К.Э. Тожа
Россия, г. Москва,
Московская академия рынка труда и информационных технологий

СИСТЕМНЫЙ АНАЛИЗ И ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ЭНЕРГОСБЫТОВЫХ КОМПАНИЙ

Создание систем защиты информационной инфраструктуры энергосбытовых компаний необходимо для их нормального функционирования. В работе проведен системный анализ, обоснование и описание проекта, который был успешно реализован в ОАО "Мосэнергосбыт".

Проанализируем особенности функционирования энергосбытовых компаний на примере ОАО "Мосэнергосбыт", которое было создано 1 апреля 2005 года в результате выделения из компании "Мосэнерго" существовавшего с 1931 года филиала, ответственного за непосредственную работу с потребителями в столичном регионе. Теперь "Мосэнергосбыт" – самостоятельное юридическое лицо. На сегодняшний день это крупнейшая энергосбытовая компания в России (реализует 8% вырабатываемой в России электрической энергии, что составляет 65,3 млрд кВт·ч в год). В ее состав входят 10 городских и 13 межрайонных отделений. В число главных направлений деятельности "Мосэнергосбыт" входят:

- покупка электроэнергии на оптовом и розничных рынках электрической энергии (мощности);
- реализация (продажа) электроэнергии на оптовом и розничных рынках электрической энергии (мощности) потребителям (в том числе гражданам);
- оказание услуг третьим лицам, в том числе по сбору платежей за отпускаемые товары и оказываемые услуги;
- диагностика, эксплуатация, ремонт, замена и проверка средств измерений и учета электрической и тепловой энергии;
- оказание услуг по организации коммерческого учета;
- предоставление коммунальных услуг населению;
- разработка, организация и проведение энергосберегающих мероприятий;
- выполнение функций гарантирующего поставщика на основании решений уполномоченных органов;
- инвестиционная деятельность;
- оказание консалтинговых и иных услуг, связанных с реализацией электрической энергии юридическим и физическим лицам.

Безусловно, главнейшей задачей ОАО "Мосэнергосбыт" на настоящий момент следует признать формирование эффективной, отвечающей требованиям времени системы сбыта электроэнергии. Решение этой задачи невозможно без создания и грамотной эксплуатации защищенной информационной инфраструктуры энергосбытовой компании. Отметим, что в этой сфере "Мосэнергосбыт" во многом выступает в качестве первопроходца, что обуславливает научную сложность, недостаточную проработанность и актуальность темы данной работы. "Мосэнерго" было одной из первых региональных энергокомпаний, прошедших процесс реформирования, и у начавшего свою работу в качестве самостоятельной сбытовой структуры "Мосэнергосбыта" не было готовых рецептов организации эффективной политики работы с энергопотребителями в новых конкурентных условиях. В то же время в распоряжении компании – богатый опыт и традиции, накопленные в период ее

функционирования в качестве филиала "Мосэнерго". Они обуславливают наличие у "Мосэнергосбыта" уже налаженных крепких связей с поставщиками электроэнергии, знание особенностей каждой категории потребителей. Работа со столь широким спектром категорий потребителей накладывает на "Мосэнергосбыт" высочайшую степень социальной ответственности. Эта ответственность проявляется фактически во всем комплексе деятельности компании и включает такие меры, как внимательное отношение к потребностям и специфике каждого клиента, разработку удобных систем оплаты энергии, открытие оборудованных по последнему слову техники центров обслуживания потребителей.

Автоматизация всех производственных процессов, обеспечение их информационной безопасности и улучшение качества обслуживания клиентов – приоритетные задачи деятельности любой энергосбытовой компании.

В 2006 году ОАО "Мосэнергосбыт" впервые разработало собственную инвестиционную программу на 2007–2009 гг., которая оценивается в 5,5 млрд рублей. Все средства должны пойти на улучшение обслуживания клиентов и создание эффективной и безопасной системы сбыта электроэнергии. Намечено сделать качественный рывок в сторону современных стандартов обслуживания клиентов, провести совершенствование биллинговой системы и внедрение автоматизированных систем контроля и учета электроэнергии.

Миссия энергосбытовой компании состоит в оказании потребителям электрической энергии полного комплекса услуг, связанного с энергоснабжением. Целью деятельности является удовлетворение потребностей клиентов в электрической энергии в необходимых объемах. Для достижения данной цели решаются следующие ключевые задачи:

1. Введение новых стандартов обслуживания потребителей электрической энергии и повышение качества сервиса.
2. Контроль и управление энергопотреблением в регионе.
3. Сохранение и расширение клиентской базы.
4. Разработка и внедрение новых технологий энергосбытовой деятельности, автоматизация бизнес-процессов.
5. Оптимизация затрат и эффективное управление деятельностью.

Для системного анализа необходимо учитывать, что потребителями ОАО "Мосэнергосбыт" являются свыше 96 тыс. коммерческих организаций в Москве и более 40 тыс. предприятий Московской области. Компания обслуживает около 5 млн бытовых абонентов. Объемы сбыта электроэнергии компанией составляют 58,7 млрд кВт·ч в год. В структуре потребителей ОАО "Мосэнергосбыт" примерно 42,5% составляют промышленные и приравненные к ним потребители, 35,2% – непромышленные абоненты, 11,8% – энергоснабжающие организации (обычно это местные муниципальные органы, которые затем перепродают электроэнергию местным потребителям), 5,0% – электрифицированный железнодорожный транспорт, 4,1% – электрифицированный городской транспорт, 1,3% – сельскохозяйственные потребители. Информационная инфраструктура создается с учетом существующей структуры компании: партнером ОАО "Мосэнергосбыт" является Центр обслуживания продаж энергии (ЗАО "ЦОПэнерго"), специалисты которого осуществляют расчеты не только с населением, но и с непромышленными предприятиями, а также занимаются техническим обслуживанием и установкой новых, более современных приборов учета электрической энергии. В состав ОАО "Мосэнергосбыт" входят:

- 10 городских отделений;
- 13 межрайонных отделений;

- отделение крупных потребителей;
- отделение по обслуживанию режимных предприятий;
- цех по ремонту приборов учета;
- подразделения по эксплуатации приборов и систем учета;
- подразделения функциональных блоков: правового обеспечения, по экономике и финансам, по информационным технологиям, по корпоративным вопросам.

Созданную информационную инфраструктуру энергосбытовой компании необходимо защищать, а важнейшим этапом создания систем технической защиты является разработка технического проекта. В техническом проекте системы защиты, например ОАО "Мосэнергосбыт", должны быть приведены программно-технические решения, используемые при создании системы защиты. После разработки и утверждения технического проекта структурные программно-технические решения, версии программных продуктов и модели технических средств должны уточняться на этапе реализации системы защиты.

Проведенный анализ позволил выявить следующие основные ИТ-услуги ОАО “Мосэнергосбыт” (в 2006 г.): доступ локальной вычислительной сети организации к корпоративной сети по выделенным скоростным цифровым каналам связи; доступ отдельных пользователей к корпоративной сети по каналам телефонным связи тональной частоты, корпоративным и МГТС (dial-up); защищенный доступ локальной вычислительной сети организации к корпоративной сети через публичные сети (Internet) по технологии виртуальных частных сетей (VPN); защищенный доступ отдельных пользователей к корпоративной сети через публичные сети (Internet) посредством VPN-клиентов; размещение и обслуживание почтовых ящиков пользователей организаций на серверах корпоративной почтовой системы MS Exchange с выделением E-mail адреса из почтового домена mosenergosbyt.ru; защищенный доступ пользователя из Internet к своему корпоративному почтовому ящику; система поддержки коллективной работы пользователей на базе клиента MS Outlook и серверов MS Exchange; маршрутизация почтовым шлюзом входящих/исходящих почтовых сообщений E-mail для внутреннего почтового сервера организации; размещение и ведение зон DNS (primary, secondary) организаций на DNS-серверах (внутренних/внешних); антивирусная проверка/защита входящих и исходящих почтовых сообщений; антивирусный мониторинг и лечение рабочих станций пользователей организаций; предоставление авторизованного доступа в Интернет через корпоративный прокси-сервер по протоколам http, https, ftp (с проведением учета по файлам протоколов); администрирование и поддержка локальных вычислительных сетей организаций; администрирование и техническое обслуживание баз данных Oracle на территории организаций; размещение и техническое обслуживание данных/приложений организаций на серверах баз данных Oracle; размещение и техническое обслуживание данных/приложений организаций на серверах баз данных MS SQL; размещение данных пользователей в централизованном файловом хранилище и организация совместной работы с файловыми ресурсами и многие другие.

Особо выделим услуги обеспечения безопасности: предоставление услуг в области шифрования информации; обслуживание шифровальных средств; распространение шифровальных средств, а также деятельность по технической защите конфиденциальной информации с предоставлением услуг сторонним организациям.

Кроме того, ИТ-службы энергосбытовых компаний занимаются разработкой прикладного программно-математического обеспечения; выполняют оптимизацию

баз данных и обеспечивают защиту информации на промышленных серверах МосЭнергосбыта; выполняют авторское сопровождение баз данных Мосэнергосбыта; обеспечивают целостность данных на физическом и логическом уровнях; осуществляют модернизацию, доработку и усовершенствование существующего прикладного программного обеспечения по дополнительным требованиям Мосэнергосбыта; ведут разработку программной и эксплуатационной документации; проводят отладку и тестирование модифицированного программного обеспечения и проводят обучение конечных пользователей.

Выделим основные информационные услуги, которые предоставляют энергосбытовые компании: физическое размещение данных и их описаний, поиск данных; защита данных от некорректных обновлений и несанкционированного доступа; обслуживание одновременных запросов к данным от нескольких пользователей (прикладных программ); анализ предметной области; проектирование и разработка баз данных; тестирование баз данных; сопровождение баз данных; конвертация данных в ORACLE; разработка и сопровождение техпроцесса и программных средств синхронизации баз данных, анализ процесса синхронизации; обеспечение мониторинга состояния БД, контроль целостности информации и структуры БД; разработка и сопровождение прикладного программного обеспечения (автоматизированных рабочих мест) для центрального офиса, городских и межрайонных отделений; методическая и практическая помощь специалистам городских и межрайонных отделений по информационным системам в вопросах сопровождения программного обеспечения.

Для обоснованного формирования требований к системе защиты данных каналов связи в качестве исходных данных обязательно используются: схема структурных сетей связи энергосбытовой компании; таблица распределения IP-адресов в ее сети передачи данных и описание защищаемых информационных потоков компании. Например, сеть передачи данных ОАО "Мосэнергосбыт" представляет собой территориально распределенную вычислительную систему, построенную по топологии "звезда". В качестве центра звезды выступает центральный ведомственный узел, в качестве оконечных пунктов – территориальные ведомственные узлы (ГО и МРО). Таким образом, весь трафик между территориальными ведомственными узлами проходит через центральный узел. В качестве каналов передачи данных между узлами используются выделенные линии. В сети применяется оборудование Cisco Systems, Inc. и стек протоколов TCP/IP. По каналам связи сети передачи данных передается конфиденциальная информация. Администрирование сетевой инфраструктуры осуществляется удаленно из центрального ведомственного узла. Проанализируем техническое описание системы защиты данных каналов связи. Основные требования к системе защиты формулируются так. Система защиты каналов связи должна обеспечивать: межсетевое экранирование узлов (сегментов сети) ЗВКВС; организацию виртуальной частной сети; защиту от НСД к передаваемой по каналам связи информации (т.е. конфиденциальность и целостность информации); защиту от внедрения ложной информации в канал связи; централизованное управление средствами защиты каналов связи ЗВКВС.

Рассмотрим такой случай, когда средства защиты информации, используемые для организации системы защиты каналов связи, должны соответствовать уровню требований к защищенности автоматизированных систем, предъявляемых ФСТЭК России, по классу 1Г. Для выполнения данных требований в качестве проектного решения в энергосбытовых компаниях целесообразно применять программно-

аппаратный комплекс "ФПСУ-IP". Для обоснования данной рекомендации приведем краткое описание комплекса ФПСУ-IP и проанализируем его.

Итак, программно-аппаратный комплекс (ПАК) ФПСУ-IP является средством комплексной защиты информационных и телекоммуникационных систем от несанкционированного доступа (НСД).

Комплекс предназначен для организации управления доступом к информационным ресурсам сетей передачи данных и обеспечения целостности, достоверности и конфиденциальности информации, передаваемой по каналам связи. ПАК разработан для применения в вычислительных сетях, использующих стек протоколов TCP/IP и среду передачи данных Ethernet. Основным элементом комплекса ФПСУ-IP является специализированный программно-аппаратный межсетевой экран (МЭ), совмещающий в себе функции сетевого фильтра, пакетного коммутатора и средства организации виртуальных частных сетей (VPN) поверх локальных и глобальных вычислительных сетей. Межсетевой экран используется для разграничения доступа абонентов сети друг к другу и/или для выделения в сети участков с повышенной степенью защиты от НСД.

Безопасность передачи информации при взаимодействии абонентов территориально-распределенных сетей повышается за счет организации межсетевых туннелей (VPN) между МЭ. В состав ПАК входит средство криптографической защиты информации (СКЗИ) "Туннель/Клиент", что позволяет осуществлять шифрование передаваемой информации в соответствии с ГОСТ 28147-89. ПАК "ФПСУ-IP" производится ООО "АМИКОН" и обладает всеми необходимыми сертификатами.

В состав программно-аппаратного комплекса входят следующие компоненты: межсетевой экран "ФПСУ-IP"; аппаратное средство для автозапуска RS-Key; программный комплекс "Центр выработки ключей" (ЦВК); подсистема удаленного администрирования; программный комплекс "Автоматизированное рабочее место удаленного администрирования" (АРМ УА) и модуль-агент удаленного администрирования. Анализируемый комплекс предназначен для применения в вычислительных сетях, использующих среду передачи данных Ethernet и стек протоколов TCP/IP.

Система защиты данных канала связи. Сетевой трафик между защищаемыми сегментами сети на маршрутизаторах ведомственных узлов по ряду критериев (IP-адреса отправителя и получателя) перенаправляется на межсетевые экраны "ФПСУ-IP".

На МЭ трафик шифруется, инкапсулируется в IP-пакеты с номером протокола 53 и в таком виде передается по внешним каналам передачи данных. На приемной стороне трафик расшифровывается комплексом "ФПСУ-IP" и передается в ЛВС. Таким образом, защищаемый трафик не передается в открытом виде по внешним каналам связи (рис. 1).

Межсетевые экраны. В анализируемом проекте была выбрана схема подключения МЭ к ЛВС ведомственных узлов с использованием одного порта "ФПСУ-IP". При этом перенаправление защищаемого трафика на межсетевые экраны осуществляется средствами маршрутизаторов Cisco. Такая схема, в отличие от подключения "в разрыв", позволяет:

- осуществлять более гибкий контроль над информационными потоками на уровне маршрутизаторов;
- легко изменять список защищаемых подсетей (сегментов) сети;
- оперативно и дистанционно отключать конкретный МЭ “ФПСУ-IP” при возникновении проблем в его функционировании.

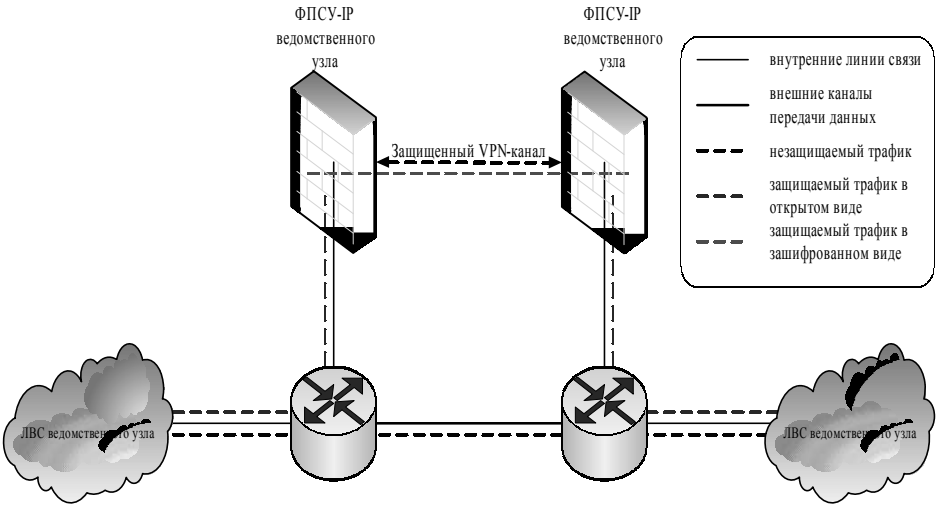

Рис. 1. Схема прохождения трафика

Отметим, что разработанная схема подключения с использованием одного порта требует внесения минимальных изменений в конфигурацию смежных с МЭ маршрутизаторов. Межсетевой экран "ФПСУ-IP" центрального ведомственного узла устанавливается в телекоммуникационный шкаф в серверном помещении. Для подключения МЭ к ЛВС центрального ведомственного узла межсетевой экран соединяется коммутационным шнуром RJ45-RJ45 со свободным портом маршрутизатора Cisco.

Межсетевой экран территориального ведомственного узла устанавливается в телекоммуникационный шкаф в серверном помещении территориального узла.

Для подключения МЭ к ЛВС территориального ведомственного узла межсетевой экран соединяется коммутационным шнуром RJ45-RJ45 со свободным портом коммутатора ЛВС. При этом идентификация и аутентификация локальных администраторов МЭ осуществляется при помощи идентификаторов TouchMemory. Для соблюдения принципа минимальных привилегий рекомендуется осуществлять администрирование удаленно и централизованно (при этом идентификаторы TouchMemory администраторам территориальных узлов не выдаются), а для перезапуска МЭ использовать устройство RS-Key, не предоставляющее административного доступа.

Для повышения надежности и отказоустойчивости системы защиты межсетевые экраны "ФПСУ-IP" должны быть подключены к источнику бесперебойного питания. Горячее резервирование межсетевых экранов данным проектом, к сожалению, не предусмотрено. Это обусловлено финансовыми ограничениями. Для усиления степени защиты рекомендуется ввести дополнительные правила межсетевого экранирования на маршрутизаторах Cisco, запрещающие прохождение защищаемого трафика в незашифрованном виде.

АРМ удаленного администратора устанавливается в здании центрального ведомственного узла. Между АРМ УА и МЭ "ФПСУ-IP" установлены двусторонние доверительные отношения (т.е. произведена взаимная аутентификация), что позволяет осуществлять удаленное управление межсетевыми экранами без дополнительной аутентификации.

Контроль доступа к АРМ осуществляется организационными мерами и встроенной системой парольной защиты ПО удаленного администрирования.

Вывод. В данной работе проведен системный анализ особенностей функционирования и проектирования систем защиты информационных инфраструктур энергосбытовых компаний на примере ОАО "Мосэнергосбыт". Надежное обеспечение безопасности информационной инфраструктуры энергосбытовых компаний повышает их конкурентоспособность.

Д.П. Рублёв, А.В. Чумаченко, О.Б. Макаревич, В.М. Фёдоров
Россия, г. Таганрог, Технологический институт ЮФУ
г. Нальчик, НИПРУ КБНЦ РАН

ИДЕНТИФИКАЦИЯ ЦИФРОВЫХ МИКРОФОНОВ ПО НЕИДЕАЛЬНОСТЯМ ТРАКТА ЗАПИСИ

За последние годы произошло массовое вытеснение и замена аналоговой техники звуко-, видеозаписи, а также фототехники в потребительском сегменте на цифровую. Наибольшее распространение получили цифровые фотокамеры и диктофоны. Помимо очевидных проблем, связанных с потенциальной возможностью утечки информации посредством данных устройств, зачастую имеющих стандартные выходы последовательной шины USB, и возможность записи с неё цифровых данных произвольного формата на внутренний носитель информации (электронно-перепрограммируемую постоянную память), актуальной является и задача подтверждения произведения имеющейся цифровой аудио-, видеозаписи, либо фиксации изображения на конкретном экземпляре устройства, определения по записи его модели и фирмы-производителя. Аналогией в данном случае является идентификация пишущей машинки по странице отпечатанной на ней на основе имеющегося слепка шрифта, отражающего уникальные особенности литер. В настоящее время известны несколько работ в области идентификации цифровых фотокамер [1,2] на основе отличительных признаков аппаратной и программной части. Цифровой образ, полученный при помощи устройства записи, несёт в себе набор особенностей, сформированных различными узлами тракта записи, что позволяет однозначно идентифицировать принадлежность одному из классов устройств. Помимо успешной идентификации устройства по имеющемуся цифровому образу, данные признаки могут быть использованы для обнаружения факта монтажа. На основе рассмотренных в работах по идентификации признаков можно выделить следующие классы признаков.

1. Признаки аппаратной части — это устойчивые во времени отклонения характеристик сенсора и последующих блоков обработки, включая АЦП, как отдельного устройства. В общем случае признаки сенсора позволяют идентифицировать конкретный экземпляр устройства. В частности для цифровых камер таковыми являются дефекты и отклонения в пределах допусков отдельных светочувствительных элементов, дефекты элементов “обвязки” светочувствительной матрицы в целом и т.д. [1,2].

2. Признаки алгоритмов постобработки. В цифровых камерах алгоритмом постобработки, оказывающим наибольшее алгоритмами постобработки, оказывающими наибольшее влияние на полученное, являются алгоритмы подавления пиксельных дефектов, алгоритмы восстановления изображения из мозаичной структуры сенсора, повышения контурной резкости и шумоподавления.

Не менее актуальной в настоящее время является задача автоматизированной и автоматической идентификации устройств аудиозаписи по сформированному ими цифровому образу. В открытой печати публикации по данной тематике ограничены. Для цифровых микрофонов первой группой признаков являются отклонения от сред-