологий и сервисов, а также удовлетворять общим требованиям, предъявляемым сегодня к любым элементам корпоративной информационной системы:

- *использование интегрированных решений.*

  Интеграция необходима в разных областях:
  - интеграция средств защиты с остальными элементами сети - операционными системами, маршрутизаторами, службами каталогов, серверами QoS-политики и т.п.
  - интеграция различных технологий безопасности между собой для обеспечения комплексной защиты информационных ресурсов предприятия - например, интеграция межсетевого экрана с VPN-шлюзом и транслятором IP-адресов.

- *обеспечение масштабирования в широких пределах.*

  Масштабируемость средств защиты позволяет подбирать оптимальное по стоимости и надежности решение с возможностью постепенного наращивания системы защиты. По мере роста и развития КИС Подсистема Информационной Безопасности должна иметь возможность легко масштабироваться без потери целостности и управляемости. Масштабирование обеспечивает эффективную работу предприятия при наличии у него многочисленных филиалов, десятков предприятий-партнеров, сотен удаленных сотрудников и миллионы потенциальных клиентов.

- *применение открытых стандартов.*

  Переход на открытые стандарты составляет одну из основных тенденций развития средств информационной безопасности. Такие стандарты как IPSec и PKI обеспечивают защищенность внешних коммуникаций предприятий и совместимость с соответствующими продуктами предприятий-партнеров или удаленных клиентов. Цифровые сертификаты X.509 также являются на сегодня стандартной основой для аутентификации пользователей и устройств. Перспективные средства защиты безусловно должны поддерживать эти стандарты уже сегодня.

Для того чтобы обеспечить надежную защиту ресурсов корпоративной информационной системы на сегодня и на ближайшее будущее, в подсистеме информационной безопасности должны быть реализованы самые прогрессивные и перспективные технологии информационной защиты. К ним относятся:

- ***Комплексный подход к обеспечению информационной безопасности***, обеспечивающий рациональное сочетание технологий и средств информационной защиты.
- ***Применение защищенных виртуальных частных сетей VPN*** для защиты информации, передаваемой по открытым каналам связи.
- ***Криптографическое преобразование данных*** для обеспечения целостности, подлинности и конфиденциальности информации.
- ***Применение межсетевых экранов*** для защиты корпоративной сети от внешних угроз при подключении к общедоступным сетям связи.
- ***Управление доступом на уровне пользователей*** и защита от несанкционированного доступа к информации.
- ***Гарантированная идентификация пользователей*** путем применения токенов (смарт-карты, touch-memory, ключи для USB-портов и т.п.) и других средств аутентификации.
- ***Поддержка инфраструктуры управления открытыми ключами PKI.***
- ***Защита информации на файловом уровне*** (путем шифрования файлов и каталогов) для обеспечения ее надежного хранения.
- ***Защита от вирусов*** с использованием специализированных комплексов антивирусной профилактики и защиты.
- ***Технологии обнаружения вторжений (Intrusion Detection)*** для активного исследования защищенности информационных ресурсов.
- ***Централизованное управление средствами информационной безопасности.***

Без знания и квалифицированного применения современных технологий, стандартов, протоколов и средств защиты информации невозможно достигнуть требуемого уровня информационной безопасности корпоративных систем и сетей.

Книга посвящена систематическому изложению современных методов, средств и технологий защиты информации в распределенных корпоративных информационных системах и компьютерных сетях.

Книга имеет следующую структуру. Основное содержание книги, состоящее из двадцати глав, разбито на четыре логически связанных крупных раздела - четыре части:

Часть 1. Интернет, электронный бизнес и проблемы безопасности корпоративных информационных систем.

Часть 2. Методы и алгоритмы криптографической защиты информации.

Часть 3. Технологии защиты информационных ресурсов.

Часть 4. Комплексное решение проблем обеспечения информационной безопасности корпоративных информационных систем.

Каждая из этих частей объединяет несколько глав, связанных общей темой.

Книга содержит также предисловие, введение, приложения и список литературы.

Часть 1 объединяет главы 1, 2 и 3.

В ***главе 1*** приводится краткая история создания глобальной сети Интернет и развития Интернет в России. Описываются основные информационные услуги сети Интернет, указываются возможности и преимущества использования Сети. Рассматриваются перспективы развития Интернет - приложений в начале третьего тысячелетия.

Глава 2 целиком посвящена проблемам и перспективам развития электронного бизнеса и электронной коммерции в Интернете. Рассматриваются особенности основных моделей электронной коммерции B2C и B2B. Описываются основные виды электронной торговли: Интернет - магазины, Интернет - биржи и Интернет - аукционы; основные Интернет - услуги: Интернет - банкинг, Интернет - трейдинг и Интернет - страхование. Подробно разбирается функционирование систем электронных платежей через Интернет. Анализируются проблемы безопасности систем электронного бизнеса; формулируются пути и способы обеспечения безопасности электронного бизнеса.

В ***главе 3*** разъясняются основные понятия информационной безопасности; рассматриваются стандартные стеки коммуникационных протоколов; описываются возможные сетевые атаки на IP-сети и службы Интернет; анализируются угрозы безопасности для корпоративных информационных систем; систематизируются меры обеспечения информационной безопасности АСОИ и рассматриваются основные этапы построения подсистемы информационной безопасности для корпоративных информационных систем.

Часть 2 содержит главы с 4 по 10.

В ***главе 4*** приводятся основные понятия и определения криптографической защиты информации. Кратко описано развитие криптографической защиты от самых первых шифров до работ К. Шеннона, теоретически обосновавшего современные симметричные шифры, и работ У. Диффи и М. Хеллмана, посвященных созданию асимметричных криптосистем. Глава завершается рассмотрением классификации средств защиты информации, использующих криптографические методы.

Глава 5 посвящена современным симметричным криптосистемам. Приведены сведения по распространенным блочным алгоритмам шифрования данных, включая новый стандарт шифрования США - алгоритм AES. Рассмотрены основные режимы работы блочных симметричных алгоритмов. Описывается отечественный стандарт шифрования данных. Показано, как можно повысить криптостойкость блочных шифров, применяя их каскадирование.

В ***главе 6*** обсуждаются современные асимметричные криптосистемы (с открытыми ключами). Приводится концепция построения асимметричной криптосистемы, описываются однонаправленные (односторонние) функции, на которых базируется криптография с открытыми ключами. Особое внимание уделено криптосистеме RSA, получившей широкое распространение как в США, так и в других странах. Рассмотрены и другие схемы асимметричного шифрования. Показано, как, используя комбинированный метод шифрования, можно построить криптосистему, объединяющую достоинства симметричных и асимметричных криптосистем.

В ***главе 7*** определены основные свойства и области применения функций хэширования. Рассмотрены функции хэширования MD4 и MD5, разработанные Р.Райвестом, и алгоритм безопасного хэширования SHA. Обсуждаются способы построения хэш-функций на основе симметричных блочных алгоритмов шифрования. Описан отечественный стандарт функции хэширования.

Глава 8 посвящена электронной цифровой подписи, позволяющей решить проблему аутентификации электронного документа и его автора. Обсуждаются алгоритмы электронной цифровой подписи RSA, Эль Гамаля и DSA. Описывается отечественный стандарт цифровой подписи. Глава завершается разделом, посвященным цифровым подписям с дополнительными функциональными возможностями. В этом разделе рассмотрены схемы слепой цифровой подписи и неоспоримой цифровой подписи, существенно расширяющие возможности обычной электронной цифровой подписи.

В ***главе 9*** вводятся понятия простой и строгой аутентификации (проверки подлинности) пользователей. Разбираются особенности простой аутентификации на основе многоразовых и одноразовых паролей, на основе цифровых сертификатов. Рассмотрены типовые схемы идентификации и аутентификации пользователя. Обсуждаются средства биометрической идентификации и аутентификации. Особое внимание уделяется строгой аутентификации, основанной на симметричных и асимметричных криптоалгоритмах. Подробно обсуждаются современные протоколы гарантированной идентификации с нулевой передачей знаний.

В ***главе 10*** описываются способы реализации таких важных функций управления криптографическими ключами, как генерация, хранение и распределение ключей. Приводятся основные варианты носителей ключевой информации. Рассматривается концепция иерархии ключей. Особое внимание уделено самому ответственному процессу в управлении ключами – распределению ключей. Приводятся особенности протокола аутентификации и распределения ключей Kerberos, описывается алгоритм открытого распределения ключей Диффи-Хеллмана.

Часть 3 объединяет главы с 11 по 16.

Глава 11 представляет собой введение в защищенные виртуальные сети VPN (Virtual Private Network). Поясняется главное свойство сети VPN - туннелирование. Описываются необходимые компоненты сети VPN - сервисы безопасности. Рассматриваются классификационные схемы защищенных виртуальных сетей VPN по ряду признаков. Приводятся VPN - решения, применяемые при построении защищенных корпоративных систем и сетей. Указываются технические и экономические преимущества внедрения технологий VPN в корпоративные информационные системы и сети.

В ***главе 12*** обсуждаются проблемы построения защищенных виртуальных каналов на канальном и сеансовом уровнях эталонной модели взаимодействия открытых систем OSI. Рассматриваются особенности применения протоколов туннелирования на канальном уровне PPTP, L2F и L2TP. Разбираются протоколы аутентификации удаленных пользователей PAP и CHAP, схемы аутентификации с одноразовыми паролями и организация централизованного контроля удаленного доступа. Описывается применение протоколов SSL и SOCKS для построения защищенных виртуальных каналов на сеансовом уровне эталонной модели OSI.

Глава 13 посвящена построению защищенных виртуальных сетей VPN на сетевом уровне модели OSI. Рассматривается архитектура стека протоколов IPSec. Описаны протокол аутентификации AH и протокол формирования защищенного пакета ESP. Приводятся сведения об алгоритмах аутентификации и шифрования, применяемых в стеке протоколов IPSec. Подробно рассматриваются протоколы управления криптоключами SKIP и IKE. Обсуждаются основные схемы применения стека протоколов IPSec и виды защищенных виртуальных сетей VPN на базе IPSec.

В ***главе 14*** рассматривается инфраструктура управления открытыми ключами PKI (Public Key Infrastructure). Обосновывается необходимость использования цифровых сертификатов открытых ключей. Обсуждаются принципы функционирования PKI. Приводятся базовые модели сертификации, логическая структура и компоненты PKI. Описан процесс создания инфраструктуры открытых ключей PKI.

В ***главе 15*** обсуждаются методы и средства защиты локальных и корпоративных сетей от удаленных атак злоумышленников через сеть Internet. Описываются основные компоненты межсетевых экранов и схемы сетевой защиты на базе межсетевых экранов. Приводятся типовые решения по применению межсетевых экранов для защиты информационных ресурсов корпоративных сетей. Рассматриваются варианты защиты периметра корпоративной сети от несанкционированного доступа (НСД) а также защита корпоративных серверов и рабочих станций корпоративной сети от НСД.

Глава 16 посвящена актуальным проблемам адаптивного управления информационной безопасностью. Обсуждается концепция адаптивного управления безопасностью корпоративной сети. Адаптивный подход к безопасности позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности, используя правильно спроектированные и хорошо управляемые процессы и средства. Подробно разбираются технологии анализа защищенности и обнаружения атак. Описываются средства адаптивного у–правления безопасностью. Приводятся данные по комплексу средств адаптивного управления безопасностью SAFEsuite компании Internet Security Systems и средствам обеспечения безопасности компании Cisco.

Часть 4 объединяет главы с 17 по 20.

В ***главе 17*** рассматривается концепция построения системы обеспечения информационной безопасности распределенной корпоративной системы и сети, разработанная компанией ЭЛВИС-ПЛЮС, которая является ведущим системным интегратором в области создания распределенных информационных систем и интегрированных сетей с использованием современных прогрессивных технологий защиты информации. Описываются компоненты концепции сетевой защиты, организация безопасного взаимодействия с открытыми коммуникационными сетями, формирование и реализация политики безопасности.

В ***главе 18*** систематически рассмотрены информационные технологии, применяемые компанией ЭЛВИС-ПЛЮС при построении защищенных виртуальных сетей VPN. Обосновывается комплексный подход к решению проблем обеспечения информационной безопасности. Показывается роль и место VPN - технологий в общей структуре обеспечения комплексной защиты информации. Приводятся конкретные данные по информационным технологиям, обеспечивающим комплексную защиту.

В ***главе 19*** описываются современные отечественные VPN - продукты, популярного продуктного ряда ЗАСТАВА 2.5 компании ЭЛВИС-ПЛЮС. Подробно рассмотрены функциональные характеристики VPN - продуктов: ЗАСТАВА-Персональный клиент, ЗАСТАВА-Корпоративный клиент, ЗАСТАВА-Сервер, ЗАСТАВА-Офис, Центр управления ЗАСТАВА, а также сервер сертификатов ЗАСТАВА, Центр сертификации ЗАСТАВА и др. Отмечаются такие достоинства продуктов ЗАСТАВА как строгое соблюдение международных и Internet стандартов и открытость архитектуры, рациональное решение проблемы криптографической защиты, развитые средства аутентификации пользователя, эффективное управление ключевой инфраструктурой, гибкая защита корпоративной компьютерной сети, многоплатформенность, масштабируемость и полнота продуктного ряда. Приводятся особенности системы VPN - продуктов ЗАСТАВА 3.2.

В ***главе 20*** рассматриваются типовые решения компании ЭЛВИС-ПЛЮС по применению средств виртуальных защищенных сетей VPN для защиты информационных ресурсов организаций и предприятий, включая корпорации с распределенными подразделениями и филиалами. Приводятся типовые решения для защиты информационных ресурсов предприятий малого и среднего бизнеса, в частности, защита документооборота, создание системы защищенной электронной почты, бухгалтерских прикладных систем, подключение мобильных пользователей к информационным ресурсам по защищенному каналу и т.п.

Типовые решения по защите информационных ресурсов предприятий крупного бизнеса учитывают разнообразие и масштаб решаемых задач, сложную распределенную структуру, многообразие связей, глубокую иерархичность и высокие требования к системам обеспечения информационной безопасности. Приводится ряд типовых решений, в частности, объединение офисов организации в единую защищенную

корпоративную сеть, обеспечение защищенного доступа удаленных и мобильных пользователей к информационным ресурсам компании, защита прикладных распределенных информационных систем, защита почтовой корпоративной системы, создание системы централизованного управления средствами защиты, защита информационных ресурсов финансовых организаций (банков, финансовых бирж, страховых компаний), имеющих офисы, клиентов, агентов по всему миру.

В состав Приложений к книге включены сравнительные характеристики VPN-продуктов российских производителей; сравнительные характеристики некоторых межсетевых экранов; основные характеристики VPN-продуктов ЗАСТАВА; описание нового американского стандарта шифрования данных AES.

Весь материал книги базируется только на открытых публикациях в Internet, отечественной и зарубежной печати. В основу книги положены материалы лекций, читаемых авторами в Московском институте электронной техники, а также результаты их научных и проектных работ, связанных с созданием средств VPN и комплексных систем защиты информационных ресурсов организаций и предприятий с распределенными подразделениями и филиалами.
