КОРЧИГАНОВА А.О., МАКАРОВ Г.В., БАЖАНОВА С.В.

ЗАЩИТА ИНФОРМАЦИИ В АИС

Аннотация. В данной статье рассмотрены проблемы защиты информации в АИС. Изучена ситуация на современном рынке программных продуктов, обеспечивающих защиту информации, предназначенной для персонального использования. Проведен комплексный анализ средств защиты информации на примере организации ОАО «Ростелеком» в Республике Мордовия. На основе проведенного исследования вынесены предложения по установке в организации средств защиты информации для частных и корпоративных клиентов.

Ключевые слова: защита информации, автоматизированная информационная система, угроза безопасности, электронно-цифровая подпись, оказание услуг, пользователи

KORCHIGANOVAA. O., MAKAROVG. V., BAZHANOVA S.V.

INFORMATION SECURITY IN THE AUTOMATED INFORMATION SYSTEM (AIS)

Abstract. The paper considers the problem of information security in AIS. The current software market for information security intended for personal use has been studied. A comprehensive analysis of information security facilities used by JSC Rostelecom (Mordovia Republic branch) has been carried out. As a result the company is advised to install information security tools for private and corporate clients.

Keywords: data protection, automated information system, security risk, digital signature, providing services, users.

Сегодня автоматизированные информационные системы (АИС) – это основа обеспечения бизнес-процессов в частных и государственных организациях. Пользование АИС для хранения, обработки и передачи информации проблемно, так как это связано с их защитой. Сейчас в России и в Европе растет количество информационных атак, которые приводят к большим финансовым и материальным потерям.

Угроза безопасности – это действие или событие, приводящее к разрушению, искажению или не правовому доступу к информационным ресурсам вместе с хранимой, передаваемой и обрабатываемой информацией, включая программные и аппаратные технологии.

Особая опасность в наше время – это компьютерные вирусы, потому что уникальных и проверенных средств защиты против них не существует. Остальные пути несанкционированного доступа надежно блокируются при правильной разработке и реализации на практике систем обеспечения безопасности.

При разработке АИС встает вопрос о решении проблем, связанных с безопасностью информации, которая является коммерческой тайной, включая безопасность информационных систем.

Особый интерес представляет внедрение и использование в организации новых средств защиты информации. Рассмотрим средства защиты информации на примере организации ОАО «Ростелеком» в Республике Мордовия. В организации имеются лицензии на оказание услуг местной, внутризоновой телефонной связи, документальной связи, радиовещания в одиннадцати регионах Приволжского федерального округа. В последнее время ее внимание сфокусировано на полном комплексе телекоммуникационных услуг и сервисов для своих пользователей в качестве универсального оператора. В основном сейчас все силы ОАО «Ростелекома» сосредоточены на внедрении своих конкурентных новинок в целях предоставления полного спектра услуг и удерживания своих постоянных клиентов, а также на привлечении новых пользователей во всех отраслях связи, чтобы предлагать качественное и комплексное обслуживание. Сейчас в связи с высокой конкуренцией и быстро изменяющимся рынком организация ищет способы совершенствования своих услуг наряду с предложениями конкурентов. Услуги обеспечения безопасности сетей передачи данных востребованы на телекоммуникационном рынке. Развитие технологий электронного документооборота, каналов удаленного обслуживания (таких как, например, Интернет-банкинг – технология отдаленного обслуживания банка, которая может предоставляться абоненту в любое удобное время и с разных компьютеров, имеющих доступ в Интернет). Постоянная потребность корпоративного сегмента в защите передаваемых по сетям организации данных становится предпосылкой для создания целого пакета услуг по защите информации. ОАО «Ростелеком» высылает абонентам, которые пострадали от вирусов, оперативные уведомления, оказывает онлайновую помощь и превентивную поддержку, что повышает уровень доверия у клиентов компании. В то же время организация осуществляет защиту своих сетей от защищенных и незащищенных компьютеров клиентов. Эта защита, предоставляемая компанией, позволяет снизить заражения в своей сети и получает конкурентное лидерство за счет расширения услуг, предоставляемых организацией, и дает новые источники доходов.

С 2010 года организация ОАО «Ростелеком» приняла решение о создании Центра компетенций, предоставляя услуги защиты информации. На его базе разрабатывается ряд проектов, направленных на организацию предоставления услуг по информационной безопасности. Это аудит и консалтинг в информационной безопасности, поставка программного обеспечения (антиспам, антивирус, резервное копирование, очистка зараженного трафика, межсетевые экраны), создание защиты информации и организация

VPN-сетей и много другое. VPN – сети, обеспечивающие защищенность данных при передаче их по незащищенным сетям.

На этапе утверждения программы финансирования и дальнейшего внедрения находится проект создания Удостоверяющего центра с целью предоставления услуг по изготовлению и выдаче ключей электронной цифровой подписи (ЭЦП).

Область применения ЭЦП довольно обширна. Это и сдача отчетных документов в электронном виде и площадки электронных торгов, и корпоративный электронный документооборот. ЭЦП востребована также для функционирования системы предоставления государственных услуг в рамках реализации Федеральной целевой программы (ФЦП) «Электронная Россия 2002-2010».

Применение электронной цифровой подписи позволяет экономить время на оформление и сдачу отчетности в государственные органы, на оформление сделки и обмен документацией, гарантирует надежность документации и минимизирует риск финансовых неудач.

В компании ОАО «Ростелеком» в корпоративных системах пользуются контентной фильтрацией для Интернета и почтового трафика. Во второй половине 2009 года отдел информационной безопасности провел тестирование шести различных продуктов, выбрал компанию BlueCoat.

ОАО «Ростелеком» заключил государственный контракт с департаментом образования по созданию виртуальной сети для общеобразовательных учреждений. Была взята задача обеспечения фильтрации «вредоносного» контента. С этой целью была установлена система активной фильтрации «BlueCoat» – мощное решение, гарантирующее пользователям безопасный доступ к Интернет-ресурсам и значительно облегчающее осуществление контроля безопасности администраторами. Это средство эффективно обеспечивает защиту от разнообразных злоупотреблений в Интернете и сетевых угроз, в том числе программ-шпионов, нежелательного контента. Результаты тестовой эксплуатации показали, что данная система успешно справляется с функциями обеспечения защиты от «вредоносного» контента и вирусов.

В целях обеспечения защиты почтового сервиса связи Интернет-пользователей от нежелательной корреспонденции (спама) с 2008 года специалистами управления безопасности введена в Республике Мордовия в эксплуатацию система «Самооборона». Её введение позволило снизить паразитный почтовый трафик в почтовых ящиках пользователей более чем на 80%. На данный момент до 82% от общего объема передаваемой информации составляет спам, который успешно блокируется системой «Самооборона».

С 2010 года ОАО «Ростелекомом» оказывает такую абонентскую услугу, как автоматическая подписка на антивирус Касперского. Пользователи с сайта могут управлять услугами, получать коды активации на антивирусный модуль. Клиенты устанавливают на своем компьютере антивирус, защищающий их компьютер от неправомерного воздействия.

Также ОАО «Ростелеком» фильтрует трафик в компании до его поступления пользователям. Осуществляет фильтрацию и блокировку ненужного контента на уровне провайдера, а только потом клиент получает «чистый» Интернет без вирусов, «шпионского» программного обеспечения и опасной информации. Эта услуга экономит время и обеспечивает безопасность информации. Техническая сторона услуги выглядит таким образом, что компания приобретает специальное оборудование «фильтрующие модули», устанавливает их на сети передачи данных. Для этого оборудования создается политика фильтрации (в рамках возможности оборудования), которая потом будет в основе тех тарифов, которые оператор связи предложит своим абонентам. В рамках политики фильтрации можно определить категории сайтов, которые являются вредоносными, и система блокирует их поступление. Все данные и информация должны проверяться на вредоносное и опасное программное обеспечение.

Когда устанавливаются различные системы безопасности, снижается вероятность нежелательных событий. Наибольший эффект дает «эшелонированная» защита. На примере организации ОАО «Ростелеком» она выглядит следующим образом: первый рубеж – очистка трафика на уровне организации, второй – работающий антивирус/межсетевой экран на компьютере пользователя. Именно на «втором рубеже» компьютер пользователя защищен от вируса на флешке.

В рамках рассмотрения услуги для абонентов первой платформой стал ПАКeSafe для ISPот компании Aladdin. Во время пилотного тестирования абоненты могли подключиться к услуге «Чистый Интернет». Система Aladdine-Safe фильтрует содержимое Интернета и почты практически без задержки, что удобно для пользователя, так как это не отнимает время от работы. Она идентифицирует и блокирует вредоносные коды, спам, контролирует сетевой трафик, выявляет вирусные атаки по сигнатурам.

Корпоративная система антивирусной защиты в ОАО «Ростелеком» выглядит таким образом: на каждом компьютере стоит антивирусный модуль, и дополнительно Интернет проверяют на пограничных серверах, расположенных в демилитаризованных зонах, используется антивирусное программное обеспечение на компьютере и пограничном сервере разных производителей.

Подводим итог вышесказанному: сегодня на рынке представлено множество продуктов и решений по обеспечению антивирусной защиты и фильтрации спама,

предназначенных для персонального использования. Но проблемы распространения вирусов и спама пока остаются главными проблемами безопасности, сказывающиеся на Интернет-пользователях. В случае отсутствия персонального антивирусного ПО или его нерегулярного обновления компьютеры абонентов являются уязвимыми к угрозам распространения вредоносного кода. В результате компьютеры, зараженные вредоносными ПО, контролируются злоумышленниками и становятся инструментами рассылки спама. При условии развития системы фильтрации до масштабов Межрегиональных компаний связи (МРК) возможно расширение перечня услуг, оказываемых ОАО «Ростелекомом», и предоставления на базе системы услуг фильтрации веб-трафика частным и корпоративным клиентам. Для частных клиентов будут интересны услуги по организации родительского контроля при посещении ресурсов сети Интернет детьми, для корпоративных клиентов – услуги по ограничению доступности Интернет-ресурсов сотрудникам организаций и предприятий с целью повышения эффективности использования рабочего времени, ограничения утечки конфиденциальной информации и распространения вредоносных программ.

Существует ряд продуктов различных производителей, которые предназначены именно для операторов связи, таких как ОАО «Ростелеком», предоставляющих своим абонентам услуги по обеспечению безопасности.

Мы предлагаем установить в организации средства защиты информации для частных лиц:

- услуга «Родительский контроль» – настраиваемое ограничение доступа к определенным категориям web–сайтов в Интернете.

- услуга «Безопасный web–серфинг» – антивирусная фильтрация web–трафика абонентов в комплексе с блокированием попыток доступа к вредоносным и мошенническим сайтам в сети Интернет.

- выявление зараженных вредоносным кодом компьютеров в сети и уведомление абонентов о возникшей у них проблеме.

Такие услуги можно предоставлять абонентам на основе программных продуктов большинства поставщиков антивирусного программного обеспечения (TrendMicro, Лаборатория Касперского и др.), а также на платформе Cisco Service Control Engine (CiscoSCE) илие Safe компании Aladdin.

Услуги на основе данных решений целиком реализуются в сетевой инфраструктуре организации. Для включения защиты абонентам не требуется устанавливать специальные программные обеспечения на своих компьютерах. Включение и настройку параметров

работы услуг абоненты могут выполнять самостоятельно из «Личного кабинета» на сайте ОАО «Ростелеком».

В результате внедрения сетевых услуг безопасности организация ОАО «Ростелеком» получит следующие преимущества:

- конкурентное преимущество за счет расширения спектра предоставляемых услуг.
- увеличение выручки за счет продажи новой дополнительной услуги.
- повышение лояльности и уровня удовлетворенности абонентов.
- повышение репутации и значимости своего бизнеса.

Предлагая родителям надежную возможность оградить детей от влияния негативного контента в Интернете, компания вносит свой вклад в социальную защиту общества.

Для оказания услуг по безопасности юридическим лицам можно использовать как решения, предназначенные для физических лиц, так и более широкий спектр дополнительных услуг: услуги удостоверяющих центров, а также обеспечение безопасности работников независимо от места их нахождения, например, предлагаемые компаниями ScanSafe и Cisco.

Оказывая услуги по безопасности, организация будет получать новые рынки и рост доходов. Конечные потребители получат высокий уровень защиты своих информационных активов с фиксированной и заранее прогнозированной стоимостью, гораздо ниже той, которую пришлось бы заплатить за создание собственной инфраструктуры безопасности.

ЛИТЕРАТУРА

1. Степанов Е. А., Корнеев И. К. Информационная безопасность и защита информации. - М.: ИНФРА-М, 2003.
2. Ясенев В.Н. Информационная безопасность в экономических системах: учебное пособие. – М.: ННГУ, 2006.
3. Охрименко С. А., Черней Г. А. Угрозы безопасности автоматизированным информационным системам – [Электронный ресурс]. – Режим доступа: http://www.ase.md/~osa/publ/ru/pubru05.html /
4. Защита информации. 2011– [Электронный ресурс]. - Режим доступа: www.svyazinvest.ru