УДК 004.056

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСТНОСТИ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ДАННЫХ МЕЖДУ НЕСКОЛЬКИМИ ПРЕДПРИЯТИЯМИ ПО СЕТИ ИНТЕРНЕТ

А.С. СИВОГРАКОВ
(Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

В данной работе рассмотрим и проанализируем основные технологии обеспечения безопасности информации при передаче данных по сети Интернет.

В настоящее время главным инструментом управления бизнесом и фактически важнейшим средством производства становятся корпоративные информационные системы. Основными видами деятельности для многих компаний становятся электронная коммерция, продажа информации в режиме on-line и другие услуги. Так же из-за того, что большинство компаний не ограничивают себя территориально им приходится реализовывать каналы для передачи данных между офисами. Для этого удобно использовать уже существующую сеть Интернет. Но передача данных по открытым сетям не гарантирует их безопасность.

Информация, обрабатываемая в корпоративных сетях, является особенно уязвимой, чему способствуют:

1. увеличение объемов обрабатываемой, передаваемой и хранимой в компьютерах информации;
2. сосредоточение в базах данных информации различного уровня важности и конфиденциальности;
3. расширение доступа круга пользователей к информации, хранящейся в базах данных, и к ресурсам вычислительной сети;
4. увеличение числа удаленных рабочих мест;
5. широкое использование глобальной сети Интернет и различных каналов связи;
6. автоматизация обмена информацией между компьютерами пользователей.

Для комплексной зашиты от угроз и гарантии экономически выгодного и безопасного использования коммуникационных ресурсов для электронного бизнеса необходимо:

1. проанализировать угрозы безопасности для системы электронного бизнеса;
2. разработать политику информационной безопасности;
3. защитить внешние каналы передачи информации, обеспечив конфиденциальность, целостность и подлинность передаваемой по ним информации;
4. гарантировать возможность безопасного доступа к открытым ресурсам внешних сетей и Internet, а также общения с пользователями этих сетей;
5. защитить отдельные наиболее коммерчески значимые ИС независимо от используемых ими каналов передачи данных;
6. предоставить персоналу защищенный удаленный доступ к информационным ресурсам корпоративной сети;
7. обеспечить надежное централизованное управление средствами сетевой защиты.

Рассмотрим наиболее распространённые способы обеспечения безопасности корпоративной информации на предприятиях.

SSL. Протокол SSL применяется в качестве протокола защищенного канала, работающего на сеансовом уровне модели OSI. Этот протокол использует криптографические методы защиты информации для обеспечения безопасности информационного обмена. [4] Протокол SSL выполняет все функции по созданию защищенного канала между двумя абонентами сети, включая их взаимную аутентификацию, обеспечение конфиденциальности, целостности и аутентичности передаваемых данных. Ядром протокола SSL является технология комплексного использования асимметричных и симметричных криптосистем.

Взаимная аутентификация обеих сторон в SSL выполняется путем обмена цифровыми сертификатами открытых ключей пользователей (клиента и сервера), заверенными цифровой подписью специальных сертификационных центров. Протокол SSL поддерживает сертификаты, с помощью которых организуется выдача и проверка подлинности сертификатов.

Конфиденциальность обеспечивается шифрованием передаваемых сообщений с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении со- единения. Сессионные ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей, извлеченных из сертификатов абонентов. Использование для защиты сообщений симметричных ключей свя-

зано с тем, что скорость процессов шифрования и расшифрования на основе симметричного ключа существенно выше, чем при использовании несимметричных ключей. Подлинность и целостность циркулирующей информации обеспечивается за счет формирования и проверки электронной цифровой подписи.

Такой способ защиты широко используется в мире Веб для приложений, в которых важна безопасность соединения, например, в платежных системах.

Протокол шифровании SSL также часто используется для шифрования каналов связи с базами данных.

Криптопровайдеры. Не возможность применения протокола шифрования SSL в некоторых случаях привела к появлению криптопротаколов. Криптопровайдер — это независимый модуль, позволяющий осуществлять криптографические операции в операционных системах, управление которым происходит с помощью функций CriptoAPI. То есть, это посредник между операционной системой, которая может управлять им с помощью стандартных функций CryptoAPI, и исполнителем криптографических операций.

Криптопровайдер должен обеспечивать:

1. реализацию стандартного интерфейса криптопровайдера;
2. работу с ключами шифрования, предназначенными для обеспечения работы алгоритмов, специфичных для данного криптопровайдера;
3. невозможность вмешательства третьих лиц в системы работы алгоритмов.

Использование криптопровайдера позволяет сделать шифрование данных прозрачным для любого приложения и любого протокола передачи данных.

Электронная цифровая подпись. Электронная цифровая подпись — реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования электронной цифровой подписи и проверить принадлежность подписи владельцу сертификата ключа электронной цифровой подписи. [2] Значение реквизита получается в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи.

Цифровая подпись предназначена для аутентификации лица, подписавшего электронный документ. Кроме этого, использование цифровой подписи позволяет осуществить:

1. Контроль целостности передаваемого документа: при любом случайном ли преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.
2. Защиту от изменений документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.
3. Невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом.
4. Доказательное подтверждение авторства документа: Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу подписи под документом.

Все эти свойства электронной цифровой подписи позволяют использовать её для следующей целей:

1. Декларирование товаров и услуг (таможенные декларации).
2. Регистрация сделок по объектам недвижимости.
3. Использование в банковских системах.
4. Электронная торговля и госзаказы.
5. Контроль исполнения государственного бюджета.
6. В системах обращения к органам власти.
7. Для обязательной отчетности перед государственными учреждениями.
8. Организация юридически значимого электронного документооборота.
9. В расчетных и трейдинговых системах.

Крипто-Про CSP. КриптоПро CSP представляет собой криптопровайдер, средство криптографической защиты, предназначенное для обеспечения целостности программных приложений при помощи методов шифрования. [3] Также программное обеспечение позволяет защитить конфиденциальную информацию при обмене данными через интернет и обеспечить юридическую достоверность электронных документов.

В современном мире необходимо рассматривать вопросы обеспечения безопасности информации при передаче данных по открытым сетям, особенно это касается внутренней корпоративной информации на предприятиях, конфиденциальность которой стоит особо остро. Постоянное усовершенствование технологий угроз защите информации ведет к технологическому развитию средств защиты и наиболее перспективны на этом пути комплексные средства обеспечения доверенного сеанса связи, которые были представлены в этой статье.

ЛИТЕРАТУРА

1. Электронный ресурс «VPN». Режим доступа: http://ru.wikipedia.org/wiki/VPN. Дата доступа: 12.08.2020
2. Веденьёв Л.Т., Леонтьев С.Е. и Попов В.О. Вопросы повышения безопасности ключей пользователей в среде вычислительной системы. Доклад на конференции РусКрипто 2009.
3. Электронный ресурс «Крипто-Про CSP». – Режим доступа: http://www.cryptostandart.ru/showtopic/index.php?id=program_cryptopro. – Дата доступа: 12.08.2020
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Москва ИД «ФОРУМ» – ИНФРА-М 2011.