В. М. Ничипорчук
Московский инженерно-физический институт (государственный университет)

АРХИТЕКТУРА КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ РАСПРЕДЕЛЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

В статье приведена разработанная автором архитектура системы защиты, решающая задачу по усилению мер защиты информации и созданию комплексной системы защиты информации распределенной автоматизированной системы. Полученное решение имеет опыт двух успешных внедрений комплексной системы защиты информации для катастрофоустойчивых распределенных автоматизированных систем по обработке конфиденциальной информации.

Существует множество типов автоматизированных систем (АС), наиболее сложными с точки зрения обеспечения безопасности данных являются АС, имеющие распределенную архитектуру с сетевым взаимодействием элементов системы [1]. Перед организациями, эксплуатирующими такую АС или планирующими масштабирование существующих систем до этого уровня, все чаще возникает задача обеспечения защиты информации, циркулирующей в АС, в связи с возрастающими потребностями информационного обеспечения протекающих бизнес-процессов. Обычно в качестве каналов связи между компонентами распределенной АС используются открытые каналы, арендованные у различных региональных провайдеров, в качестве системы хранения данных используются один или несколько файловых серверов с дисковым RAID-массивом, централизованное управление всеми компонентами АС отсутствует, большая часть АС слабо документирована. Чаще всего имеющиеся средства защиты и организация защиты информации не удовлетворяют в полной мере возросшим требованиям по обеспечению конфиденциальности, целостности и доступности обрабатываемой информации в связи с отсутствием комплексной системы защиты информации.

Объект защиты представляет собой территориально-распределенный комплекс по обработке финансовой информации, а также предоставлению дополнительных сервисов связи между удаленными подразделениями. Объект включает в себя головной центр обработки данных (ЦОД), резервный центр обработки данных и около сотни удаленных региональных подразделений (Рис. 1).

Рис. 1. Структура системы

Исходя из анализа требований признано необходимым поэтапное создание и внедрение системы защиты путем ее разбиения на ряд взаимосвязанных элементов (функциональных подсистем). Такое модульное построение не только облегчает все этапы создания единой комплексной системы, но и делает систему более гибкой, позволяя заменять и модифицировать каждую подсистему, не затрагивая остальные элементы системы.

Все основные подсистемы АС и элементы системы защиты тесно взаимосвязаны, каждая из подсистем предоставляет функции другим системам, а также использует их функции. Общая структура и схема связей между подсистемами показана на рис. 2.

Рис. 2. Схема связей между подсистемами

Учитывая опыт создания современных информационных систем и создаваемую в рамках проекта защищенную сеть передачи данных, обеспечивающую защищенную передачу любых данных между центральным подразделением и региональными подразделениями, была предложена архитектура системы (Рис. 3) [2]. Предложенная архитектура отображает взаимодействие сети хранения данных, службы единого каталога, службы электронной почты, антивирусной подсистемы, подсистемы резервирования критически важных ресурсов, подсистемы резервирования каналов связи и подсистемы защиты каналов связи.

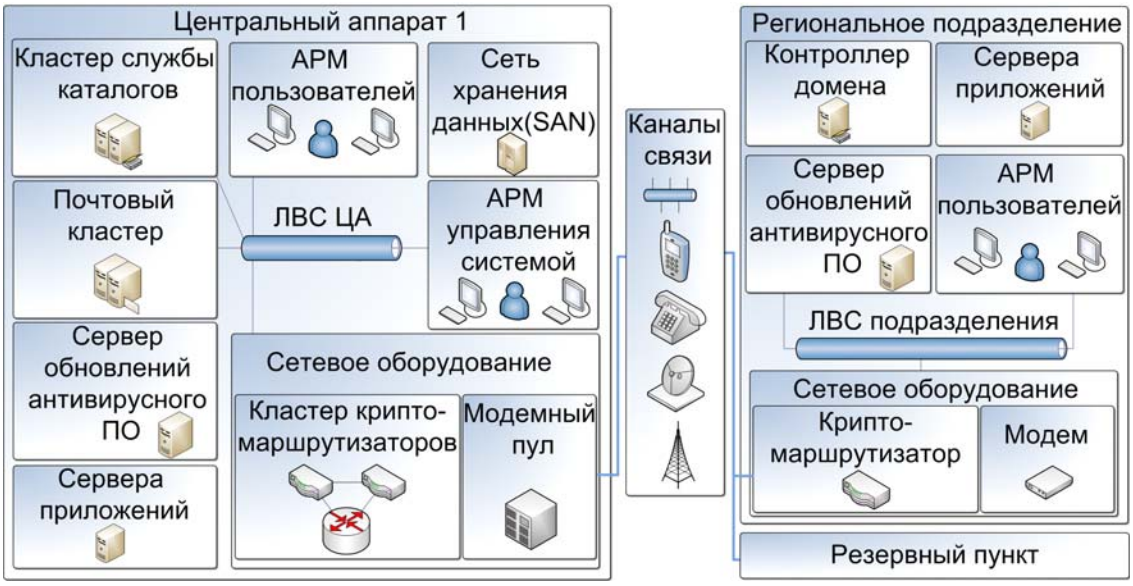

Рис. 3. Общая архитектура системы

Все сетевое взаимодействие по открытым сетям проходит через защищенную виртуальную частную сеть, построенную с помощью криптомаршрутизаторов [3].

Сеть хранения данных построена в центральном офисе. Пользователи центрального аппарата (ЦА) и территориальных подразделений получают доступ к информации, расположенной в системе хранения данных, посредством серверов корпоративной почтовой системы и серверов приложений.

Корпоративная почтовая система строится по централизованному принципу. Все пользователи для получения и отправки электронной почты обращаются к почтовому кластеру, расположенному в центральном офисе.

Служба единого каталога строится по территориально-распределенному принципу. В каждом сегменте локальной сети (ЦА и территориальных подразделений) установлен контроллер домена. Все контроллеры домена территориальных подразделений синхронизируются с контроллером домена ЦА. Идентичность контроллеров домена, используемых в подразделениях, позволяет повысить надежность и доступность системы авторизации пользователей и упростить процесс внедрения и последующего обслуживания системы.

Для снижения вероятности принятия неавторизованного пользователя и упрощения хранения ключей шифрования и ЭЦП используются интеллектуальные карты (ИК). Использование таких карт позволило внедрить двухфакторную аутентификацию пользователей и обеспечить аппаратно защищенное хранение закрытых ключей шифрования и ЭЦП.

Антивирусная подсистема, предназначенная для защиты серверов и рабочих станций пользователей, построена по территориально-распределенному принципу. В каждом сегменте локальной сети (ЦА и территориальных подразделений) установлен сервер обновления. Серверы обновлений территориальных подразделений получают обновления от сервера ЦА и обеспечивают процесс обновления антивирусного ПО на всех серверах и рабочих станциях данного подразделения.

Служба каталогов предоставляет множество способов аутентификации объектов системы. По умолчанию пользователи используют однофакторную аутентификацию (имя пользователя и пароль), данный способ аутентификации обладает рядом недостатков, в том числе такие проблемы, как нахождение золотой середины между простыми паролями и сложными паролями, которые для огромного количества пользователей не имеют общего решения. Поэтому было принято решение усилить аутентификацию путем использования ИК Aladdin Etoken, в данном случае ИК используется как защищенное хранилище сертификата, используемого Active Directory для аутентификации владельца.

Данный метод обеспечивает строгую двухфакторную аутентификацию пользователей при входе в сеть Windows и службу каталога Active Directory на основе цифровых сертификатов стандарта X.509. Функции удостоверяющего центра (англ. certification authority, CA) выполняет служба сертификатов, входящая в состав серверов Windows. Решение поддерживает технологию Windows Single Sign-On, которая обеспечивает единую регистрацию пользователя и устраняет необходимость дополнительной регистрации в каждой из используемых прикладных программ. ИК совместима с продуктами PKI ведущих мировых и отечественных производителей, в нашем случае использовался криптопровайдер «Крипто Про».

В системе ИК предназначена для усиления функций безопасности ОС Microsoft Windows 2000/XP/2003 за счёт полного отказа от парольной аутентификации в пользу строгой двухфакторной аутентификации, хранения сертификатов для обеспечения конфиденциальности и целостности электронной почты Domino Lotus документов за счёт использования ЭЦП и шифрования данных, обеспечения безопасного подключения к удалённому рабочему столу Windows XP или Windows Server 2003, аутентификации в среде IBM Domino Lotus, включая системы электронной почты и документоориентированные базы данных.

Таким образом, мы получаем единую сквозную систему аутентификации пользователей. Помимо сертификатов аутентификации пользователя ИК содержит сертификаты для шифрования и подписи почтовых сообщений (Рис. 4).

Рис. 4. Хранение сертификатов на ИК Etoken

Невозможно представить крупную современную компанию без корпоративной электронной почты. Электронная почта значительно упрощает обмен информацией, ежедневно помимо обычных записок и уведомлений через почту циркулирует конфиденциальная информация, содержащая сведения ограниченного распространения. В связи с этим в случае отсутствия специальных средств защиты корпоративная почта потенциально является каналом утечки конфиденциальной информации. Среди таких средств защиты используются средства шифрования всего трафика в сети между почтовым клиентом и сервером (подсистема защиты каналов), средства шифрования и ЭЦП отдельных почтовых сообщений.

В системе защиты объекта используются оба вышеуказанных средства. По умолчанию в штатном режиме работы подсистемы защиты каналов используются оба эти средства, в данном случае функция защиты отдельных почтовых сообщений используется для обеспечения аутентичности почтовых сообщений (ЭЦП), шифрование тела сообщения обеспечивается функциями подсистемы защиты каналов (шифрование трафика). В случае отказа основного канала связи используются резервные каналы связи, защита трафика которых не обеспечивается подсистемой защиты каналов, в данном случае подсистема защиты электронной почты шифрует и подписывает каждое отдельное сообщение.

Полученная подсистема представляет собой законченное программное решение по автоматизации работы почтового сервера, способного передавать зашифрованную и подписанную электронную почту. Даная система поддерживает работу пользователей с помощью клиента IBM Lotus Notes. Для осуществления операций по засекречиванию конфиденциальной информации, содержащейся в почтовом сообщении, используются сертифицированные ФСБ средства шифрования на основе криптопровайдера «Крипто Про» версии 2.0 или 3.0.

Для защиты информации, передаваемой по открытым каналам связи, была спроектирована и внедрена подсистема защиты каналов. Она предназначена для автоматизации процесса криптографической защиты данных, содержащих конфиденциальную информацию различного характера, передаваемых по открытым каналам связи между структурными подразделениями и ЦА. Криптографическая защита обеспечивается посредством программно-аппаратного комплекса «Континент-К». Полученная система автоматизирует выполнение следующих задач: предоставление безопасного прямого доступа сотрудников территориальных структурных подразделений к конфиденциальной информации, расположенной в информационных системах ЦА; управление маршрутами потоков информации в сети (формирование

карты подключения территориальных структурных подразделений); фильтрация трафика в сети; защита информации от несанкционированного доступа по классу «1Г».

Общая архитектура подсистемы представлена на рис. 5.

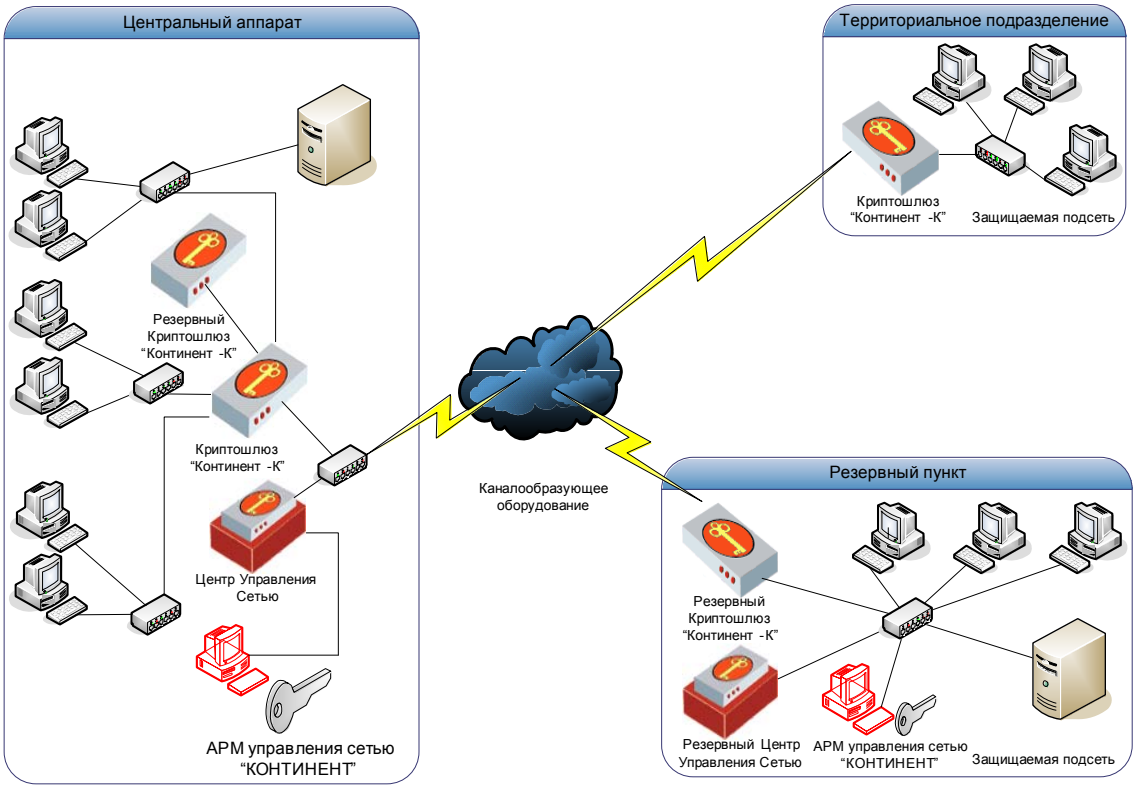

Рис. 5. Общая архитектура подсистемы защиты каналов

Описанная в статье архитектурная модель комплексной системы защиты распределенной автоматизированной системы и ее подсистем нашла практическое применение в двух проектах по созданию комплексной системы защиты информации. Оба проекта были доведены до этапа опытной эксплуатации подсистем защиты.

СПИСОК ЛИТЕРАТУРЫ:

1. *Герасименко В. А., Малюк А. А.* Основы защиты информации. М., 1997.
2. *Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В.* Информационная безопасность открытых систем: Учебник для вузов. М. 2006.
3. *Запечников С. В., Милославская Н. Г., Толстой А. И.* Основы построения виртуальных частных сетей: Учеб. пособие для вузов. М. 2003.