УДК 519.862

Т.В.Глотова, Х.И.Бешер

АНАЛИЗ ПОДХОДОВ, ОБЕСПЕЧИВАЮЩИХ ЗАЩИЩЕННОСТЬ СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

Воронежский институт высоких технологий

В статье рассматриваются вопросы, связанные с использованием различных подходов для повышения эффективности защищенности компьютерных систем. Отмечается важность интеграции различных технологий безопасности для обеспечения комплексной защиты информационных ресурсов предприятия. Показано, что межсетевые экраны являются главным средством контроля по доступу к ресурсам корпоративной сети извне. Дана классификация групп пользователей, которые подлежат распознаванию при анализе сетевого трафика. Отмечается важность использования учетных данных пользователей, хранящихся в службе каталогов сети. Приведены характеристики аутентификация на основе сертификатов. Указаны главные свойства средств обнаружения вторжений. Говорится о необходимости аппаратной реализации типовых функций, используемых при аутентификации.

Ключевые слова: информационная безопасность, компьютерная система, информационная сеть, сетевой трафик, защита информации.

В настоящее время неотъемлемыми элементами в бизнесе многих компаний можно отметить осуществление электронных транзакций с использованием глобальных возможностей Internet и других публичных сетей. Прогнозируемые превращения в ближайшем будущем Internet в новые публичные сети (New Public Network), которые предоставляют массовым пользователям все типы информационных услуг и переносящие все типы трафиков в глобальных масштабах, должны превращать эти тенденции в норму жизни [1, 2].

Применение электронной коммерции, проведение продажи информации, доведение консультационных услуг в режимах on-line и различные другие виды услуг становятся для компаний в развивающихся условиях как основные виды деятельности, в этой связи проведение разрушения информационных ресурсов, их временная недоступность или применение несанкционированным образом могут дать для компаний значительные материальные ущербы [3, 4].

Создание массовых и разных связей компании на основе примененеия Internet при одновременном обеспечении безопасности подобных коммуникаций в существующих условиях рассматривается как основной фактор, влияющий на процессы развития средств защиты предприятия [5,6].

С целью формирования прочных основ в массовых глобальных сетях IP-технологии быстрым образом приобретают различные новые

характеристики, связанные с поддержкой дифференцированных по пользователям и приложениям качеств обслуживания (QoS), управления сетями на базе централизованных политик, группового вещания и т.д., и т.п.

Непрерывным образом возникают и различные информационные сервисы, например, сервисы, связанные с передачей голоса - VoIP, сервисы, направленные на поиск и доставку новостей PointCast и другие. В средствах безопасности должны быть учтены подобные изменения, поскольку в каждой новой технологии и новом сервисе могут потребоваться свои адекватные средства защиты, а также будет оказываться влияние на уже используемые.

Например, проведение дифференцированного обслуживания трафика на базе признаков, которые находятся в заголовке и поле данных IP-пакета, будет затруднительно вследствие применения средств инкапсуляции и шифрации IP-пакетов, которые используют для защищенных каналов VPN и идет закрытие доступа к необходимым признакам. В перспективных средствах защиты данных компании необходимо учитывать возникновение соответствующих технологий и сервисов, кроме того они должны соотноситься с общими требованиями, которые предъявляются в настоящее время к различным элементам корпоративных сетей [7,8].

Но без того, чтобы следовать открытым стандартам трудно представить построение системы защиты коммуникаций с компаниями-партенерами и массовым клиентом, их можно найти в Intrenet. То, что были приняты такие стандарты как IPSec и IKE можно считать значительным шагом по пути открытости стандартов и такие тенденции должны поддерживаться.

Необходимо, чтобы обеспечивались интегрированные решения [9-11]. Проведение интеграции важно с точки зрения разных аспектов: осуществление интеграции разных технологий безопасности с целями того, чтобы обеспечивалась комплексная защита по информационным ресурсам компании - например, проведение интеграции межсетвых экранов с VPN-шлюзом и трансляторами IP-адресов, проведение интеграция средств защиты и остальных сетевых элементов - операционные системы, маршрутизаторы, службы каталогов, сервера QoS-политика и т.п.

Важно проводить процессы масштабирования в широких пределах, другими словами обеспечивается эффективная работа при существовании у компании многих филиалов, десятков организаций-партнеров, сотен удаленных работников и миллионы возможных клиентов [12-14].

Традиционным образом межсетевые экраны рассматриваются как основное средство по контролю внешнего доступа для ресурсов корпоративных сетей, путем ограничения проникновения трафика в

область внутренних подсетей предприятий и тем самым существенным образом снижается потенциальная угроза для ресурсов корпоративных сетей. В течение долгого времени происходила ориентация характеристик межсетевых экранов на достаточно простые схемы доступа: свойства доступа контролировались для одной точки, которая рассматривалась по путям соединения внутренних сетей с Internet или другими публичными сетями, рассматриваемые как источник потенциальных угроз.

Происходило деление всех субъектов доступа по группам по IP-адресам, причем достаточно часто - по двум группам - внутренним и внешним пользователям. Тогда в качестве субъектов доступа были подсети и проведение классификации трафика осуществлять было весьма просто – на основе IP-адресов, явным образом указанным в пакетах.

Для внешних пользователей позволялось для того, чтобы иметь доступ к внутренним ресурсам сетей применять один-два известных сервиса Internet, например электронные почты, базирующиеся на протоколе SMTP, а трафики остальных сервисов отсекались.

В настоящее время в связи с тем, что широко используются разнотипные соединения внутренних сетей компаний с Internet и через Internet, а также повышаются требования по процессам защиты ресурсов от различных внутренних угроз схемы, касающиеся контроля доступа существенным образом усложняются.

У организаций появляются, в основном, не одна точка контроля доступа. Первое, это точки, для которых проводится контроль доступа по не одной внешней сети, например, к публичной компоненте Internet и IP-сетям провайдеров. Организация может также поддерживать различные связи с Internet на основе различных провайдеров для того, чтобы повышать надежность или на основе других соображений. Также, привлечение для автоматизированной обработки информации всех отделов организации и рост требований по защите информации, которая обрабатывается и передается, ведет к необходимости применения межсетевых экранов для внутренних подсетей, что определяет возникновение дополнительных точек, направленных на то, чтобы был контроль доступа [15-17].

Использование нескольких межсетевых экранов внутри сетей организации ведет к требованиям по изменению их характеристик. В основном это связано с возможностями координированных работ по всем экранам на базе общих политик доступа. Осуществление координации необходимо для того, чтобы корректным образом проводить обработку пакетов пользователей, вне зависимости от того, через какие точки доступа проходят их маршруты. Изменения маршрутов пакетов могут осуществляться как по долговременным, так и по кратковременным основам.

Осуществление долговременных изменений (по часам или суткам) идет обычно вследствие перемещений пользователей среди разных географических пунктов (сейчас пользователи работают в базовом здании, потом - дома, а через неделю - в филиалах в других городах) и для того, чтобы был учет достаточно сделать загрузку по всем межсетевым экранам единого набора правил по контролю доступа. Могут наблюдаться Краткие по времени изменения в маршрутах пакетов – это касается секунд или даже миллисекунд – они связаны с тем, что у IP-маршрутизации динамическая природа (ожидаемые переходы на маршрутизации при учете маршрутизаторов - QoS-based routing -, лишь приведет к усилению такой динамики).

Краткие во времени изменения в маршрутах требуют от экранов не только координированных заданий по правилам доступа, но и то, чтобы была синхронизация по состояниям отслеживаемых сессий для различных экранов с тем, чтобы любые пакеты корректным образом соотносились с определенными сессиями.

Для того, чтобы обеспечить масштабируемость, осуществление координации правил доступа определяет централизованную систему задания и распространения соответствующих правил [18-20].

Для новых условий необходимо создать изменения и по субъектам доступа – помимо подсетей это относится и к группам пользователей и даже отдельным пользователям. Это касается, прежде всего, того, что путем применения Internet и других глобальных сетей и корпоративных сетей сейчас происходит связь различных категорий пользователей, и им требуется предоставлять различные доступы к внутренним ресурсам. Также, проведение ориентации по пользователям можно рассматривать как следствие использования межсетевых экранов для того чтобы был контроль трафиков среди внутренних подсетей, что определяет для субъектов межсетевого доступа большое число работников данной фирмы. Как результат от межсетевых экранов требуется проведение распознавания большого количества групп работников, среди которых:

- Работники подразделений организации, имеющие доступ во внутреннюю сеть,
- Удаленные и мобильные работники компании,
- Работники организаций-партнеров по бизнесу, это касается удаленных и мобильных,
- Клиенты организации, которые получают услуги на основе Internet,
- Потенциальные клиенты, которые просматривают рекламу организаций на основе Internet.

Можно в каждой из таких категорий пользователей отметить отличия по правам доступа, причем в категориях можно выделить

подкатегории, а для некоторых пользователей (например, руководителей) требуется поддержка индивидуального доступа.

Проведение классифицирования таких групп пользователей лишь базируясь на их IP-адресах, как это обычно делают в межсетевых экранах, практически невозможно, при учете использования таких способов управления IP-адресами как DHCP, NAT и туннелирование. В этой связи проведение контроля доступа на уровнях пользователя требует, чтобы была поддержка в межсетевых экранах, поддерживались собственные средства по работе с учетной информацией пользователя и средства аутентификации. Также, весьма желательно достижение тесной интеграции таких средств с используемыми в сетях системами администрирования и аутентификации пользователя.

Пользователи, прошедшие аутентификацию для межсетевого экрана, становятся объектами правил доступа, которые разработаны или для них лично, или для группы пользователей, куда они входят. Помимо детализации прав доступа, работы на уровнях пользователей позволяют повышать эффективность в аудите событий, которые связаны с безопасностью. Подобный аудит предоставляет информацию о том, кто, когда и на основе каких средств (протоколов и приложений) имел доступ к ресурсам организации.

Проведение управления безопасностью на пользовательском уровне не позволяет исключить применения IP-адресов когда принимаются решения по доступу и отслеживанию активности пользователя. Также, исполнение детального аудита трудно представить без информации о том, каким из пользователей принадлежит IP-адрес, который указан в пакетах, на основе которых выполняется тот или иной доступ к ресурсу. Для условий с динамическим назначением и изменением адресов такая задача требует от систем, связанных с безопасностью дополнительных работ по тому, чтобы установить соответствие среди пользователей и применяемыми ими IP-адресами.

Для того, чтобы работать с пользователями межсетевые экраны (а при необходимости и другие средства безопасности, например, шлюз VPN) могут исполнять аутентификацию пользователя или полностью самостоятельным образом, или с использованием внешних систем аутентификации и авторизации, которые существуют для сетевых операционных систем или систем, направленных на удаленный доступ. Самостоятельное исполнение аутентификации на основе экрана приводит к тому, что дублируется база учетных записей пользователей, это нежелательный процесс по многим причинам.

При повышении эффективности работы с различными пользователями межсетевые экраны должны уметь применять учетные данные, которые хранятся в службе каталогов сети, при формировании

соответствующих правил доступа (например, при обращении к ним на основе протокола LDAP), а также осуществлять транзитную аутентификацию, при этом выполняется посредническая роль среди пользователей и применяемой в сетях системой аутентификации. Подобный вариант функционирования средств безопасности дает возможности пользователям средств безопасности сосредоточиться на выполнении своих прямых обязанностей и не осуществлять дублирование работ по проведению администрирования пользователей.

В качестве особого случая можно отметить аутентификацию массовых клиентов организации, которая появляется при ведении бизнеса на основе Internet. Когда усложняются схемы бизнеса возникают разные категории массовых клиентов, для которых надо давать разные права по доступу. При процессах аутентификации массового клиента традиционные схемы на базе индивидуальных паролей являются неэффективными, поскольку они требуют ввода в систему и хранения каждых паролей, и, поэтому, плохо масштабируются. Для того, чтобы поддержать работу с массовым пользователем весьма желательно, чтобы межсетевые экраны поддерживали технологию аутентификации на базе цифровых сертификатов. Такие сертификаты дают возможности разбиения пользователей по нескольким классам и предоставления доступа в зависимости от принадлежности пользователе к определенным классам. Инфраструктура публичных ключей необходима, чтобы организовать жизненный цикл сертификатов и позволяет, например, проверять подлинность предъявленных сертификатов за счет осуществления проверок подлинности цифровой подписи сертифицирующей организации (Certificate Authority) или цепочек сертифицирующих организаций, тогда, когда фирма, выдавшая сертификат, не входит в перечень пользующихся на данном предприятии доверием сертификационных центров.

Проведение аутентификации на базе сертификатов может использоваться не только для массового клиента, но и для сотрудников предприятий-партнеров, а также и для собственных сотрудников.

Проведение поддержки межсетевыми экранами сертификатов и инфраструктуры публичных ключей ведет к исключительно масштабируемой системе аутентификации, поскольку в таких случаях в системе необходимо хранение только открытых ключей нескольких корневых сертифицирующих организаций и поддержка протоколов взаимодействия с их серверами сертификатов. Для того, чтобы была успешная работа в гетерогенных средах, порождаемых взаимодействием с разными пользователями и организациями, необходимо, чтобы в средствах безопасности была поддержка продуктов PKI основных ведущих производителей, таких как Entrust, Netscape, Microsoft и т.п. Во ряде случаев требуется контроль доступа не на основе IP-адресов или

каких-либо данных об отправителях/получателях, а в зависимости от содержания передаваемой информации. Например, многие атаки на сеть базируются на том, что внедряются вирусы в код загружаемых пользователями компании программ или в макросы загружаемых документов. Во многих случаях источниками угроз можно рассматривать содержимое электронной почты, которая рассылается массовым порядком [21-23].

Еще одним распространенным видом содержания, которое представляет возможную опасность для сетей, можно считать Java и ActiveX апплеты, которые загружаются в компьютеры организации при просмотрах активных Web-страниц.

Средства контроля содержания можно также рассматривать как эффективное дополнение в традиционных средствах контроля доступа в тех случаях, когда, например, доступы на уровнях пользователей были ошибочным образом заданы слишком свободно, но известны списки ключевых слов, которые содержатся в конфиденциальных документах.

Поскольку для каждого вида потенциально опасного содержания необходимо использование специфических методов контроля, то проведение доступа по содержанию обычно производится на основе отдельных продуктов, дополняющих функции межсетевых экранов. Нов, для увеличения оперативности процессов защиты необходимо, чтобы экраны могли самостоятельным образом исполнять некоторые наборы примитивных функций, часто также их относят к контролю доступа по содержанию, например:

- разрешать выполнять только определенное подмножество операций, которые определенны в протоколе (например, только команды GET в протоколе FTP или метода GET в протоколе HTTP),
- давать доступ лишь для определенного списка URL,
- давать доступ на базе списка разрешенных адресов в электронной почте.

Для остальных случаев межсетевые экраны должны уметь взаимодействовать со специализированными продуктами, передавать им проверки определенного вида содержания.

Средства контроля доступа защищают внутренние ресурсы сети от преднамеренного и непреднамеренного разрушения или использования. Широкое использование Internet и других публичных сетей для организация различных связей предприятия делает необходимым защищать информацию также и при ее передаче. Эта задача решается средствами создания виртуальных частных сетей (VPN) в публичных сетях с коммутацией пакетов. Средства VPN организуют в публичных сетях защищенные каналы, по которым передаются корпоративные данные.

Технология VPN предусматривает проведение комплексной защиты передаваемых данных: при формировании VPN-канала идет проверка аутентичность по двум сторонам, создающих канал, а потом каждый пакет ведет перенос цифровой подписи отправителя, удостоверяющей аутентичность и целостность пакетов. Для достижения защиты от несанкционированного доступа пакет может шифроваться, причем для того, чтобы скрыть адресную информацию, раскрывающую внутреннюю структуру сети, пакет может шифроваться вместе с заголовками и инкапсулироваться во внешние пакеты, несущие лишь адрес внешнего интерфейса VPN-шлюза.

Предыдущие поколения VPN-шлюзов (которые защищают данные по всем узлам сети) и VPN-клиентов (которые защищают данные отдельных компьютеров) во многом применяли фирменные алгоритмы и протоколы защиты данных (для аутентификации сторон, реализации цифровой подписи и шифрования). В настоящее ситуация изменилась - базой для организации защищенных VPN-каналов стал комплекс стандартов Internet, который известен под названием IPSec. Стандартам IPSec характерна гибкость: в них оговариваются обязательные для аутентификации и шифрования протоколы и алгоритмы, что обеспечивает базовую совместимость IPSec-продуктов, и в то же время разработчику продукта не запрещается дополнять этот список другими протоколами и алгоритмами, что делает возможным постоянное развитие системы безопасности.

Для того, чтобы была аутентификация сторон и генерировались сессионные ключи в IPSec предусмотрены возможности применения цифровых сертификатов и инфраструктуры PKI, что делает решение IPSec масштабируемым и согласованным с другими средствами защиты, например, контроля доступа. Протоколы IPSec прошли успешную широкомасштабную проверку в экстрасети ANX автомобильных концернов Америки, и поддержка IPSec сегодня стала обязательным условием для перспективных VPN-продуктов.

Средства VPN предприятия должны эффективно поддерживать защищенные каналы различного вида:

- с удаленными и мобильными работниками (получение защищенного удаленного доступа),
- с сетями филиалов компаний (получение защиты intranet),
- с сетями компаний-партнеров (получение защиты extranet).

Для защиты по удаленному доступу важно существование клиентских частей VPN для базовых клиентских операционных систем, которые в настоящее время пока не поддерживают протоколы IPSec в стандартной поставке. От шлюза VPN в этом варианте требуется хорошая

масштабируемость для поддержания сотен, а возможно и тысяч защищенных соединений.

При защите extranet основным требованием является соответствие реализации VPN-продуктов стандартам IPSec, что с большой степенью уверенности подтверждается наличием у продукта сертификата ICSA. Предприятие может снять с себя часть забот по защите данных, воспользовавшись услугами провайдера по организации VPN. Провайдер настраивает параметры защищенных каналов для своих клиентов в соответствии с их требованиями, а при необходимости дополняет услуги VPN услугами межсетевого экрана, также настраиваемого по заданию пользователя.

В том случае, когда VPN-шлюз поддерживает удаленное защищенное управление, провайдер может взять на себя услуги по конфигурированию и эксплуатации шлюза, установленного на территории пользователя.

Средства контроля доступа в сеть на основе межсетевых экранов и средства организации защищенных каналов представляют собой две основные составляющие любых систем защиты предприятия, поэтому они должны применяться вместе и работать согласованно. Интеграция этих средств может порождать определенные проблемы, особенно в том случае, когда эти средства выполнены в виде отдельных продуктов. Так как и межсетевой экран и VPN-шлюз могут требовать проведения аутентификации пользователей, то желательно согласовывать эти процедуры и выполнять их по возможности прозрачным для пользователя способом. Использование общих схем аутентификации, например, на основе цифровых сертификатов и PKI, упрощает эту задачу.

Существуют другие аспекты интеграции, которые связаны с взаимным расположением экранов и шлюзов относительно внешней связи. Экраны могут исполнять контроль доступа только при работе с незашифрованным трафиком, поэтому по этой причине он должен располагаться после VPN-шлюза. С другой стороны, многие VPN-шлюзы, выполненные как отдельные продукты, не могут защитить себя от разнообразных атак из внешней сети, с чем хорошо справляются межсетевые экраны. Из этих соображений экран помещается перед VPN-шлюзом, но тогда экран пропускает любой зашифрованный трафик, полагаясь на то, что аутентифицированная сторона не причинит вреда внутренним ресурсам сети, что не всегда соответствует действительности. Часто производители отдельных VPN-устройств считают предпочтительной параллельную установку экрана и VPN-шлюза за счет двух каналов доступа к публичной сети. Эта архитектура потенциально еще более опасна, чем предыдущие : VPN-устройство открыто для атак из

публичной сети, а контроль доступа для трафика, проходящего через VPN-шлюз, не производится.

Наиболее просто вопросы интеграции решаются при объединении функций межсетевого экрана и VPN-шлюза в одном продукте, но это требует высокопроизводительной платформы, так как вычислительная сложность операций аутентификации и VPN существенно выше сложности операций фильтрации трафика при контроле доступа. При решении проблем производительности реализация межсетевого экрана и VPN-щлюза в одном продукте является наиболее перспективной для организации комплексной защиты корпоративной сети.

Повысить уровень защищенности корпоративной сети можно с помощью средств обнаружения вторжений (Intrusion Detection). Средства обнаружения вторжений хорошо дополняют защитные функции межсетевых экранов. Если межсетевой экран старается отсечь потенциально опасный трафик и не пропустить его в защищаемые сегменты, то средствами обнаружения вторжений анализируется результирующий (то есть прошедший через межсетевой экран или созданный внутренними источниками) трафик для защищаемых сегментов и выявляются атаки по ресурсам сетей или действия, которые можно классифицировать как потенциально опасные. Средства обнаружения вторжений могут также применяться и в незащищенных сегментах, например, перед межсетевым экраном, для получения общей картины об атаках, которым подвергается сеть извне.

Средства обнаружения вторжений автоматизируют такие необходимые элементы деятельности системы безопасности, как:

- проведение регулярного анализа событий, которые связаны с доступом к ресурсам, на основе данных журналов аудита,
- проведение выявления атак и подозрительной активности, исполнение ответных действий – проведение реконфигурации средств защиты (межсетевые экраны, настройки операционных систем и т.п.) для того, чтобы пресечь подобные атаки в будущем.

Для выполнения своих функций средства обнаружения вторжений обычно используют экспертные системы и другие элементы искусственного интеллекта (например, подсистему самообучения).

Средства обнаружения вторжений могут обнаружить атаку в реальном времени, анализируя реальный трафик в сети, а не журнал аудита. В этом случае желательным свойством такой системы будет тесная интеграция с межсетевым экраном для немедленного блокирования трафика злоумышленника.

Средства обнаружения вторжений должны учитывать тенденции развития технологий корпоративных сетей - наличие большого количества

коммутируемых сегментов, логическую структуризацию сети на основе VLAN, защиту внутреннего трафика с помощью VPN и т.п. Только в этом случае анализ трафика будет полным, а защищенность сети - высокой. Еще одним важным требованием к средствам, направленным на обнаружение вторжений, можно назвать их масштабируемость, которая требуется для выполнения эффективного контроля в условиях постоянно увеличивающего количества сегментов и подсетей, а также количества защищаемых узлов в корпоративной сети [24, 25].

Возникновение и широкое распространение новых высокоскоростных сетевых технологий, это касается и технологий доступа к глобальным сетям и Internet (xDSL, кабельные модемы и т.п.), определяет перед средствами защиты новые задачи в области производительности. Созданные первоначально для работы на одном канале доступа со скоростями в десятки, максимум сотни килобит, межсетевые экраны и VPN-устройства сегодня должны обрабатывать трафик в реальном времени на скоростях в десятки, а иногда и сотни мегабит.

Если учитывать вычислительные сложности и специализированный характер по многим операциям, которые выполняются средствами защиты, то в качестве основного направления роста производительности таких средств будет аппаратная реализация типовых функций, которые используются при осуществлении аутентификации и других VPN-операциях. Аппаратные устройства могут быть выполнены как дополнение к стандартным компьютерным платформам, или же на основе автономного специализированного устройства, которое включает компьютерную платформу и выполняет все функции экрана или VPN-шлюза.

ЛИТЕРАТУРА

1. Канавин С.В. Перспективы применения систем мобильного широкополосного доступа в сетях подвижной радиосвязи на основе стандартов MOBILE WIMAX и LTE / С.В.Канавин, А.С.Лукьянов // Вестник Воронежского института высоких технологий. 2016. № 16. С. 79-82.
2. Глотова Т.В. Особенности архитектуры защищенного корпоративного портала / Т.В.Глотова, В.Н.Кострова / Вестник Воронежского института высоких технологий. 2016. № 16. С. 29-32.
3. Литвинский К.О. Модель подсистемы поддержки принятия решения в системе управления техногенными рисками предприятиях топливно-энергетического комплекса / К.О.Литвинский,

В.А.Малышев, Ю.В.Никитенко // Экономика устойчивого развития. 2015. № 1 (21). С. 91-100.

4. Подсистема проектирования защищенных беспроводных сетей / И.Я. Львович, А.П. Преображенский, Е. Ружицкий, О.Н. Чопоров // Информация и безопасность. - 2015. - Т. 18. - № 4. - С. 556-559.
5. Малышев В.А. Нечеткие алгоритмы планирования и модели взвешенного прогноза распределения ресурсов системы управления специального назначения / В.А.Малышев, В.С.Прокофьев // Вестник Воронежского института высоких технологий. 2008. № 3. С. 049-052.
6. Белоножкин В.И. Методика формализации правила разграничения доступа к информационным ресурсам / В.И. Белоножкин, О.Н. Чопоров // Информация и безопасность. - 2007. - Т. 10. - № 1. - С. 169-172.
7. Мельникова Т.В. Модель проектирования беспроводных систем связи с учетом природных и промышленных помех / Т.В.Мельникова // Вестник Воронежского института высоких технологий. 2016. № 16. С. 61-63.
8. Сазонова С.А. Оценка надежности работы сетевых объектов / С.А.Сазонова // Вестник Воронежского института высоких технологий. 2016. № 16. С. 40-42.
9. Лавлинская О.Ю. Технологии облачных вычислений и их применение в решении практических задач / О.Ю.Лавлинская, Т.М.Янкис // Вестник Воронежского института высоких технологий. 2016. № 16. С. 33-36.
10. Часовской А.А. Оценка перспектив внедрения облачных вычислений на предприятиях и в государственном секторе на примере ФРГ / А.А.Часовской, Е.В.Алференко / Вестник Воронежского института высоких технологий. 2016. № 16. С. 94-97.
11. Нечаева А.И. Особенности функционирования информационных баз на складе / А.И.Нечаева // Вестник Воронежского института высоких технологий. 2016. № 16. С. 64-66.
12. Ермолова В.В. Архитектура системы обмена сообщений в немаршрутизируемой сети / В.В.Ермолова, Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2010. № 7. С. 79-81.
13. Малышев В.А. Структурная модель подсистемы решения задач и прогнозирования в системах автоматизированного проектирования / В.А.Малышев // Вестник Воронежского государственного технического университета. 2005. Т. 1. № 11.
14. Воронов А.А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А.А.Воронов,

И.Я.Львович, Ю.П.Преображенский, В.А.Воронов // Информация и безопасность. 2006. Т. 9. № 2. С. 8-11.

15. Паневин Р.Ю. Реализация транслятора имитационно-семантического моделирования / Р.Ю.Паневин, Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2009. № 5. С. 057-060.
16. Чопоров О.Н. Рационализация управления региональными системами на основе использования методов системного анализа, информационных и ГИС-технологий / О.Н.Чопоров, Н.А.Гладских, С.С.Пронин, М.И.Чудинов, С.Н.Семенов, К.Л.Матюшевский // Прикладные информационные аспекты медицины. 2007. Т. 10. № 2. С. 15-19.
17. Формирование требований к системе информационной безопасности в проектных организациях нефтегазового комплекса / Б.В. Васильев, Н.И. Баранников, А.В. Заряев, В.С. Зарубин, О.Н. Чопоров // Информация и безопасность. - 2015. - Т. 18. - № 4. - С. 508-511.
18. Зяблов Е.Л. Разработка лингвистических средств интеллектуальной поддержки на основе имитационно-семантического моделирования / Е.Л.Зяблов, Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2009. № 5. С. 024-026.
19. Иванов М.С. Разработка алгоритма отсечения деревьев / М.С.Иванов, Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2008. № 3. С. 031-032.
20. Преображенский Ю.П. Адаптивные алгоритмы для бесконечных стохастических игр / Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2010. № 7. С. 46-47.
21. Баранов А.В. Проблемы функционирования mesh-сетей / А.В.Баранов // Вестник Воронежского института высоких технологий. 2012. № 9. С. 49-50.
22. Преображенский Ю.П. Оценка эффективности применения системы интеллектуальной поддержки принятия решений / Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2009. № 5. С. 116-119.
23. Паневин Р.Ю. Структурные и функцинальные требования к программному комплексу представления знаний / Р.Ю.Паневин, Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2008. № 3. С. 061-064.
24. Применение каскадных моделей при оценке рисков распространения вредоносной информации в социальных сетях / Д.О. Карпеев, Д.А. Савинов, А.В. Заряев, В.С. Зарубин, О.Н. Чопоров // Информация и безопасность. - 2015. - Т. 18. - № 4. - С. 512-515.

25. Дешина А.Е. Инновационные технологии регулирования рисков мультисерверных систем в условиях атак комплексного типа / А.В. Дешина, О.Н. Чопоров, К.А. Разинкин // Информация и безопасность. - 2013. - Т. 16. - № 3. - С. 371-374.
26. Симонов К.В. Объекты и схема воздействий террористического характера на интернет-пространство / К.В. Симонов, О.Н. Чопоров // Информация и безопасность. - 2011. - Т. 14. - № 4. - С. 623-624.
27. Чопоров О.Н. Подход к оцениванию опасности угроз как мера совпадения импульсных потоков и вероятности совпадений / О.Н. Чопоров, С.В. Лыков // Информация и безопасность. - 2011. - Т. 14. - № 4. - С. 629-630.

T.V. Glotova, H.I.Besher

THE ANALYSIS APPROACHES THAT GUARANTEE THE SECURITY OF MODERN COMPUTER SYSTEMS

Voronezh Institute of high technologies

The paper discusses issues related to using different approaches to improve the efficiency of computer systems security. The importance of integration of different security technologies together to provide comprehensive protection of information resources of the enterprise is demonstrated. It is shown that firewalls are the main means of controlling access to resources on the corporate network from the outside. The classification of user groups that are subject to recognition in the analysis of network traffic is discussed. The importance of using user credentials stored in the directory service network is shown. The characteristics of the authentication based on certificates are given. The main properties of the means of intrusion detection are stated. The authors refer to the need of the hardware implementation of typical functions used in authentication.

Keywords: information security, computer system, information network, network traffic protection information.

REFERENCES

1. Kanavin S.V. Perspektivy primeneniya sistem mobil'nogo shirokopolosnogo dostupa v setyakh podvizhnoy radiosvyazi na osnove standartov MOBILE WIMAX i LTE / S.V.Kanavin, A.S.Luk'yanov // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 79-82.
2. Glotova T.V. Osobennosti arkhitektury zashchishchennogo korporativnogo portala / T.V.Glotova, V.N.Kostrova / Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. S. 29-32.
3. Litvinskiy K.O. Model' podsistemy podderzhki prinyatiya resheniya v sisteme upravleniya tekhnogennymi riskami predpriyatiyakh toplivno-energeticheskogo kompleksa / K.O.Litvinskiy, V.A.Malyshev, Yu.V.Nikitenko // Ekonomika ustoychivogo razvitiya. 2015. No.1 (21). pp. 91-100.

4. Podsistema proektirovaniya zashchishchennykh besprovodnykh setey / I.Ya. L'vovich, A.P. Preobrazhenskiy, E. Ruzhitskiy, O.N. Choporov // Informatsiya i bezopasnost'. - 2015. - Vol. 18. - No.4. - pp. 556-559.
5. Malyshev V.A. Nechetkie algoritmy planirovaniya i modeli vzveshennogo prognoza raspredeleniya resursov sistemy upravleniya spetsial'nogo naznacheniya / V.A.Malyshev, V.S.Prokof'ev // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2008. No.3. pp. 049-052.
6. Belonozhkin V.I. Metodika formalizatsii pravila razgranicheniya dostupa k informatsionnym resursam / V.I. Belonozhkin, O.N. Choporov // Informatsiya i bezopasnost'. - 2007. - Vol. 10. - No.1. - pp. 169-172.
7. Mel'nikova T.V. Model' proektirovaniya besprovodnykh sistem svyazi s uchetom prirodnykh i promyshlennykh pomekh / T.V.Mel'nikova // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 61-63.
8. Sazonova S.A. Otsenka nadezhnosti raboty setevykh ob''ektov / S.A.Sazonova // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 40-42.
9. Lavlinskaya O.Yu. Tekhnologii oblachnykh vychisleniy i ikh primenenie v reshenii prakticheskikh zadach / O.Yu.Lavlinskaya, T.M.Yankis // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 33-36.
10. Chasovskoy A.A. Otsenka perspektiv vnedreniya oblachnykh vychisleniy na predpriyatiyakh i v gosudarstvennom sektore na primere FRG / A.A.Chasovskoy, E.V.Alferenko / Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 94-97.
11. Nechaeva A.I. Osobennosti funktsionirovaniya informatsionnykh baz na sklade / A.I.Nechaeva // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 64-66.
12. Ermolova V.V. Arkhitektura sistemy obmena soobshcheniy v nemarshrutiziruemoy seti / V.V.Ermolova, Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2010. No.7. pp. 79-81.
13. Malyshev V.A. Strukturnaya model' podsistemy resheniya zadach i prognozirovaniya v sistemakh avtomatizirovannogo proektirovaniya / V.A.Malyshev // Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2005. Vol. 1. No.11.
14. Voronov A.A. Obespechenie sistemy upravleniya riskami pri vozniknovenii ugroz informatsionnoy bezopasnosti / A.A.Voronov, I.Ya.L'vovich, Yu.P.Preobrazhenskiy, V.A.Voronov // Informatsiya i bezopasnost'. 2006. Vol. 9. No.2. pp. 8-11.

15. Panevin R.Yu. Realizatsiya translyatora imitatsionno-semanticheskogo modelirovaniya / R.Yu.Panevin, Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2009. No.5. pp. 057-060.
16. Choporov O.N. Ratsionalizatsiya upravleniya regional'nymi sistemami na osnove ispol'zovaniya metodov sistemnogo analiza, informatsionnykh i GIS-tekhnologiy / O.N.Choporov, N.A.Gladskikh, S.S.Pronin, M.I.Chudinov, S.N.Semenov, K.L.Matyushevskiy // Prikladnye informatsionnye aspekty meditsiny. 2007. Vol. 10. No.2. pp. 15-19.
17. Formirovanie trebovaniy k sisteme informatsionnoy bezopasnosti v proektnykh organizatsiyakh neftegazovogo kompleksa / B.V. Vasil'ev, N.I. Barannikov, A.V. Zaryaev, V.S. Zarubin, O.N. Choporov // Informatsiya i bezopasnost'. - 2015. - Vol. 18. - No.4. - pp. 508-511.
18. Zyablov E.L. Razrabotka lingvisticheskikh sredstv intellektual'noy podderzhki na osnove imitatsionno-semanticheskogo modelirovaniya / E.L.Zyablov, Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2009. No.5. pp. 024-026.
19. Ivanov M.S. Razrabotka algoritma otsecheniya derev'ev / M.S.Ivanov, Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2008. No.3. pp. 031-032.
20. Preobrazhenskiy Yu.P. Adaptivnye algoritmy dlya beskonechnykh stokhasticheskikh igr / Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2010. No.7. pp. 46-47.
21. Baranov A.V. Problemy funktsionirovaniya mesh-setey / A.V.Baranov // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2012. No.9. pp. 49-50.
22. Preobrazhenskiy Yu.P. Otsenka effektivnosti primeneniya sistemy intellektual'noy podderzhki prinyatiya resheniy / Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2009. No.5. pp. 116-119.
23. Panevin R.Yu. Strukturnye i funktsinal'nye trebovaniya k programmnomu kompleksu predstavleniya znaniy / R.Yu.Panevin, Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2008. No.3. pp. 061-064.
24. Primenenie kaskadnykh modeley pri otsenke riskov rasprostraneniya vredonosnoy informatsii v sotsial'nykh setyakh / D.O. Karpeev, D.A. Savinov, A.V. Zaryaev, V.S. Zarubin, O.N. Choporov // Informatsiya i bezopasnost'. - 2015. - Vol. 18. - No.4. - pp. 512-515.
25. Deshina A.E. Innovatsionnye tekhnologii regulirovaniya riskov mul'tiservernykh sistem v usloviyakh atak kompleksnogo tipa / A.V. Deshina, O.N. Choporov, K.A. Razinkin // Informatsiya i bezopasnost'. - 2013. - Vol. 16. - No.3. - pp. 371-374.

26. Simonov K.V. Ob"ekty i skhema vozdeystviy terroristicheskogo kharaktera na internet-prostranstvo / K.V. Simonov, O.N. Choporov // Informatsiya i bezopasnost'. - 2011. - Vol. 14. - No.4. - pp. 623-624.
27. Choporov O.N. Podkhod k otsenivaniyu opasnosti ugroz kak mera sovpadeniya impul'snykh potokov i veroyatnosti sovpadeniy / O.N. Choporov, S.V. Lykov // Informatsiya i bezopasnost'. - 2011. - Vol. 14. - No.4. - pp. 629-630.