ГАЗЕТА ДЛЯ КОРПОРАТИВНЫХ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И РЕШЕНИЙ

18+

PCWEEK RUSSIAN EDITION

СК ПРЕСС

№ 7 (906) • 19 АПРЕЛЯ • 2016 • МОСКВА

http://www.pcweek.ru

Импортозамещение на таможне

НИКОЛАЙ НОСОВ

Средства массовой информации еще не успели как следует прокомментировать слова Владимира Путина на совещании 30 марта с членами правительства в Ново-Огарево о необходимости перехода госкомпаний на российское ПО уже в этом году, как Федеральная таможенная служба приступила к выполнению задания президента страны. Конечно, то, что конференция ФТС "О проблемах импортозамещения в таможенных органах и новых разработках в сфере информационно-коммуникационных технологий" состоялась на следующий день, — совпадение, но отнюдь не случайное. Ведомство понимало, куда "дует ветер" и куда им нужно двигаться и без дополнительных указаний сверху. И неожиданностью для собравшихся были разве что конкретные указанные сроки перехода.

Дмитрий Данилин

Общесистемное ПО

Впрочем, "ветер дует" уже давно. Еще год назад на конференции "Таможенные информационные технологии: преимущества и перспективы" мы интересовались у представителей ведомства об импортозамещении в общесистемном ПО. Ответ был: "Свободное ПО требует больших усилий по сопровождению. Мы не имеем возможности его использовать. Нам нужны надежные решения и хорошая поддержка. Этим требованиям отвечает западное проприетарное ПО".

Фактическая ситуация изменилась мало. Согласно приведенным на конференции цифрам — импортозависимость оборудования и технологий, применяемых в общесистемном ПО, в таможенных органах составляет 99%.

Но отношение к этому изменилось. Заявлено, что ФТС будет тестировать и выбирать российские разработки, причем указывались такие системы, как Astra Linux, "Альт Линукс", ОС МСВС 5.0, ОС "Заря" и "Роса".

На повторно поставленный нами вопрос начальник Главного управления информационных технологий ФТС России Дмитрий Данилин ответил, что служба готова использовать общесистемное ПО на базе Linux, что специалистов стало больше. А если не будет хватать — их быстро научат в Российской таможенной академии, где уже давно готовят специалистов по ИТ на кафедре информатики и информационных таможенных технологий. "Мы будем обязаны использовать ПО из списка Минкомсвязи. И мы будем вынуждены уже в этом году переходить от его тестирования к использованию. Но основной переход

ПРОДОЛЖЕНИЕ НА С. 3

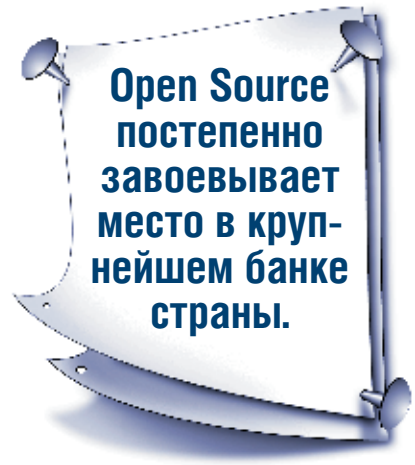
Сбербанк, OpenStack и особенности работы с СПО

НИКОЛАЙ НОСОВ

В полном соответствии с общемировыми тенденциями и российским курсом на импортозамещение наша крупнейшая ИТ-компания с банковской лицензией обратила внимание на Open Source. В последний день Гайдаровского форума на панельной дискуссии президент и председатель правления Сбербанка Герман Греф выступил с неожиданным заявлением о переходе на Open Source-платформу — программный продукт GridGain In-Memory Data Fabric.

Генеральный директор "Сбербанк-Технологий" Алиса Мельникова впоследствии смягчила заявление руководителя банка. Она уточнила, что использование GridGain In-Memory Data Fabric является "одним из важных, но далеко не единственным направлением". По ее словам, несмотря на успешно проведенное тестирование СУБД PostgreSQL как возможной замены СУБД Oracle, с учетом того, что Сбербанк владеет неограниченной корпоративной лицензией на указанный продукт Oracle, никаких планов по переходу на СПО-платформу у него нет.

Но все же Open Source постепенно завоевывает место в крупнейшем банке страны. Новое свидетельство тому — открытый тендер "Выбор организации на выполнение работ по разработке программного обеспечения в отношении платформы динамической инфраструктуры OpenStack (Автоматизированная система Платформа динамической



инфраструктуры [АС ПДИ], IaaS) для нужд ПАО Сбербанк", информация о котором появилась на сайте госзакупок.

В конкурсной документации прямо написано: АС ПДИ "не должна содержать в своём составе никакого закрытого или коммерческого ПО". Все компоненты системы должны распространяться под открытыми лицензиями (например, Apache 2.0, GPL, LGPL, MIT, Creative Commons) и быть совместимыми между собой.

ИТ-инфраструктура Сбербанка

Все информационные системы Сбербанка распределяются по трём различным зонам

ПРОДОЛЖЕНИЕ НА С. 3

В НОМЕРЕ:

ROSS'2016: СПО в России — от Москвы до самых до окраин

ЕЛЕНА ГОРЕТКИНА

В последнее время интерес российских предприятий к Open Source растет в связи с экономическими проблемами и тенденцией к импортозамещению. Судя по докладам на апрельском саммите Russian Open Source Summit (ROSS)'2016, именно эти вопросы стимулируют организации к поиску альтернативных решений на базе свободного ПО (СПО), способных заменить дорогие зарубежные продукты с высокой стоимостью владения.

ПРОЕКТЫ

Расширяется и география СПО-проектов. Представленные на саммите системы реализованы в разных уголках страны, причем практически все они уже введены в эксплуатацию и используются, принося выгоду своим владельцам. Растет и разнообразие реализованных систем, которые охватывают различные сегменты ИТ-рынка — от инфраструктурных решений до прикладного ПО.

Правда, не всё идет гладко, поскольку у СПО есть своя специфика, да и сам рынок Open Source в нашей стране еще находится на стадии формирования. Делясь своим опытом, докладчики рассказали о проблемах, с которыми им пришлось столкнуться, и предложили рекомендации по преодолению подводных камней.

Экономия на стоимости владения как стимул для перехода на СПО

Большинство представленных проектов относится к госсектору, что неудивительно. Ведь ИТ-бюджеты органов власти продолжают сокращаться, но остались нерешенные задачи, появляются новые вопросы и для всех них необходимы ИТ.

Рубен Энфиаджян

Судя по докладам, основная причина перехода государственных предприятий на СПО связана со стремлением сократить стоимость владения программным обеспечением, хотя тема импортозамещения тоже звучала, но в меньшей степени.

Общую идею сформулировал Рубен Энфиаджян, начальник департамента управления инфраструктурой автоматизированной информационной системы Пенсионного фонда РФ (ПФР), который отметил, что использование Open Source может помочь оптимизировать стоимость владения продуктом за счет его доработки и поддержки своими силами. Это может дать значительную экономию, так как не секрет, что затраты на поддержку со стороны производителя коммерческого продукта зачастую бывают существенными, а согласно политике многих производителей такая техническая поддержка является одним из требований при покупке решения.

Он рассказал о двух СПО-проектах, недавно реализованных в ПФР, — системе электронного документооборота (СЭД) и подсистеме внешнего взаимодействия с клиентами на базе личного кабинета застрахованного лица.

Для разработки СЭД был проведен конкурс и выбран подрядчик с условием, что код остается в собственности государства. Сопровождение системы также отдано на аутсорсинг. По словам Рубена Энфиаджяна, в результате создана и внедрена отечественная кроссплатформенная

ПРОДОЛЖЕНИЕ НА С. 8

ASUS®
В ПОИСКАХ НЕВЕРОЯТНОГО

№1

№1 на мировом рынке 13-дюймовых ультратонких ноутбуков с Windows

По данным из отчетов GFK и NPD за 2015 год
(без учета моделей-трансформеров)

от 79 990 руб.

ASUS ZenBook™ UX305CA
Быстрый. Тонкий. Красивый.

- Новейший процессор Intel® Core™ m7-6Y75
- Операционная система Windows 10 Домашняя
- Ошеломляющий 13,3" IPS-дисплей с разрешением QHD+ (3200x1800)* или Full HD (1920x1080) и матовым покрытием
- Абсолютно бесшумный благодаря пассивной системе охлаждения

Улучшить классический дизайн ультрабуков Zenbook было непросто, однако мы смогли это сделать. Новая модель Zenbook UX305 выполнена в изумительном по красоте корпусе толщиной 12,3 мм и весом всего 1,2 кг. В ее аппаратную конфигурацию входит невероятно четкий 13,3-дюймовый дисплей формата QHD+, мощный процессор Intel® Core™ M шестого поколения и высокоскоростной твердотельный накопитель емкостью до 512 ГБ. Это тот же Zenbook, что и раньше, только лучше!

Intel Inside®, значит потрясающие возможности.

intel inside™ CORE™ m

* спецификации отличаются в зависимости от модели

ПРИСОЕДИНЯЙТЕСЬ К НАМ В СОЦИАЛЬНЫХ СЕТЯХ:

VK.COM/**ASUS** FACEBOOK.COM/**ASUS.RU** TWITTER.COM/**ASUS_RUSSIA** INSTAGRAM.COM/**ASUS_RUSSIA**

Импортозамещение...

ПРОДОЛЖЕНИЕ СО С. 1

состоится в 2017 г.", — сказал Дмитрий Данилин.

Типы импортозамещения

Начальник Центрального информационно-технического таможенного управления ФТС России Алексей Тимофеев объяснил, как понимать задачу импортозамещения в условиях санкций в области высокотехнологичных товаров, и перечислил возможные типы импортозамещения:

- "прямое" замещение импортных товаров на товары российского производителя;
- "прямое расширенное" замещение — то же самое, но на товары Евразийского экономического союза;
- замещение импортных товаров из стран, проводящих санкционную политику в отношении России";
- локализация производства высокотехнологичной продукции и ее сертификация в России (OEM-партнерство);
- замещение импортных товаров из стран, не проводящих по отношению к России санкционную политику, например Китая;
- замещение импортных товаров на свободно распространяемые товары или продукты с открытым кодом.

При этом он отметил, что в условиях сжатых сроков, поставленных Президентом РФ, предпочтительным выглядит четвертый вариант — локализация производства. И предложил не забывать про шестой вариант — использование свободного ПО.

Системы управления базами данных

Особое внимание на конференции было уделено системам управления базами данных. Нет, компания Oracle, чья СУБД сейчас используется в ФТС, не отказала в поддержке, но резко повысила стоимость сопровождения. Так что вопрос перехода на другие СУБД стал актуальным и без всякой программы импортозамещения.

На конференции выступили поставщики трех СУБД, которые хотят занять место Oracle в информационных системах ФТС. Каждый из них доказывал свои преимущества.

Заместитель генерального директора ООО "Постгресс Профессиональный" Иван Панченко указал, что российская СУБД Progress Pro создана на базе свободной SQL-СУБД Progress, поддерживаемой открытым сообществом, в котором ведущую роль играют российские разработчики. В 2007 г. были опубликованы результаты тестов этой СУБД, показавшие ее производительность на уровне 85% от производительности Oracle. СУБД Progress успешно используется зарубежными государственными органами, такими как французские Национальный фонд семейных пособий (CNAF) и Национальная метеослужба Франции. Progress Pro входит в Единый реестр российского ПО.

Директор по продажам ООО "Тимекс Рус" Руслан Мельников предложил в качестве замены южнокорейскую СУБД Tibero, которая уже тестировалась ФТС. Плюсом системы является ее практически полная совместимость с Oracle. Поэтому специалистам по Oracle, работающим в ФТС, даже не придется переучиваться. Еще один плюс — Tibero была выбрана в качестве СУБД для Национальной системы платежных карт (НСПК).

Третья альтернатива Oracle — СУБД "ЛИНТЕР". Основное ее достоинство, как считает представивший систему Роман Баркалов, — это полностью российская разработка. Докладчик вспоминал 188-ФЗ от 29 июня 2015 г. и особо отметил, что их СУБД не просто полностью не зависит от иностранных государств, но и удовлетворяет всем российским требованиям в области безопасности.

Импортозамещение телекоммуникационного оборудования

"В 1990-е доля импортного оборудования в таких отраслях, как телекоммуникации и связь, являющихся стратегическими, достигла 90%. Этот запредельный для национальной безопасности уровень, к сожалению, сохраняется и сейчас", — заявил на конференции Алексей Тебекин, проректор Российской таможенной академии по научной работе.

У ФТС уже есть проблемы с западными вендорами, возникшие после введения санкций. "В конце 2014 г. Cisco, предварительно спросив, будем ли мы использовать их оборудование в военных целях, и получив естественный ответ — нет, т. к. мы гражданское министерство, отказало нам в обслуживании своих устройств. Приходится пока обходиться своими силами", — сказал Дмитрий Данилин.

При этом он отметил, что отечественных коммутаторов и маршрутизаторов большой емкости просто физически нет. "Либо они есть, но выпущенные китайцами с наклейкой типа "Родничок". Это нам не подходит. Мы ждем действительно российскую разработку", — пояснил он, добавив, что сейчас ФТС тестирует только российские коммутаторы и маршрутизаторы малой емкости.

Нельзя сказать, что в плане импортозамещения ничего не делается. Об этом свидетельствует и созданный реестр российского ПО, и отдельные достижения в создании национальной платежной системы. Есть и обнадеживающие цифры ФТС — импортозависимость оборудования и технологий, применяемых в таможенных органах в программных и технических средствах защиты информации, составляет всего 8%. Однако в целом процесс идет очень медленно и требует постоянного подталкивания с самого верха, что, видимо хорошо понимают в руководстве страны.

Послесловие

В день проведения конференции на сайте Центрального информационно-технического таможенного управления появилось сообщение: "В связи со сбоем аппаратно-технических средств Главного центра обработки данных ФТС России с 31.03.2016 в таможенных органах, непосредственно подчиненных ФТС России, отсутствует техническая возможность совершения таможенных операций, связанных с помещением товаров под таможенную процедуру. Ведутся восстановительные работы".

"С 12 часов 31 марта в результате сбоя в работе электронной системы декларирования российской таможни полностью парализована экспортная деятельность российских предприятий, направляющих свои грузы в Китай. Причины технической неисправности не известны", — сообщило издание "Южный Китай — Особый взгляд".

Проблемы коснулись таможенных управлений "по всей стране". Сроки окончания восстановительных работ переносились несколько раз. На момент публикации данной статьи они решены не были.

Сбербанк...

ПРОДОЛЖЕНИЕ СО С. 1

функционального назначения:

- продуктивные зоны, выполняющие задачи штатного функционирования информационных систем;
- зоны тестирования, где контролируется качество разработок и настроек информационных систем перед их внедрением в продуктивные зоны;
- зоны разработки, где информационные системы разрабатываются, настраиваются и тестируются.

АС ПДИ, которую предполагается использовать в ЦОДе Сбербанка в Южном Порту (Москва), предназначена для организации доступа к тестовым средам и управления их жизненным циклом, состоящим из следующих этапов:

- описание конфигурации в терминах используемых базовых инфраструктурных сервисов;
- размещение заказа на создание;
- разворачивание тестовой среды средствами АС ПДИ:
- эксплуатация тестовой среды;
- уничтожение тестовой среды.

Система должна поддерживать до 8500 одновременно запущенных виртуальных машин, до 700 физических серверов-гипервизоров, до 1000 пользователей, в том числе до 250 одновременно работающих.

В рамках первой фазы подсистема вычислительных сетей (ПВС) должна быть реализована при помощи базовой функциональности модуля OpenStack Neutron. При этом все изменения референсной архитектуры OpenStack реализуются с использованием штатного и предусмотренного архитектурой механизма расширения (плагины OpenStack Deployment Service — Fuel), чтобы обеспечить повторяемость при повторном разворачивании.

Система должна включать ПВС, осуществляющую управление жизненным циклом экземпляров виртуальных машин (создание, размещение и удаление) и основанную на ПО OpenStack Nova.

Подсистема хранения данных (объектная) реализуется на базе ПО с открытым исходным кодом OpenStack Swift.

Подсистема оркестрации должна реализовывать механизм исполнения бизнес-процессов (workflow engine) на базе OpenStack Mistral.

Система управления доступом на базе OpenStack Keystone должна поддерживать интеграцию с внешним каталогом пользователей Microsoft Active Directory по протоколу LDAP и применение ролевой модели разграничения доступа к ресурсам и операциям.

Сбербанк и открытое сообщество

Интересно, что в требованиях прямо написано, что должна быть обеспечена поддержка сообщества OpenStack (здесь и далее имеются в виду участники соответствующих проектов) для программного кода, спецификаций, документации и автоматических тестов, разработанных в рамках проекта. При этом необходимо:

- обеспечить положительные отзывы на программный код, спецификации и автоматические тесты, разработанные в рамках проекта и относящиеся к основным компонентам OpenStack, со стороны сообщества OpenStack;
- обеспечить размещение программного кода (модель лицензирования кода определяется совместно с заказчиком), спецификаций, документации и автоматических тестов в основном публичном репозитории исходного кода OpenStack.

Пожалуй, это первый такого рода документ Сбербанка, где требуются положительные отзывы на программный код со стороны сообщества и размещение в публичном репозитории исходного кода на GitHub.

Как работать с OpenStack

Как Сбербанк сможет работать с OpenStack? В чем преимущества этого решения? За комментариями мы обратились к Илье Алексееву, координатору российского сообщества OpenStack.

PC Week: Как устроен проект OpenStack?

ИЛЬЯ АЛЕКСЕЕВ: Серьезное преимущество модели Open Source заключается в возможности объединить ресурсы компаний, в которых работают лучшие специалисты ИТ-индустрии. При этом у каждой компании свои интересы, желание адаптировать разработку под свое "железо" или свои программные решения, свои взгляды на то, какие направления разработки наиболее важны. Чтобы найти баланс, все решения принимаются публично — все всё видят. Общую стратегию определяет технический комитет. Состав комитета определяется выборами, его задача определять техническую стратегию развития в целом.

Илья Алексеев

Сам OpenStack разделен на ряд программных проектов, охватывающих определенные направления. Для каждого отдельно взятого проекта есть также избираемый технический лидер проекта (Project Technical Lead, PTL) и основная команда (Core Reviewers, CR). При создании патча и отправке его в основную ветку кода именно эта команда принимает решение о принятии или непринятии патча. Проектирование также открытый процесс. Таким образом, road map развития выбирает сообщество в целом.

PC Week: Насколько сложно попасть в технический комитет?

И. А.: Сообщество очень демократично. Всё определяется выборами. При этом учитываются авторитет человека и его вклад в сообщество — свой написанный код, его положительная оценка другими, его собственные оценки и рецензии на код других разработчиков. Таким же образом выбираются PTL по отдельным направлениям OpenStack.

PC Week: Как можно выполнить требование Сбербанка и разместить разработку в основном публичном репозитории исходного кода на GitHub? Кто принимает такое решение?

И. А.: Решение принимают разработчики конкретного проекта. Непосредственно решение принимается членами основной команды проекта (CR + PTL). CR вы можете стать, если наберёте достаточный авторитет в сообществе, чтобы другие CR данного проекта присвоили вам такой статус. Это долгий и не совсем простой процесс.

PC Week: Какие есть модели работы с OpenStack?

И. А.: Есть несколько подходов. Самый простой — вы скачиваете "ванильную" версию, сами ее ставите, адаптируете под свои нужды и поддерживаете. Вариант полностью бесплатный, но надо понимать, что вам придется развивать экспертизу в своей компании. В этом варианте лучше всего, если вы будете участвовать в сообществе своими группами разработчиков.

Второй подход — использовать компанию, специализирующуюся на OpenStack. Эта компания адаптирует решение под ваши нужды и даже сможет в дальнейшем осуществлять поддержку. Но если эти изменения не попадут в основной публичный репозиторий (Upstream), то со временем ваша версия будет все сильней отличаться от основной и ее поддержка будет обходиться вам все дороже.

Третий вариант — заключить договор с компанией, у которой есть опыт работы с сообществом и широкая экспертиза, способность отстаивать свои решения в сообществе, и на этой базе начать развивать собственную экспертизу. Похоже, что по этому пути и идет Сбербанк. Выбранная компания-подрядчик будет размещать свои разработки в основном публичном репозитории. И будем надеяться, что после этого Сбербанк разовьет свою экспертизу в необходимом объеме.

PC Week: Почему Сбербанк выбрал OpenStack?

И. А.: OpenStack — оптимальное открытое решение для облачных приложений. Сейчас его используют крупнейшие западные компании, такие как Bloomberg, Wal-Mart, eBay, PayPal и др. Это обеспечивает им гибкость и сокращает время разработки. Как заявил Герман Греф, время разработки и внедрения новых продуктов в Сбербанке должно измеряться часами, а не месяцами, поэтому выбор облачной платформы OpenStack для разработки ПО банка представляется вполне логичным.

Автор статьи — канд. техн. наук, член ассоциации RCCPA.

СОДЕРЖАНИЕ

№ 7 (906) • 19 АПРЕЛЯ, 2016 • Страница 4

НОВОСТИ

УПОМИНАНИЕ ФИРМ В НОМЕРЕ

ЭКСПЕРТИЗА

ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ

БЛОГОСФЕРА PCWEEK.RU

Реестр отечественного ПО создается… А зачем?

Андрей Колесов,
pcweek.ru/business/blog

Минкомсвязи опубликовало очередную новость об успехах в деле формирования Единого реестра российского ПО: в нём уже более трёхсот программных продуктов. Что ж, процесс наладился, идет… Возможно, к концу года этот список будет насчитывать тысячу позиций или даже десять тысяч… Поскольку уже видно, что Реестр — это нечто осязаемое, можно задаться вопросом: зачем все это нужно?

Недавно на встрече с президентом Путиным глава министерства Никифоров рассказал о Реестре как о проекте по поддержке российских разработчиков ПО. И в чем же эта поддержка заключается, каковы ее результаты? Пока видны только затраты: нужно оформлять заявки, проводить экспертные советы…

Насколько я помню, Реестр нужен, чтобы заставить российские госорганы покупать отечественное ПО (согласно закону о госзакупках ФЗ-44). Но как в реальности он влияет на процесс закупок? Повышается ли "российская доля"? Растет ли она в абсолютных показателях? Довольны ли госорганы такой новой практикой? И что думают те, кого они поддерживают (разработчики ПО)?

Понятно, что сейчас, когда Реестр только-только принял осязаемые формы, получить полные ответы на все эти вопросы сложно (хотя мнение у фирм-разработчиков наверняка уже есть). Но собираемся ли мы давать такие ответы по итогам 2016 г.? А если собираемся (что, мне кажется, просто необходимо), то существуют ли механизмы для этого? Есть ли механизм учета закупок ПО по ФЗ-44? Предусматривает ли он разделение ПО на "отечественное" и "неотечественное"? Короче: как Минкомсвязи собирается оценивать эффективность проекта по созданию Реестра?

Проблема проекта "Реестр" видится как раз в том, что вопрос о его эффективности, о его реальном влиянии на процесс госзакупок, о его пользе с точки зрения поддержки российских разработчиков до сих пор вообще не ставился. Пока получается так: сказали копать — копаем…

Производство волоконно-оптических кабелей в России снизилось до уровня 2010 г.

Петр Чачин,
pcweek.ru/gover/blog

В 2015 г. в стране сократился выпуск волоконно-оптических кабелей (ВОК). Об этом на московской конференции "Transport Networks Russia 2016" сообщил заместитель заведующего отделением "Кабели, провода и арматура для систем телекоммуникаций и информатизации" ВНИИКП Анатолий Воронцов.

По его словам, за прошлый год производство ВОК в России по сравнению с 2014-м снизилось на 32,7%, до 3,8 млн. км в одноволоконном исчислении, и тем самым откатилось на пять лет назад, к уровню 2010-го.

По данным докладчика форума Comnews, на сегодняшний день в нашей стране действует 18 кабельных заводов, оснащенных современным оборудованием и способных выпускать любую кабельную продукцию. Их мощность в одноволоконном исчислении достигает 11 млн. км кабеля в год. Так что загрузка кабельных предприятий сейчас составляет порядка 30%.

И это при том, что в 2015 г. уже действовала довольно мощная программа Минкомсвязи РФ по сокращению цифрового неравенства между регионами, в рамках которой государственным оператором было построено около 20 тыс. км волоконно-оптических линий связи (ВОЛС). В целом в ходе данного проекта к концу 2018-го предстоит построить еще тысячи километров новых ВОЛС.

Между тем компания "Оптиковолоконные системы" в апреле-мае нынешнего года планирует начать промышленное производство оптического волокна на заводе в Саранске (Мордовия). Этот завод является первым и пока единственным в России предприятием, способным изготавливать отечественное оптоволокно. Удастся ли новому предприятию в условиях спада спроса на российскую кабельную продукцию утвердиться на российском рынке ВОК и выполнить свой бизнес-план, разработанный ещё в то время, когда был стабильный спрос на волокно? Ведь пока потребности страны в оптоволокне на 100% удовлетворяются за счет импорта.

Актуализируем права доступа

Валерий Васильев,
pcweek.ru/security/blog

Заявок на предоставление доступа в компаниях приходится обрабатывать много, а заявок на отзыв — считанные единицы. Почему? Вот как отвечает на этот вопрос Даниил Казаков, директор департамента технологий управления доступом фирмы RedSys.

Человеческая природа такова, что когда сотрудникам даются нетиповые, разовые задания, они настоятельно добиваются получения новых прав доступа, необходимых для выполнения порученной работы. Зато выполнив её, как правило, не спешат отзывать временные права доступа, сохраняя их за собой.

Бывает также, что перед уходом в отпуск сотрудник передаёт свои логины и пароли коллегам для завершения или продолжения важной работы.

Можно привести и другие примеры срочных временных изменений прав доступа. А вывод таков: необходим регулярный пересмотр этих прав и отзыв утративших актуальность.

Часто делается это вручную. Но если количество компьютеризированных рабочих мест достигает тысячи, специалисты RedSys рекомендуют внедрить систему управления правами доступа — IDM, что в этом случае становится экономически обоснованным. Срок окупаемости системы зависит от сложности бизнес-процессов и ИТ-инфраструктуры заказчика и составляет от одного до пяти лет.

Верхи не могут, низы не хотят, или О революционной ситуации в мире СПО

Сергей Бессонов,
pcweek.ru/foss/blog

Ещё один разработчик попросил исключить своё ПО из дистрибутива. Интересный поворот, не находите? Это как если бы производитель колбасы потребовал убрать свои продукты с полок магазина торговой сети.

Но обо всём по порядку. Разработчик XScreensaver, программы-скринсейвера, попросил убрать свою программу из дистрибутива Debian. Мотивировал он это тем, что в дистрибутиве используется очень старая версия, от 2014 г., и майнтейнеры не хотят обновлять её до свежих. Из-за чего в программе остаются неисправленными ошибки и уязвимости.

Автор даже сделал предупреждение для пользователей о том, что они используют старую версию ПО. Естественно, пользователи забросали майнтейнеров пакета просьбами обновить ПО или убрать это предупреждение. И майнтейнеры… убрали предупреждение!

В результате пользователи, исправно сообщающие об ошибках в программе, направляются в апстрим, где сидят разработчики, которые уже года два как все ошибки устранили. В связи с этим разработчик и потребовал вообще удалить этот пакет из дистрибутива — работать стало невозможно.

Это не первый случай удаления пакета из репозиториев крупных дистрибутивов, другой был связан с разработчиками OwnCloud, которые потребовали удалить свой пакет из репозиториев Ubuntu по той же причине: в дистрибутиве лежала слишком старая версия с незакрытыми уязвимостями и неисправленными ошибками. Ставить OwnCloud в Ubuntu разработчики рекомендуют при помощи официального микрорепозитория.

С ростом количества конечных пользователей на платформах Linux вопрос взаимодействия разработчиков с ними становится всё острее. Хорошо было в начале 2000-х, когда пользователей было мало, они были опытные и не "доставали" разработчиков по мелочам. Сейчас же увеличение числа "хомячков" вскрывает всё больше проблем.

Вопрос этот решается по-разному. Например, разработчики Ubuntu реализуют механизм под названием Snappy — микроконтейнер на базе LXC, который содержит в себе приложение с необходимыми ему библиотеками, что позволяет изолировать приложение от системы и обновлять его независимо от цикла обновления дистрибутива.

Другой подход реализуют разработчики видеоредактора OpenShot. Они предлагают скачать его в виде пакета, собранного в системе AppImage, которая позволяет создавать универсальные бинарные файлы, пригодные для запуска в любом дистрибутиве.

Так или иначе, интерес к микрорепозиториям, универсальным бинарникам, аналогам "маковского" формата DMG и другим способам реализовать доставку софта мимо репозиториев будет расти. Сложившаяся ситуация требует революции.

Linux в Windows: дождались

Сергей Голубев,
pcweek.ru/foss/blog

Даже самые смелые фантазии иногда сбываются. Пользователи Windows 10 смогут запускать bash. А в ней соответственно — массу классических Linux-утилит и средств разработки, управлять которыми будет система apt. Причину такого решения назвал Стивен Воан-Николс: разработчикам требуется оболочка Linux независимо от того, в какой среде они работают.

Иными словами, на обычного пользователя Linux это новшество не ориентировано, поскольку никакого практического смысла для них в нём нет. Наверное, именно по этой причине "сенсация" была встречена пользовательским сообществом совершенно равнодушно.

Во всяком случае нет ни малейших оснований говорить, что таким образом компания Microsoft хочет "переманить" в свою систему пользователей Linux, которым в Windows для полного счастья не хватает только возможности запускать find, grep и sed. По крайней мере на рабочих станциях какой-то значимой для бизнеса конкуренции тут нет и никогда не было.

Насколько это новшество востребовано самими разработчиками? Пока в профильном блоге Microsoft по поводу "сенсации" есть всего одна запись с малосодержательными комментариями. Что может объясняться огромным числом очень недорогих "облачных" решений, позволяющих использовать любую платформу.

На мой взгляд, новшество Microsoft — это либо пиар, либо "игра мышцами" (в конце концов, нельзя исключать те или иные честолюбивые мотивации у бизнеса). К реальной жизни это вряд ли имеет какое-то отношение.

Представляем новый сверхнадёжный 32-процессорный x86 сервер Huawei KunLun

Фундамент ИТ-системы для построения критически важных бизнес-приложений

Новый сервер Huawei KunLun – это основа для непрерывных бизнес-процессов. Инновационная межпроцессорная архитектура и технологии RAS 2.0 обеспечивают надёжность, необходимую для построения критически важных бизнес-приложений.

Leading New ICT
Building a Better Connected World*

*Создадим новые ИКТ-сети для мира общения

e.huawei.com/ru

HUAWEI

СК ПРЕСС PCWEEK RUSSIAN EDITION

Учредитель и издатель
АО «СК ПРЕСС»

Издательский директор
Е. АДЛЕРОВ
Издатель группы ИТ
Н. ФЕДУЛОВ
Издатель
С. ДОЛЬНИКОВ
Директор по продажам
М. СИНИЛЬЩИКОВА
Генеральный директор
Л. ТЕПЛИЦКИЙ
Шеф-редактор группы ИТ
Р. ГЕРР
Ведущий эксперт группы ИТ
С. КОСТЯКОВ

Редакция

Главный редактор
А. МАКСИМОВ
1-й заместитель главного редактора
И. ЛАПИНСКИЙ
Научные редакторы
В. ВАСИЛЬЕВ,
Е. ГОРЕТКИНА,
О. ПАВЛОВА, С. СВИНАРЕВ,
П. ЧАЧИН
Обозреватели
С. ГОЛУБЕВ, С. БОБРОВСКИЙ,
А. КОЛЕСОВ
Специальный корреспондент
В. МИТИН
Корреспонденты
О. ЗВОНАРЕВА,
М. РАЗУМОВА, М. ФАТЕЕВА
Тестовая лаборатория
А. БАТЫРЬ
Ответственный секретарь
Е. КАЧАЛОВА
Литературные редакторы
Н. БОГОЯВЛЕНСКАЯ,
Т. НИКИТИНА, Т. ТОДЕР
Фотограф
О. ЛЫСЕНКО
Художественный редактор
Л. НИКОЛАЕВА
Группа компьютерной верстки
С. АМОСОВ, А. МАНУЙЛОВ
Техническая поддержка
К. ГУЩИН, С. РОГОНОВ
Корректор
И. МОРГУНОВСКАЯ
Тел./факс: (495) 974-2260
E-mail: editorial@pcweek.ru

Отдел рекламы

Руководитель отдела рекламы
С. ВАЙСЕРМАН
Тел./факс:
(495) 974-2260, 974-2263
E-mail: adv@pcweek.ru

Распространение

АО "СК Пресс"
Отдел распространения, подписка
Тел.: +7(495) 974-2260
Факс: +7(495) 974-2263
E-mail: distribution@skpress.ru
Адрес: 109147, Москва,
ул. Марксистская, д. 34, к. 10,
3-й этаж, оф. 328

109147, Россия, Москва,
ул. Марксистская, д. 34, корп. 10,
PC WEEK/Russian Edition.

Газета зарегистрирована Комитетом РФ по печати 29 марта 1995 г.
Свидетельство о регистрации № 013458.
Отпечатано в ООО "Доминико",
тел.: (495) 380-3451.
Тираж 35 000.
Цена свободная.
Использованы гарнитуры шрифтов "Темза", "Гелиос" фирмы TypeMarket.

МФУ HP M577dn: удобство в эксплуатации, развитая защита, высокое качество

ДМИТРИЙ ЕРОХИН

Настольные многофункциональные устройства сегодня занимают ведущее положение на российском рынке лазерных печатающих устройств и, как отмечают аналитики IT Research, даже в условиях отмечаемого в настоящее время значительного сокращения платежеспособного спроса не уступают рынок менее дорогим лазерным принтерам. При этом сегмент цветных МФУ в подавляющем большинстве представлен однопроходными устройствами, имеющими одинаковую скорость печати в монохромном и цветном режимах. Именно к таким устройствам относится и модель Color LaserJet Enterprise MFP M577dn, выпущенная недавно компанией HP и предназначенная для использования в корпоративном окружении.

ПЕРВЫЙ ВЗГЛЯД

Устройство объединяет в себе лазерный печатающий механизм (A4/Letter) с паспортным быстродействием 38 стр./мин и планшетный сканер с модулем автоматической подачи документов на 100 листов, а при установке дополнительной аналоговой факс-платы приобретает возможности факса. Боковой откидывающийся лоток на 100 листов бумаги средней плотности (или 10 конвертов) дополняет основной нижний лоток на 550 листов. Если же потребности в печати особенно велики, то на этот случай предусмотрена установка еще трех подающих лотков (каждый также на 550 листов) и стойки, т. е. общее количество одновременно загружаемой бумаги может достигать 2300 листов. Стандартные варианты подключения — Ethernet 10/100/1000 и порты USB (основной, а также для прямой печати без компьютера файлов PDF, PS и других форматов и сохранения сканируемых документов). Для печати с мобильных гаджетов с функцией Wi-Fi Direct аппарат можно доукомплектовать модулем NFC/Wireless для HP Jetdirect 3000w, кроме того, допускается дооснащение сервером печати HP Jetdirect 2900nw для беспроводной связи. Данные для отложенной или конфиденциальной печати хранятся на встроенном жестком диске объемом 320 Гб,

HP Color LaserJet Enterprise MFP M577dn

ОЗУ размером 1,75 Гб можно расширить модулем SODIMM DDR3 до 2,5 Гб.

МФУ работает в среде Windows (начиная с XP и заканчивая 64-разрядными серверными версиями) и OS X 10.8+. Для мобильной печати реализована поддержка HP ePrint (включая Android, iOS и Blackberry), AirPrint и Android Printing.

Конструктивное исполнение МФУ производит очень приятное впечатление. Предусмотрены даже такие мелочи, как светодиодная подсветка приемного лотка. Но, безусловно, наиболее привлекающая внимание деталь МФУ — крупный (более 20 см по диагонали) цветной сенсорный дисплей. Он имеет отклоняемую конструкцию (вплоть до почти вертикального положения) и выглядит как закрепленный на принтере планшетный компьютер. Благодаря высокой чувствительности экрана использовать его действительно так же удобно, как и настоящий планшет. Небольшие нарекания может вызвать лишь русификация экранного интерфейса, не всегда понятная из-за сокращений и неточного перевода. Тем не менее меню организовано в целом удобно и наглядно, разве что ему недостает единообразия навигации (например, из некоторых диалогов нет очевидного выхода), а названия пунктов интерфейса в Справке не всегда соответствуют их действительным названиям. Вместе с тем нельзя не отметить у модели обилие настроек (в том числе по работе с цветом), так что удобство большого экрана трудно переоценить.

Стоит отметить, что серия M577 примечательна моделями с усиленной защитой данных, реализованной на уровне самого аппарата. В МФУ помимо аппаратного шифрования (AES-256) данных на встроенном жестком диске применены технологии защиты памяти от несанкционированного внешнего вмешательства и автоматической перепрошивки эталонной BIOS, недоступной для злоумышленников в случае атаки. Насколько это актуально — сказать сложно, однако, по мнению производителя, проблема защиты (особенно в корпоративном секторе) сегодня становится все более актуальной в связи с растущим числом пользователей, применяющих для печати мобильные устройства.

Как показал реальный опыт работы с предоставленным нам экземпляром МФУ, начальная инициализация устройства при включении занимает около 2 мин. Благодаря печке с мгновенным разогревом в дальнейшем задержек уже не возникает. Интересный нюанс: в аппарате применяются компактные, но емкие (примерно 12,5 тыс. черно-белых и 9,5 тыс. цветных страниц) тонер-картриджи с технологией JetIntelligence, способствующей меньшему потреблению энергии, более эффективному расходу тонера и защите от подделок. Дополнительное энергосбережение объясняется тем, что принтер анализирует распечатываемую страницу и в зависимости от ее содержимого выбирает один из нескольких температурных режимов печки. Замена картриджей выполняется с фронтальной стороны аппарата и не представляет сложности даже для неспециалистов. Отметим также, что рекомендуемый производителем ежемесячный объем печати (определяется с учетом интервалов на замену расходных материалов и периода расширенной гарантии на устройство) составляет 2500—7500 стр., хотя максимальная месячная нагрузка существенно выше — до 80 тыс. стр.

В тестах на производительность изделие HP в целом подтвердило заявленные характеристики. Скорость печати контрольных заданий варьировалась от 37,8 до 38,2 стр./мин, т. е. была в пределах погрешности, а в дуплексном режиме превосходила 40 стр./мин, время вывода первой страницы в одностороннем режиме печати не превышает 9—10 с. Столь же быстро выполнялось и копирование односторонних документов с использованием автоподатчика. Кстати, устройство автоподачи имеет двусторонний сканирующий модуль, что способствует дополнительному комфорту при копировании страниц с содержимым на обеих сторонах. Скорость такого копирования в наших испытаниях составила около 18 стр./мин. Единственную заминку у аппарата вызвала печать насыщенного цветной графикой 16-страничного документа PDF: после семи страниц МФУ "задумалось" на несколько секунд, из-за чего итоговая средняя скорость составила 25,7 стр./мин.

Только хвалебных слов заслуживает качество печати. Совмещение цветов — идеальное, тонкие волосяные линии (в том числе цветные) остаются различимыми даже на выворотке со сплошным черным фоном. Мелкий текст (тоже в том числе цветной и на выворотке) остается разборчивым вплоть до размера 1—2 пункта. Градиентные и сплошные заливки передаются равномерно и в большинстве случаев без полос.

В целом аппарат HP оставил весьма приятные впечатления. Высокое качество печати, богатая функциональность, удобство эксплуатации, высокая производительность — вот те качества, благодаря которым мы можем рекомендовать его к приобретению организациям.

Самая большая проблема больших данных — их слишком трудно загружать

ДЖЕЙСОН ХАЙНЕР

Многие компании купаются в данных, которых больше, чем они могут использовать. К сожалению, слишком многие из тех, кто буквально тонет в данных, связывают эту проблему с самими большими данными. С точки зрения технологии большие данные представляют совершенно особое явление — сочетание структурированных данных (принадлежащей вашей компании информации) с неструктурированными (из общедоступных источников, таких как социальные сети и правительственные органы).

Когда вы накладываете неструктурированные данные поверх структурированных и используете аналитическое ПО для их визуализации, вы можете делать то, чего никогда не могли прежде, — прогнозировать продажи продуктов, более целенаправленно обращаться к клиентам, выявлять новые рынки и т. д.

Большие данные больше не страдают от недостатка инструментов, как несколько лет назад. Тогда работа с большими данными требовала наличия в штате специалистов по данным (data scientists), владеющих инструментами с открытым исходным кодом, такими как R и Hadoop.

Сегодня имеется множество компаний, готовых помочь визуализировать большие данные, начиная с таких специализированных фирм, как Tableau, Qlik, TIBCO и MicroStrategy, и заканчивая разработчиками законченных решений вроде Microsoft, IBM, SAP и Oracle.

Однако, по словам руководителей ИТ-подразделений, выступавших на прошлой неделе в г. Орландо на мероприятии Midmarket CIO Forum / Midmarket CMO Forum, одна из главных трудностей, с которой сталкиваются компании при использовании всех этих аналитических платформ, заключается в загрузке данных.

Один из CIO сказал: "Наша самая большая проблема в области ИТ связана с тем, как загрузить данные. Вот настоящее мучение".

Знаменательно, что это утверждение подкрепляется результатами исследований.

Согласно исследованию компании Xplenty, специализирующейся на интеграции данных, треть специалистов по бизнес-интеллекту тратит от 50 до 90% своего времени на очистку сырых данных и подготовку их к загрузке в платформу обработки данных компании. Возможно, это связано с тем, что только 28% компаний считают, что извлекают из своих данных ценность стратегического значения.

Проблема очистки данных означает также, что некоторые из технических специалистов, пользующихся сегодня наибольшим спросом, тратят значительную долю своего времени на отупляющую работу по сортировке и организации наборов данных, прежде чем они будут подвергнуты анализу.

Это явно не очень хорошо масштабируется и серьезно ограничивает потенциал больших данных. А по мере того как мы собираем все больше и больше данных (с помощью Интернета вещей), трудности только усугубляются.

Имеются три потенциальных решения этой проблемы.

1. Совершенствование аналитического ПО для больших данных. Поскольку на протяжении последних пяти лет многие из этих компаний вкладывали в большие данные

ПРОДОЛЖЕНИЕ НА С. 11 ▸

Smart-UPS On-Line SRT производства Schneider Electric — ИБП высокого уровня готовности

На рынке ИБП действует целый ряд важнейших технологических и рыночных тенденций, которые находят свое отражение в эволюции продуктового предложения ведущих игроков. При этом у российского рынка есть и своя специфика, связанная с необходимостью развивать ИТ-инфраструктуру в условиях неопределенности бизнеса и ограниченности бюджетов.

Аналитики компании ITResearch отмечают неуклонное сокращение продаж массовых ИБП, связанное со сжимающейся базой настольных ПК. По данным компании, российский рынок ИБП в 2015 г. по сравнению с докризисным 2007-м снизился на 80% в натуральном выражении. Однако падение в денежном выражении было намного менее драматичным, что объясняется сдвигом рынка ИБП в сторону более дорогого инфраструктурного on-line-оборудования. Соответственно в данном сегменте происходит нарастание конкуренции, в первую очередь в связи с тем, что игроки массового рынка пытаются привнести сюда прежние принципы работы, включая ценовые войны.

ИБП Smart-UPS On-Line SRT2200XLI с дополнительным блоком внешних батарей

Но, несмотря на возросшее значение "ценового" фактора, подавляющее число корпоративных заказчиков не поддаются соблазну сэкономить. И дело здесь даже не в стоимости владения, в составе которой цена закупки оборудования тоже далеко не определяющая, а в стоимости простоев, которые зачастую абсолютно недопустимы, поскольку оборачиваются несоизмеримыми финансовыми и имиджевыми потерями. Поэтому, несмотря на появление множества аналогов, высококачественное и высокотехнологичное оборудование отраслевого лидера компании Schneider Electric остается неизменно востребованным.

Более того, Schneider Electric задает новые стандарты, поднимая потребительские характеристики современных ИБП на труднодостижимую для конкурентов высоту. Наступление эпохи мобильности приводит к тому, что времени на разворачивание ИТ-инфраструктуры отводится всё меньше. Поэтому всё более востребованными становятся модульные и стоечные решения Schneider Electric, которые находятся непосредственно в стойке, рядом с защищаемым критичным оборудованием. Это не только сокращает сроки запуска системы, но и позволяет зачастую собирать и обслуживать систему собственными силами.

Современные топологии и форм-факторы

Стоит отметить, что все легкие ИБП могут быть исполнены в трех основных форм-факторах, задающих сферу их применения. Классическими вариантами являются tower, или "башня", предполагающая напольную или настольную установку, а также Rack/Mount (RM), или "стоечное" исполнение. Но помимо этого в последние годы всё большей популярностью пользуется так называемый универсальный корпус — Rack/Tower (RT), позволяющий с легкостью размещать ИБП или в стойку, или (со специальными ножками) в напольном варианте. Именно на данном направлении сейчас сосредоточена инженерная мысль всех ведущих производителей, и именно в таком форм-факторе выпускаются все старшие модели легких ИБП, естественно, с лучшими техническими характеристиками.

Топология исполнения RT ИБП может быть как интерактивной (реже), так и on-line (двойного преобразования). Данный термин означает, что ИБП сначала переводит переменный ток внешней сети в постоянный, а затем уже формирует из него синусоидальное напряжение для питания нагрузки. Таким образом подключенное оборудование получает высококачественное питание, полностью избавленное от каких-либо угрожающих внешних факторов.

Естественно, данные процессы оборачиваются определенными потерями энергии, которые в случае легких on-line-ИБП могут достигать 10% и более, в то время как интерактивные ИБП работают почти со 100%-ным КПД (примером последних могут служить высококачественные линейки ИБП Schneider Electric с синусоидальным выходным напряжением при работе от батарей Smart-UPS SMC, SMT и SMX, которые по потребительским характеристикам практически не уступают on-line-решениям).

Однако при малых мощностях суммарные потери электроэнергии не столь уж велики. Кроме того, в случае отличной внешней электросети всегда есть возможность пустить ток по обходному пути (по байпасу), когда on-line-ИБП работает без потерь, т. е. фактически как интерактивное устройство.

Подтверждая статус технологического лидера, в сегменте легких on-line ИБП компания Schneider Electric выпускает модульные решения семейства Symmetra и широкий спектр высокоэффективных RT-решений Smart-UPS On-Line мощностью от 1 до 20 кВА. Устройства данных линеек аналитическое издание "Бестселлеры ИТ-рынка" не раз признавало "бестселлерами года", т. е. наиболее продаваемыми ИБП в своих классах на российском рынке.

Позиционирование модельного ряда Smart-UPS On-Line

Модельный ряд ИБП Smart-UPS On-Line в стоечном варианте занимает пространство от 2U до 12U и предназначен для бесперебойного питания оборудования с высокой плотностью мощности: серверов, сетей голосовой связи и передачи данных, медицинских лабораторий и небольших промышленных установок. Недавно представленные модели мощностью 15 и 20 кВА позволяют подключать энергоемкие блейд-серверы и стойки с высокой плотностью мощности. Когда критически важные для бизнеса системы нуждаются не в минутах, а в часах автономной работы, ИБП Smart-UPS On-Line может комплектоваться дополнительными батарейными кабинетами, обеспечивающими повышенные требования к времени автономной работы.

ПО управления PowerChute поддерживает безопасное автоматическое завершение работы сетевых операционных систем. Все модели мощностью 5 кВА и выше комплектуются встроенной платой сетевого управления (опция для моделей мощностью менее 5 кВА). ИБП от 8 кВА имеют на выходе клеммы для подключения оборудования напрямую проводами, а также возможность подключения по трехфазному входу. Вся линейка ИБП Smart-UPS On-Line представляет особый интерес для требовательных заказчиков, которым важны такие характеристики, как очень широкий диапазон входного напряжения, предельно точная стабилизация выходного напряжения, стабилизация частоты, встроенный байпас и коррекция входного коэффициента мощности.

Текущая линейка Smart-UPS On-Line

Новая линейка Smart-UPS On-Line SRT была представлена в 2014 г. в мощностных модификациях 5, 6, 8 и 10 кВА. А в декабре 2015 г. она была расширена моделями мощностью 2,2 и 3 кВА. Линейка Smart-UPS On-Line SURT в мощностном диапазоне от 2,2 до 10 кВА уже не производится, но пока доступна в мощностях 1, а также 15—20 кВА.

Текущий модельный ряд Smart-UPS On-Line SRT представлен моделями SRT2200XLI, SRT2200RMXLI, SRT3000XLI, SRT3000RMXLI, SRT5KXLI, SRT5KRMXLI, SRT6KXLI, SRT6KRMXLI, SRT8KXLI, SRT8KRMXLI, SRT10KXLI, SRT10KRMXLI.

Модели с индексами KXLI и KRMXLI отличаются тем, что вторые поставляются в стоечном исполнении.

Преимущества Smart-UPS On-Line SRT

Аппараты линейки Smart-UPS On-Line SRT обладают широким диапазоном входного напряжения: от 120 до 280 В при неполной нагрузке. Технология двойного преобразования энергии обеспечивает точные выходные параметры напряжения и частоты, а также нулевое время переключения на питание от батарей для реактивной нагрузки.

Самый мощный представитель линейки Smart-UPS On-Line SRT на 10 кВА в стоечном исполнении

Уникальной особенностью модельного ряда Smart-UPS On-Line SRT являются лучшие отраслевые показатели по выходной мощности, ранее практически недоступные в данных диапазонах мощностей. Все модели мощностью от 6 до 10 кВА имеют коэффициент мощности 1,0, т. е. максимальная мощность в ваттах (Вт) равна заявленной мощности в вольт-амперах (ВА). У моделей на 2,2, 3 и 5 кВА коэффициент мощности равен 0,9, что также выше, чем у большинства одноклассников. Это позволяет им передавать больше энергии источникам питания с активной коррекцией коэффициента мощности, применяемым в современных серверах и сетевых устройствах. Такое уникальное решение в данном классе не имеет аналогов на рынке и позволяет использовать данные ИБП с более серьезной ИТ-нагрузкой, чем у конкурентов.

ИБП Smart-UPS On-Line SRT представляют собой устройства высокого уровня готовности, в которых инвертор непрерывно регулирует выходные параметры. В результате они могут применяться для защиты широчайшего класса оборудования, в том числе нетерпимого к малейшим провалам напряжения или отклонениям его частоты (например, устройств с неимпульсными источниками питания, которые широко распространены на производстве и в системах управления). За счет высокой эффективности, достигающей 97%, они выдают больше энергии для питания электроники с активной коррекцией коэффициента мощности на входе. Возможность работы с перегрузкой в 150% позволяет подключать к ним принтеры, насосы, запитывать сразу несколько рабочих мест.

Все модели новой линейки оснащаются встроенными платами сетевого управления, что позволяет управлять работой источника через веб-интерфейс, SNMP и Telnet, выключать несколько серверов с помощью PowerChute Network Shutdown, а также обеспечивает возможность контроля широкого набора параметров, вплоть до мониторинга температуры. Для эффективного мониторинга режима работы и потребления энергии предусмотрен встроенный счетчик электроэнергии. ИБП оснащены разъемом SmartSlot, поддерживают управление и обновление ПО через сеть и совместимы с InfraStruxure Manager.

Данные автоматической самодиагностики и уведомления о прогнозируемых отказах отображаются светодиодными индикаторами, что упрощает эксплуатацию ИБП. Для оперативного отражения полной информации о состоянии ИБП служит графический ЖК-дисплей с многоцветной подсветкой, который также используется для просмотра диагностических данных и регистрационных журналов, что помогает выявлять неисправности прежде, чем они приведут к простою. При этом сигнализация о тревожных и аварийных событиях изменением цветового фона дисплея позволяет заметить событие на большом расстоянии от ИБП.

В новой линейке ИБП Smart-UPS On-Line реализован механизм интеллектуального управления батареями и прогнозирования рекомендуемой даты их замены. Также предусмотрена возможность "горячей" замены батарей пользователем и подключения внешних аккумуляторов в режиме Plug-and-Play. При появлении электричества в сети можно сразу же начать питание нагрузки, не дожидаясь зарядки батареи. Важным эксплуатационным преимуществом является то, что новые ИБП рассчитаны на сокращенные сроки подзарядки батарей, что актуально в случае высокой вероятности нескольких последовательных отключений с короткими периодами нормальной работы. Кроме того, ИБП допускает включение с незаряженной батареей, что позволяет запускать нагрузку немедленно после восстановления электроснабжения.

ИБП имеют управляемые группы розеток, что дает возможность увеличения времени автономной работы за счет отключения второстепенного оборудования, а также позволяет обеспечить управляемые перезапуски устройств, последовательное включение/выключение и управление работой ИБП по расписанию. Встроенный автоматический и опциональный ручной сервисный байпасы обеспечивают возможность питания подключенного оборудования даже при отказе самого ИБП.

Учитывая способность большинства вычислительных и сетевых устройств без последствий выдерживать краткие перебои в электроснабжении (20 мс и более), возможна эксплуатация ИБП Smart-UPS On-Line в экорежиме, когда двойное преобразование не выполняется и уровень эффективности достигает 97%. В результате не только снижается потребление электроэнергии, но и уменьшается выделение тепла, что положительно сказывается на сроке службы ключевых компонентов, таких как батареи. Наконец, в наиболее мощных моделях (на 8/10 кВА) предусмотрена вторая линия питания, подключаемая в режиме "байпас".

Благодаря такому набору функциональных и эксплуатационных характеристик APC Smart-UPS On-Line SRT могут использоваться для защиты очень широкого спектра различного оборудования: серверов, сетевого оборудования, АТС, хранилищ данных, систем безопасности и СКУД, промышленного и медицинского диагностического оборудования.

На все модели предоставляется трехлетняя гарантия на электронику и двухлетняя на внутренние и внешние батареи.

ROSS'2016...

ПРОДОЛЖЕНИЕ СО С. 1

СЭД на базе исключительно Open Source-компонентов. В частности, в качестве СУБД используется открытая база данных PostgreSQL, на которую ПФР перешел с СУБД IBM DB2. Сейчас в системе обрабатывается примерно миллион документов в год, а в 2017-м в соответствии с планом их число должно вырасти до трех миллионов.

Переход на электронные рельсы позволил значительно ускорить работу. Однако Рубен Энфиаджян признал, что достичь этих показателей было нелегко, так как вначале проходило обучение персонала и на первых порах регистрация документов занимала даже больше времени, чем при использовании бумаги: "Нынешних результатов мы добились лишь года через полтора".


Егор Васильев

Впрочем, такого рода проблемы характерны для внедрения любых новых ИТ-систем, как открытых, так и проприетарных. Но что связано именно с открытостью СЭД, так это снижение стоимости владения за счет минимизации операционных затрат на эксплуатацию.

Код СЭД уже передан в Национальный фонд алгоритмов и программ (НФАП) при Минкомсвязи, идея которого в том, чтобы всё ПО, разработанное на государственные деньги, другие госорганизации и ведомства могли использовать повторно. Правда, у СЭД Пенсионного фонда такие желающие пока не появились. По мнению Рубена Энфиаджяна, причина в том, что СПО — это новый тренд, еще не ставший массовым.

В качестве второго примера использования СПО он привел подсистему внешнего взаимодействия с клиентами, которыми являются все граждане страны и юридические лица, оплачивающие страховые взносы. Здесь используются ОС FreeBSD, СУБД PostgreSQL, поисковый сервер Sphinx, серверы приложений Apache, кэширования memcached, приема и балансировки запросов nginx, обработки запросов php-fpm.

Сейчас эта подсистема активно используется, и к ней постепенно подключаются новые сервисы. В результате за год с небольшим количество обрабатываемых обращений выросло в несколько десятков раз и по некоторым сервисам уже исчисляется миллионами.

Сравнивая проприетарные и открытые решения, Рубен Энфиаджян отметил, что хотя первые стоят дорого и приводят к зависимости от западных производителей, для них предусмотрено сопровождение с гарантированным качеством, существуют отработанные промышленные продукты, имеются готовые универсальные пакеты под ключ. К недостаткам СПО он отнес неопределенность в сопровождении: дорого или ненадежно, а по целому ряду направлений нет промышленных продуктов и готовых типовых решений, из-за чего на разработку уходит много времени. Однако в числе плюсов — то, что сами продукты — бесплатные или дешевые и их использование позволяет исключить зависимость от зарубежных компаний.

"Между этими двумя полюсами и приходится лавировать, — сказал Рубен Энфиаджян. — Теперь, начиная новую разработку, мы всегда смотрим, можно ли это сделать на свободном ПО, и стараемся выполнить все ключевые показатели по импортозамещению и использованию СПО в соответствии с планом Минкомсвязи России".

Из пользователей — в вендоры

Федеральную службу судебных приставов (ФССП) России можно считать ветераном в области применения СПО, так как она еще в 2013-м, когда и речи не было об импортозамещении, занялась созданием на базе Open Source своей информационной системы АИС ФССП России, разработку которой выполнил внешний подрядчик.

Егор Васильев, заместитель начальника УИТ ФССП по вопросам ИБ, объяснил, что интерес к Open Source прежде всего обусловлен экономическими соображениями: "Нашей службе и раньше выделялось гораздо меньше средств, чем другим ведомствам, а в прошлом году ИТ-бюджет значительно сократился по сравнению с 2014-м".

Исходя из этих реалий были выработаны принципы, без которых ФССП не удалось бы построить свою АИС: использование ПО с открытым кодом, максимальная унификация и минимальное разнообразие для упрощения внедрения в территориальных органах и объектах, централизация ключевых сервисов для взаимодействия с госорганами и самостоятельная сертификация разработанного ПО вместо приобретения дополнительных средств защиты.

Теперь, когда система уже давно внедрена и активно используется, в ФССП решили пойти дальше и сформировать на ее базе два продукта, которые согласно принятым критериям могут считаться отечественными, и передать их в Реестр российского программного обеспечения, тем самым превратившись из пользователя ПО в его поставщика. Впрочем, для мира Open Source это нормальное явление.


Сергей Дударев

Первый продукт — технологическая платформа системы АИС ФССП, построенная на базе открытой СУБД и ОС Linux с применением технологии Java. На этой платформе реализованы все основные сервисы и ведомственные процессы, в том числе средства безопасности.

Второй продукт — типовой дистрибутив ОС GosLinux на базе CentOS. По словам Егора Васильева, еще в 2013-м было решено использовать бесплатную ОС для всех приставов и работников аппарата управления, чтобы не платить за установку ПО для 40 тыс. рабочих мест и 2,5 тыс. серверов. Сейчас идет третий год внедрения GosLinux, и на нее переведено 20—25% техники по всем территориальным органам и объектам ФССП. До конца года планируется обеспечить 50%-ный охват.

В августе 2015-го GosLinux была размещена в НФАП. Егор Васильев вспоминает, что в тот момент в фонде было много специализированных информационных систем, не очень пригодных для повторного использования: "GosLinux стала первой универсальной системой, которую могут применять другие ведомства и, что более важно, региональные органы. Уже было пять скачиваний".

Чтобы оценить экономический эффект, в ФССП подсчитали, что стоимость владения GosLinux, включая разработку дистрибутива, подготовку документации для сертификации и работы по внедрению, составила 15,4 млн. руб., а проприетарные продукты Microsoft обошлись бы в 794 млн. руб.

Особый интерес представляет разработанная в ФССП схема бездисковой передачи сертифицированных обновлений для ОС региональным органам с помощью сертифицированного репозитория. В ФССП хотят поделиться этой схемой, чтобы ее могли применять остальные пользователи НФАП. Как пояснил Егор Васильев, Министерству связи и массовых коммуникаций было сделано соответствующее предложение: "Сейчас этот фонд предоставляет доступ к файлам и дистрибутивам через веб. По нашему мнению, необходимо реализовать полноценный репозиторий, который обеспечит автоматизированное обновление ПО потребителей, а также сервисы для разработчиков. Другими словами, мечтаем о национальном GitHub".

СПО в регионах

В силу экономических сложностей региональные власти начинают обращать больше внимания на затраты, в том числе имеющие отношение к ИТ. Так, в Хабаровском крае было замечено, что несогласованность между органами власти приводила к тому, что при внедрении новых ИТ-систем аналогичное ПО покупалось разными организациями; определённые проблемы возникали также из-за отсутствия консолидирующей системы учета расходов на информатизацию региона.

Поэтому решено было создать платформу, собирающую сведения об ИТ-проектах в регионе, включая затраты на внедрение и сопровождение, выстроить процесс согласованного использования информационных систем на всех направлениях развития региона и предоставить контролирующим органам механизм по непрерывному мониторингу затрат на информатизацию.

"Изначально стояла задача построить реестр, чтобы потом интегрировать его в государственную систему для передачи сведений. Но мы решили пойти немного дальше и сделать не просто учет ИТ-систем по ряду критериев, которых около девяноста, но собирать также сведения по ИБ и затратам", — объяснил Дмитрий Симон, главный специалист отдела ИС Министерства ИТ и связи Хабаровского края.

По его словам, реестр построили на СПО, включая Linux, СУБД MongoDB, node.js и браузер в качестве клиента. Разработку выполнила сторонняя компания, выбранная в результате тендера, у которой этот продукт на условиях лицензии был затем куплен MIT, но с ограничениями, такими как запрет на сублицензирование и продажу копий этого ПО, а также возможность использования его только на территории Хабаровского края.


Андрей Савиных

Однако Дмитрий Симон отметил, что с этой платформой получился интересный результат: "Мы увидели, что у нас есть некий шаблон реестра, который могут использовать и другие ведомства. Поэтому к нам стали обращаться разные организации". В итоге на базе одного продукта уже созданы три реестра: система управления ИТ-проектами региона, реестр связи Хабаровского края и типовой муниципальный реестр. Так что вместо одной СПО-системы удалось получить три.

С необходимостью перехода на СПО столкнулись и Барнаульские Горэлектросети (БГЭС). Раньше здесь использовалась проприетарная биллинговая система на базе СУБД Oracle. Но по словам Сергея Дударева, руководителя проектов управляющей компании БГЭС, главным вопросом были цены, поскольку проприетарное ПО стоит очень дорого.

Таким образом, было решено построить биллинг на СПО, тем более что организация уже имела опыт использования открытого ПО для непрофильной деятельности. Партнером по разработке и внедрению стала компания Siberium.

В качестве продуктов выбрали ERP/CRM-систему iDempiere, портал Liferay, OpenSuse Linux, PostgreSQL и Java. На их основе была создана единая информационная система, объединившая управление взаимоотношениями с потребителями, контроль за установками, проверками и техническим обслуживанием систем и приборов учета, финансовый/управленческий учет и аналитику для поиска утечек электроэнергии.

Сейчас большинство этих подсистем находится на этапе ввода в эксплуатацию; планируется, что все они заработают в полном объеме уже в этом году. Кроме того, на нынешний год намечено подключение новых потребителей и перенос на новую платформу системы документооборота.

Правда, не обошлось без проблем, которые, впрочем, никак не касаются СПО, а характерны для многих проектов внедрения нового ПО. Как отметил Сергей Дударев, основные трудности были связаны с нежеланием персонала менять привычный стиль работы, а также с тем, что при планировании внедрения не были в полной степени учтены все процессы. Из-за этого произошло отставание от плана примерно на три месяца, хотя в бюджет уложиться удалось. Делясь опытом, Сергей Дударев посоветовал больше внимания уделять планированию проекта и согласованию всех деталей, чтобы в дальнейшем избежать недопонимания.

СПО в коммерческом секторе

Хотя большинство представленных на конференции СПО-проектов были связаны с госструктурами, это не значит, что бизнес остался в стороне от общего тренда. Причины здесь такие же — дороговизна проприетарных решений и необходимость экономии.

Именно эти соображения подстегнули СКБ-Банк из Екатеринбурга к поиску СПО для создания интеграционной шины класса Enterprise Service Bus. "На тот момент в банке уже было решение, которое всех устраивало, но оно дорого стоило, да ещё нужно было расширять систему и докупать лицензии, а цены в связи с ростом курса валюты очень выросли", — рассказал Андрей Савиных, руководитель проектов СКБ-Банка.

К тому же, по его словам, нужно было переделывать имевшуюся систему, так как она перестала справляться с возросшей нагрузкой. Поэтому было решено перейти на СПО, тем более что СКБ-Банк уже имел опыт в области Open Source: почти все сотрудники работали с LibreOffice.

Как рассказал Андрей Савиных, нужен был полнофункциональный коробочный СПО-продукт от одного вендора с возможностью поддержки, с большим количеством внедрений, способностью к масштабированию и к тому же не требовательный к аппаратным ресурсам. Рассмотрев продукты WSO2, MULE ESB и Apache ServiceMix, банк выбрал последний.

Но не обошлось без проблем. По словам Андрея Савиных, трудно было найти интегратора, который согласился бы помогать во внедрении на приемлемых условиях. К сожалению, эта проблема характерна для Open Source в России. У нас пока еще мало компаний, оказывающих услуги по доработке, кастомизации, внедрению и сопровождению открытых решений. Видимо, причины здесь рыночные: заработать на бесплатном ПО непросто. Этот вопрос также обсуждался на ROSS'2016.

С трудом найдя интегратора, СКБ-Банк приступил к внедрению Apache ServiceMix, добавив из системы JBoss Fuse компании Red Hat несколько дополнительных модулей для администрирования и мониторинга, а также средства разработки, тестирования и отладки.

Чтобы накопить опыт и минимизировать риски, пояснил Андрей Савиных,

внедрение началось с процессов с небольшим количеством сообщений. Сейчас охват постепенно расширяется. На втором этапе планируется доработать ядро, внедрить кластеризацию и другие сервисы.

Рассматривая плюсы и минусы СПО, Андрей Савиных отметил, что открытое ПО работает не хуже проприетарных решений, не является особо сложным и обеспечивает высокую производительность. Но нужно быть готовым к тому, что придётся изучать большой объем документации на английском языке, а также к возникновению нештатных ситуаций, для которых не всегда можно со 100%-ной гарантией быстро найти решение. Правда, он добавил, что и с проприетарными продуктами у банка были подобные проблемы.


Александр Беляев

В качестве рекомендаций он посоветовал компаниям обзавестись квалифицированными специалистами, способными развивать и поддерживать СПО-систему, постоянно повышая свою квалификацию. А для начала желательно найти интегратора, который может оказать помощь в первых проектах и в поддержке платформы. Кроме того, внедрение стоит начинать с наименее критичных сервисов, расширяя систему по мере накопления опыта.

Ответом со стороны интеграторов, продвигающих СПО, стало выступление Александра Беляева, руководителя направления Open Source компании КРОК, который привел в пример решение по виртуализации, построенное на базе СПО oVirt.

По его словам, проект начался с того, что одна крупная компания решила продлить поддержку на систему виртуализации VMware, но оказалось, что нужно заплатить порядка миллиона долларов. Ради экономии было решено поискать решение на базе СПО с аналогичным функционалом и сертификатом ФСТЭК.

КРОК предложила в качестве замены продукт oVirt, который по архитектуре и возможностям похож на VMware. Масштаб системы большой: порядка 100 Тб данных, 50 серверов, 20 устройств в SAN-сети. Но судя по расчетам, экономия достигнута немалая: переход на новое решение обошёлся заказчику примерно в 20 млн. руб. против миллиона долларов за поддержку VMware.

"Мы выполнили адаптацию и доработку по регламенту ФСТЭК. Сейчас проходит сертификация", — рассказал Александр Беляев. Делясь опытом, он рекомендовал при внедрении СПО действовать аккуратно, с применением тестовой среды, потому что продукты очень по-разному документированы. С ними нужно тщательно разбираться, чтобы понять, как они работают, и при реализации проекта всё отрабатывать заранее.

Что касается сертификации, не стоит полагаться на то, что открытый код проще сертифицировать, чем закрытый. "В нашем решении используется столько разных продуктов, что нам потребовалось собрать массу документов, необходимых для сертификации", — пояснил Александр Беляев.

Помимо внедрения системы у заказчика КРОК получила еще один результат: построенный продукт было решено оформить в виде коробочного решения Z/Virt, передать его в Реестр российского ПО, получить сертификат ФСТЭК и использовать в других проектах.

Как превратить СПО в активы

С увеличением масштаба использования СПО перед организациями встает задача управления этим хозяйством. А между тем, по словам Олега Фатеева, координатора OpenStack в России, этому вопросу пока уделяется мало внимания.

Для проприетарных продуктов уже сложилась практика управления ими как программными активами организации с помощью решений класса Software Asset Management (SAM). А в области Open Source пока царит анархия, хотя то, что ПО открытое и бесплатное, не значит, что его не надо учитывать и контролировать. Так, по последним данным компании Black Duck Software, которая регулярно проводит аудит организаций, у половины из них отсутствовали GPL-лицензии, у 75% оказались модули с неизвестными лицензиями, у 95% — модули вообще без исходных кодов и, что самое интересное, почти у всех (98%) обнаружилось неизвестное пользователям СПО.


Олег Фатеев

Как считает Олег Фатеев, когда речь идет об активах, нужно рассматривать совокупную стоимость владения. Здесь главное преимущество открытого ПО по сравнению с проприетарным заключается в экономии на стоимости лицензий, которая позволяет получить выгоду при приобретении и масштабировании систем. Однако затраты на специалистов для СПО могут оказаться выше, поскольку от них требуется более высокая квалификация. Если компания строит корпоративные решения на базе Open Source, эти нюансы необходимо учитывать.

Важен и вопрос лицензирования. Лицензия GPL является одной их самых сложных, в том числе и по сравнению с любыми проприетарными лицензиями, и к тому же не единственной для Open Source. Поэтому в случае применения СПО организации приходится оперировать различными лицензиями и разными их редакциями.

К счастью, СПО уже полностью легализовано в Гражданском кодексе России. Если раньше этого не было, то сейчас есть понятие открытой лицензии, лицензионного договора по упрощенной форме и безвозмездного использования. В результате СПО полностью соответствует законодательству РФ, что имеет очень большое значение.

Олег Фатеев порекомендовал применять для СПО-активов системы SAM с открытым кодом, так как странно было бы для управления СПО использовать проприетарные продукты. Таких систем довольно много, но они различаются по функционалу, так что при выборе следует иметь в виду, что вам нужно: просто ли инвентаризация или управление исходными кодами.

Но в любом случае необходимо серьезно относиться к управлению СПО-системами, поскольку государство все больше внимания обращает на лицензирование ПО. По словам Олега Фатеева, уже 8 тыс. офицеров МВД прошли обучение в этой сфере.

Безопасность АСУ ТП: лед тронулся?

ЕЛЕНА ГОРЕТКИНА

В последние годы все больше внимания вызывают вопросы информационной безопасности АСУ ТП на предприятиях и критически важных объектах. Эксперты объясняют это рядом факторов, главный из которых — **БЕЗОПАСНОСТЬ** целый ряд целенаправленных атак на подобные объекты и высокая стоимость возможного ущерба. Ведь стороннее вмешательство в технологические процессы может вызвать не только аварии, но и настоящие катастрофы.

В нашей стране актуальность этой темы также растет. Немалую роль здесь сыграл интерес к ней со стороны регулирующих органов. К тому же уже нельзя не учитывать и набирающую силу тенденцию к распространению Промышленного Интернета вещей.

Как эти события влияют на текущую ситуацию в области обеспечения безопасности АСУ ТП в нашей стране? Какова специфика этого направления и его перспективы? На эти и другие вопросы отвечают представители компаний, специализирующихся в области создания и внедрения ИБ-решений.

Ситуация меняется

Уже не один год говорится о том, что создавшееся положение в сфере безопасности АСУ ТП оставляет желать много лучшего. Но сейчас, по мнению большинства экспертов, здесь наметились позитивные сдвиги. Говорить о кардинальных переменах еще рано, но уже ведутся и планируются к запуску проекты разной степени глубины — от первоначальных аудитов состояния ИБ до комплексных проектов по внедрению средств защиты в промышленных системах.

Дмитрий Даренский, начальник отдела промышленных систем компании "Информзащита", объясняет это тем, что большинство операторов и владельцев систем уже осознали, что защищенность АСУ ТП все же влияет на экономические показатели деятельности предприятий.

Кроме того, безопасности в данной области в последнее время уделяется больше внимания из-за растущей интеграции между промышленной и бизнес-инфраструктурой и прихода в мир АСУ ТП классических ИТ. Однако, по мнению Дмитрия Ярушевского, руководителя отдела кибербезопасности АСУ ТП компании "ДиалогНаука", у этой медали есть и обратная сторона: "Когда безопасность становится модным трендом, качество предоставляемых услуг и продуктов неизбежно страдает".

Так, иногда проявляется тенденция подбирать и внедрять ИБ-продукты и сервисы, основываясь не на результатах анализа угроз и рисков защищаемого техпроцесса и АСУ, а по каким-либо иным соображениям. Кроме того, многие вендоры анонсируют свои продукты как предназначенные для защиты АСУ ТП, хотя это в лучшем случае все те же корпоративные системы защиты информации, "завернутые" в промышленные защищенные корпуса с парой новых сигнатур. При этом сохраняется привычный для корпоративных систем акцент на конфиденциальность, необходимость постоянных обновлений и доработки конфигураций. А это не совсем то, что нужно для защиты АСУ ТП, работающих в режиме 24/7/365.

Да и сами предприятия уделяют внимание безопасности АСУ ТП далеко не в полном объеме. Как отметил Павел Коростелев, менеджер отдела продвижения продуктов компании "Код безопасности", государство постепенно усиливает надзор в этой области, но до тех пор, пока за несоответствие требованиям регуляторов не будет введено серьезных санкций, тема будет развиваться очень неспешно. Он видит две основные причины тому. Первая — риск влияния средств защиты на технические процессы. Люди, ответственные за промышленную безопасность, слишком хорошо понимают опасность внедрения в инфраструктуру дополнительных элементов. Вторая причина связана с отсутствием реальных инцидентов в сфере безопасности. Пока не наберется "критическая масса" конкретных примеров влияния рисков ИБ на работоспособность технологических систем, их владельцы не будут считать такой риск существенным и не станут снижать его.

Евгений Дружинин, старший эксперт отдела безопасности промышленных систем управления компании Positive Technologies, согласен с тем, что исторически ИБ для АСУ ТП всегда играла роль скорее мешающего элемента. Однако, по его мнению, к сегодняшнему дню на практике доказано, что множество систем управления обладают уязвимостями, которые могут повлиять на основную функциональность. Благодаря этому стало формироваться понимание важности роли ИБ как одной из ключевых составляющих безотказной работы АСУ ТП.

Еще одна проблема связана с тем, что на рынок выходят интеграторы, не очень компетентные в области защиты АСУ ТП, что не только не уменьшает риски, но, наоборот, может и добавить их. Эту проблему отметил Олег Кузьмин, директор департамента информационной безопасности компании "Ай-Теко": "На наш взгляд, на предприятиях, эксплуатирующих АСУ ТП, целесообразно периодически проводить оценку необходимости и достаточности принимаемых мер по этим вопросам и своевременно корректировать действия по совершенствованию ИБ-системы. Но для этого требуются крайне специфические знания в области функционирования АСУ ТП и умение разбираться в общих организационно-технических вопросах. А большинство системных интеграторов, предлагающих в настоящее время услуги по обеспечению безопасности АСУ ТП, по сути, не могут их оказывать в требуемом объеме при таком качестве работ, которое устроило бы заказчика, и практическая польза от подобных услуг будет весьма сомнительной".

Безопасность безопасности рознь

Так в чем же заключается специфика обеспечения безопасности в области АСУ ТП? Чем подходы и решения в этом сегменте отличаются от используемых для защиты традиционных ИТ-систем и что у этих направлений общего?

По единодушному мнению экспертов, различия в обеспечении безопасности АСУ ТП и традиционных ИТ-систем настолько существенны, что общим является разве что само слово "безопасность". В вопросах ИБ АСУ ТП много специфичных особенностей, начиная с принципиальных технических и функциональных различий между ИТ-системами и системами автоматизации, равно как и в определении их критичности, и заканчивая несходством методик проведения работ по аудиту, проектированию, внедрению и эксплуатации систем защиты.

По мнению Дмитрия Ярушевского, главная специфика этой области заключается в том, что защищать необходимо не саму АСУ, не информацию в ней, а управляемый технологический процесс: "Об этом зачастую забывают. В корпоративных системах мы привыкли иметь дело с информацией, научились оценивать риски для бизнеса, связанные с нарушением ее конфиденциальности, целостности и доступности. Достаточно понять, откуда информация берется, куда поступает, как и где обрабатывается и хранится, а затем разработать модель нарушителя, установить в нужных местах средства защиты — и можно спать спокойно. Конечно, я утрирую, но в общем виде это примерно так и выглядит".

Для сравнения он предложил представить производственную площадку горно-металлургического комбината: восемь цехов и тридцать участков технологических процессов, объединенных общим бизнес-процессом. Количество различных АСУ ТП здесь может превышать сотню. Останов одних систем может привести к останову всей линии производства и многомиллионным убыткам, искажение данных в других — к выпуску бракованной продукции, а нарушение работы третьих повлечет даже выброс в атмосферу ядовитых веществ. Поэтому, прежде чем подступаться к вопросам обеспечения безопасности, специалисту необходимо понять, какие угрозы и риски вообще существуют во всех этих АСУ и как реализация этих угроз может повлиять на отдельные участки технологических процессов и на производство в целом.

Предположим, специалист, разобравшись в принципах работы, архитектуре и выявленных уязвимостях этих систем, выяснил, что один из самых "тонких" с точки зрения безопасности участков — это установленные в цехе HMI-пульты, с которых осуществляется управление неким оборудованием. Доступ к ним имеют все работники цеха, а это около тысячи человек, использующих один общий логин/пароль, запрашиваемый только при перезапуске оборудования. Но очевидный вариант — создать для каждого оператора персональные учетные записи — не годится, так как в масштабах всего предприятия совокупные потери времени на аутентификацию будут слишком велики. Нужны альтернативные решения, которые зависят от архитектуры, используемого оборудования и ПО целевой АСУ ТП.

Евгений Дружинин считает, что из всех задач главная заключается в обеспечении безотказности и прогнозируемости выполнения функций по управлению АСУ ТП, остальные имеют более низкий приоритет. Однако стандартные механизмы защиты, привычные миру ИТ, напрямую здесь неприменимы, а иногда даже опасны из-за сложной и зачастую устаревшей архитектуры используемых систем.

Даниил Тамеев, руководитель направления по работе с ПиТЭК Центра информационной безопасности компании "Инфосистемы Джет", в качестве главного аспекта защиты технологических сегментов промышленных объектов выделил доступность, а не характерные для корпоративного сегмента конфиденциальность и целостность. Задачу обеспечения безопасности усложняет и то, что основная часть систем, являющихся объектом защиты, функционирует в режиме реального времени, а значит, даже малейшие задержки в работе, вызванные наложенными средствами защиты, недопустимы.

По мнению Олега Кузьмина, основная специфика обеспечения ИБ в АСУ ТП заключается в первую очередь в необходимости понимания общей организации производства, задач, решаемых с использованием АСУ ТП, управленческих и технологических процессов на предприятии, вопросов промышленной безопасности, а также в приоритетности стоящих задач, которые существенно отличаются от тех, что существуют в традиционных ИТ-системах.

Тем не менее эксперты усмотрели некоторое сходство в том, что для защиты АСУ ТП необходимо выстроить процессы, хорошо знакомые в мире ИТ: оценка рисков, управление рисками, доступом, инцидентами и т. д. Используемые принципы тоже схожи: сегментирование сетей, предоставление минимальных прав пользователям, регистрация событий и пр. Однако, отметил Дмитрий Ярушевский, важно помнить, что практическая реализация этих процессов и принципов может сильно отличаться от реализации их в корпоративных информационных системах.

К тому же, несмотря на сходство в логике защиты, стратегия обеспечения безопасности АСУ ТП значительно сложнее, чем для ИТ-систем. "Необходимо обладать широкими компетенциями, чтобы понимать последствия развертывания и функционирования подсистем ИБ в действующей АСУ ТП. Многие работающие в АСУ ТП операционные системы и приложения могут быть несовместимы с коробочными ИБ-продуктами, а системных ресурсов может просто не хватить для средств ИБ", — предупреждает Павел Коростелев.

Действия государства

Помимо сложности самих систем организацию защиты АСУ ТП затрудняет ряд проблем, главной из которых эксперты считают дефицит госрегулирования. Важное значение в сфере госрегулирования имеет выпущенный в 2012 г. документ "Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критично важных объектов инфраструктуры РФ" ▸

Наши эксперты

ДМИТРИЙ ДАРЕНСКИЙ, *начальник отдела промышленных систем, "Информзащита"*

ЕВГЕНИЙ ДРУЖИНИН, *старший эксперт отдела безопасности промышленных систем управления, Positive Technologies*

ПАВЕЛ КОРОСТЕЛЕВ, *менеджер отдела продвижения продуктов, "Код безопасности"*

ОЛЕГ КУЗЬМИН, *директор департамента информационной безопасности, "Ай-Теко"*

ДАНИИЛ ТАМЕЕВ, *руководитель направления по работе с ПиТЭК Центра информационной безопасности, "Инфосистемы Джет"*

ДМИТРИЙ ЯРУШЕВСКИЙ, *руководитель отдела кибербезопасности АСУ ТП, "ДиалогНаука"*

и приказ ФСТЭК России № 31, изданный в 2014-м.

Эксперты положительно оценили появление этих документов, но посетовали на то, что вся нормативно-правовая база носит лишь рекомендательный характер. "Хотя приказ ФСТЭК № 31 заставил владельцев АСУ ТП обратить внимание на безопасность промышленных систем, большинство из них до сих пор воспринимают его довольно поверхностно в силу отсутствия методологических материалов и необязательности выполнения требований самого приказа", — сформулировал общее мнение Евгений Дружинин.

Поэтому эксперты считают, что данного приказа недостаточно для кардинального улучшения ситуации, и связывают ожидания с планами регулятора по его доработке и совершенствованию нормативно-правой базы.

Так, по мнению Дмитрия Ярушевского, нужны глубокие концептуальные документы, описывающие, что именно, от чего и как необходимо защищать; как оценивать риски и как управлять ими. Нужна гибкая и детальная система классификации АСУ ТП или отдельных частей, определение того, какие требования следует применять к различным сегментам АСУ ТП, какие процессы следует выстроить у заказчика, какие подразделения должны отвечать за обеспечение безопасности и так далее.

Необходима также переработка базовой модели угроз и методики определения актуальных угроз с учетом специфики АСУ ТП и применяемых технологий. "Иными словами, работы непочатый край. Этим уже не один десяток лет занимаются зарубежные коллеги, и их опытом и разработанными документами стоит воспользоваться", — считает Дмитрий Ярушевский.

Что обязательно нужно, так это более подробные документы и методические рекомендации, детально описывающие способы выполнения требований регулятора. "Тематика защиты АСУ ТП такова, что исполнители проектов должны обладать широким кругозором, и чем детальнее будут описаны требования регулятора по организации защиты, тем легче их будет выполнять", — уверен Павел Коростелев.

К тому же 31-й приказ ФСТЭК — верхнеуровневый документ, а для учета уникальной специфики АСУ ТП в зависимости от той или иной отрасли нужны отраслевые стандарты. По словам Евгения Дружинина, уже существует ряд околоотраслевых стандартов, но они "заточены" не столько под отрасль, сколько под конкретную специфику предприятий, таких как "Газпром" или ФСК ЕЭС: "Данный вопрос может быть относительно легко решен через создание отраслевых рабочих групп, включающих производителей систем, операторов, интеграторов и специалистов по ИБ".

Реакция предприятий

Поскольку госрегулирование еще только набирает обороты, владельцы предприятий не торопятся реализовывать серьезные ИБ-проекты по защите АСУ ТП, так как не понимают, какую выгоду они получают от такого рода вложений. Отчасти это связано с тем, что оценка возможных финансовых убытков вследствие ИБ-инцидентов еще в новинку для риск-менеджмента и не входит в зону ответственности службы ИБ. Из-за этого риски возможного воздействия на АСУ ТП катастрофически недооцениваются. Например, существует классическое заблуждение, что подобные системы отделены от внешнего мира и поэтому безопасны. А без четкого понимания рисков трудно обосновать необходимость запуска сложных и дорогих ИБ-проектов на промышленных объектах.

Поэтому большинство предприятий идут по пути наименьшего сопротивления и минимальных затрат — например, повышают защищенность систем за счет реализации организационных и компенсирующих мер. И это уже хорошо. По мнению Дмитрия Даренского, практика показала, что такие меры способны значительно повысить уровень защищенности систем.

Ведь на многих предприятиях существуют серьезные организационные проблемы. Например, зачастую непонятно, в чью же зону ответственности подпадает безопасность АСУ ТП и кто должен решать эти задачи. Одни подразделения кивают на другие, и в худшем случае этим вопросом вообще никто не занимается. В результате технологи работают с АСУ, построенной внешними подрядчиками в соответствии с их пониманием безопасности, а безопасники обеспечивают защиту физического периметра предприятия и информации в корпоративной сети.

"До тех пор пока у заказчиков, подрядчиков, и регуляторов не сложится определенного понимания, в чьей именно зоне ответственности находится обеспечение безопасности АСУ ТП, и пока бизнес не поймет, насколько это действительно важно, ситуация кардинально не изменится", — считает Дмитрий Ярушевский.

Это мнение разделяет Павел Коростелев, который отметил, что изменить ситуацию может либо ужесточение законодательства, либо достаточное количество подтверждений того, насколько серьезно уровень безопасности АСУ ТП влияет на такие риски, как ущерб окружающей среде, здоровью и жизни людей, повреждение оборудования и нарушение непрерывности технологических процессов.

Поможет ли импортозамещение?

Курс нашего государства на импортозамещение оказывает влияние на самые разные аспекты применения ИТ, в том числе и на защиту АСУ ТП. Так, Дмитрий Даренский заметил, что именно после объявления этого курса крупные российские производители средств обеспечения безопасности начали заявлять о выпуске на рынок специализированных продуктов для защиты АСУ ТП. И хотя в промышленную эксплуатацию ни одно решение еще не введено, тем не менее интерес к ним со стороны рынка быстро набирает обороты, и вполне возможно, что уже в этом году появятся первые внедрения и первая реакция пользователей.

Благодаря политике импортозамещения отечественные разработчики получают преимущества на рынке перед иностранными конкурентами, но конкуренция продолжается. А что будет, если, обязав всех владельцев АСУ ТП использовать только отечественные разработки, устранить эту конкуренцию? Дмитрий Ярушевский сомневается, что это положительно отразится на качестве решений: "На мой взгляд, курс на импортозамещение должны держать не заказчики, а отечественные разработчики. Надо, чтобы они стремились создавать такие продукты, которые заказчики выберут вместо импортных. Этому и стоит посвятить бюджеты, направляемые сейчас на бездумное замещение китайского "железа" с европейским ПО на китайское же "железо" с доработанным СПО под российским названием".

В целом эксперты считают, что пока невозможно однозначно оценить, как именно повлияет политика импортозамещения на уровень обеспечения безопасности АСУ ТП. Значительная часть компонентов таких систем и средств их защиты разрабатывается в странах, присоединившихся к санкциям против России. Но из-за того, что заказчики недооценивают риски, из-за недостаточной строгости законодательства и сложной экономической ситуации спрос на эти средства невысок. Разработка российских средств защиты АСУ ТП, безусловно, нужна, но в силу чрезвычайной трудоемкости она должна быть экономически оправданна.

Типовые проблемы в организации информационной безопасности АСУ ТП

При подготовке обзора опрошенным нами экспертам было предложено перечислить типовые проблемы в организации ИБ АСУ ТП, с которыми им приходилось сталкиваться на стадии предпроектного обследования объектов. В обобщенном виде ответы экспертов представлены ниже.

- Отсутствие какой-либо организации в решении вопросов безопасности АСУ ТП. Зачастую само понятие информационной безопасности АСУ ТП на объекте не используется и ответственность за ее обеспечение ни на кого не возложена.
- Нормативная база по ИБ плохо проработана или вообще отсутствует, нет и организационно-распорядительной документации по обеспечению ИБ в АСУ ТП, а корпоративные процессы и процедуры безопасности эту систему не затрагивают.
- Отсутствие требований по ИБ или их несоблюдение со стороны персонала, эксплуатирующего промышленные системы.
- Низкий уровень компетенции в вопросах ИБ у специалистов по автоматизации, проектированию, внедрению, эксплуатации, обслуживанию.
- Слабая осведомленность в вопросах автоматизации у специалистов по ИБ.
- Частичное или полное отсутствие документации на используемую АСУ ТП. Система в эксплуатации не первый десяток лет, документы потерялись, было много доработок, люди, стоявшие у истоков, уволились, и теперь никто толком не знает, как она работает.
- Непонимание целей проведения работ, расхождение между утвержденным заданием и ожиданиями заказчика, а также отсутствие понимания между функциональными подразделениями. При этом попытки наладить взаимодействие различных подразделений предприятия не предпринимаются.
- Неконтролируемый доступ к технологическим системам и отсутствие контроля за действиями подрядчиков и используемыми каналами удаленной связи с разработчиками АСУ ТП.
- Устаревшее технологическое и ИТ-оборудование.
- Отсутствие антивирусной защиты, каких-либо обновлений и контроля съемных носителей в технологической среде, использование устаревших ОС.

А с этим могут быть проблемы. С одной стороны, импортозамещение решает вопрос доверия к АСУ ТП, но с другой — порождает множество других, в том числе касающихся защищенности самих АСУ ТП. Это связано с тем, что зачастую разработчики отечественных систем, не имеющие крупных внедрений и выстроенного канала дистрибуции, не могут конкурировать с крупными зарубежными производителями по многим пунктам. И ключевой задачей при создании АСУ ТП остается их функциональное наполнение, а все остальные вопросы, касающиеся в том числе безопасности, решаются по остаточному принципу.

Поэтому важно, чтобы курс на импортозамещение не только давал толчок к массовому внедрению уже имеющихся систем, но и заставлял производителей повышать качество и конкурентоспособность своих решений.

Новые технологии — новые угрозы

Вслед за появлением Интернета вещей (IoT) в мир производства пришла концепция Промышленного Интернета вещей (IIoT), направленная на объединение промышленных производственных систем на уровне технологических процессов, интеллектуальных машин и систем управления. Идея состоит в том, чтобы исключить человека из ряда процессов, повысить производительность и обусловить рост экономики.

Очевидно, распространение Промышленного Интернета вещей так или иначе повлияет на подходы к обеспечению безопасности АСУ ТП. Но, по единодушному мнению экспертов, это дело будущего, так как предприятия пока не понимают, что это такое и зачем нужно.

Как считает Дмитрий Даренский, IIoT является результатом попытки объединить две концепции — Интернета вещей и Промышленного Интернета: "Эта попытка мне кажется не совсем удачной, потому что направлена на объединение концепций, индустриальной и потребительской".

Тем не менее сейчас для данных концепций полным ходом идут разработки стандартов, в том числе и в области обеспечения кибербезопасности. Этим занимаются специально созданные консорциумы, такие как Industrial Internet Consortium, основанный в 2014 г. компаниями IBM, Cisco, General Electric, Intel и AT&T. В Германии это делается в рамках программы "Industry 4.0", а в Китае — в рамках государственной программы "Internet+".

В России также предпринимаются попытки создать консорциум Промышленного Интернета. Возглавляет эту работу "Ростелеком" при поддержке Минпромторга. Эксперты надеются, что со временем их действия помогут сформировать спрос на такие технологии со стороны предприятий, и готовы включиться в эту работу, так как сама тема имеет перспективу в нашей стране, хотя и более отдаленную, чем в остальном мире.

Как всякая новинка, Промышленный Интернет вещей влечет за собой и новые угрозы. Ведь IIoT затрагивает вопросы построения умного производства, интеграции АСУ ТП с другими системами (ERP, MES, PLM), позволяющими воздействовать на весь производственный цикл. Всё это создает дополнительные риски, и их недостаточная проработанность с точки зрения ИБ рано или поздно может отразиться на реальном производстве.

Эксперты уверены, что, несмотря на некоторую отсталость в применении новых технологий и сильную изношенность промышленного оборудования, тема IIoT через некоторое время будет актуальна и для российских предприятий. "Более или менее серьезно это направление безопасности начнет обсуждаться и, возможно, развиваться не раньше чем через два-три года", — сформулировал общее мнение Олег Кузьмин.

Самая большая...

ПРОДОЛЖЕНИЕ СО С. 6

значительные средства, маловероятно, что в ближайшем будущем произойдет прорыв в области инструментов, который облегчит очистку данных. Следует ожидать их последовательного улучшения.

2. Подготовка данных становится одним из направлений науки о данных. Подобно помощникам юристов, которые решают важные частные вопросы, те, кто занят подготовкой данных, могли бы делать примерно то же самое для специалистов по данным. В определенном смысле это уже происходит.

3. ИИ поможет очистке данных. Возможно также, что будут созданы ПО и алгоритмы для очистки, сортировки и категоризации данных. Это обязательно произойдет, но следует также ожидать, что это не станет универсальным решением. Microsoft, IBM и Amazon делают ставку на использование людей для маркировки данных, с чем не может справиться ПО. А это три ведущие корпорации мира в области автоматизации и написания алгоритмов.

Как обеспечивается кибербезопасность российских АЭС

НИКОЛАЙ НОСОВ

В последнее время в СМИ стали часто появляться сообщения о хакерских атаках на физические объекты. В связи с этим возникает вопрос: насколько защищены наши атомные электростанции? Об этом и о других предметах,

ИНТЕРВЬЮ

*связанных с кибербезопасностью АСУ ТП атомных станций, мы расспросили **Вадима Подольного**, заместителя технического директора, директора департамента разработки ПО и кибербезопасности компании "Русатом — Автоматизированные Системы Управления".*

PC Week: Может ли хакер проникнуть в одну из подсистем АЭС и, например, поднять стержни, вызвав расплавление активной зоны или аварию типа Чернобыльской?

ВАДИМ ПОДОЛЬНЫЙ: АСУ ТП атомной электростанции находится в изолированной сети и от Интернета отключена. Никто не может подключиться к АСУ ТП и начать нелегитимно управлять АЭС, например, отдавать команды на извлечение регулирующих стержней — за это отвечает система безопасности АЭС, работающая на строго заданных алгоритмах.

PC Week: Как выглядит архитектура кибербезопасности АЭС?

В. П.: У АЭС, как и у любого крупного промышленного объекта автоматизации, можно выделить логически пять контуров кибербезопасности. В первом находятся все датчики, подключенные к программно-логическим контроллерам (ПЛК).

Во втором контуре информация с ПЛК собирается и приводится в единообразный вид. Это так называемый шлюзовой контур, в нем находится шлюзовое оборудование. В нем же собираемая информация обрабатывается и передается в локальную сеть системы верхнего блочного уровня (СВБУ).

Третий — контур оперативного управления. В нем находится СВБУ, с которой взаимодействует оператор, управляющий технологическим оборудованием АЭС.

Четвертый — контур неоперативного управления. В нем автоматизированные рабочие места (АРМ) снабжены средствами визуализации технологических процессов, но лишены возможности управления. За данными АРМ работают технологи, отвечающие за конкретную подсистему АЭС. Связь технологов с операторами по месту обеспечивается по изолированным каналам в голосовом режиме.

И, наконец, пятый контур — контур внешнего доступа. Он предназначен для сопряжения с кризисным центром, в который поступает информация о состоянии АЭС через протокол удаленного доступа без возможности управления.

Все контуры изолируются друг от друга различными мерами.

PC Week: Но получается, что у АЭС есть внешний канал связи с кризисным центром?

В. П.: Да, есть. Эта связь идет по автономным, изолированным от Интернета каналам связи. Кризисный центр предназначен для мониторинга параметров работы АЭС в различных режимах эксплуатации систем.

PC Week: Недавно сообщалось, что отключение 23 декабря 2015 г. электричества в большей части Ивано-Франковской области Украины было вызвано хакерской атакой на компьютерные сети "Прикарпатьеоблэнерго". Четвёртого января аналитики американской iSIGHT Partners, занимающейся вопросами безопасности, получили примеры вирусного кода и подтвердили, что именно он стал причиной инцидента. Компонент KillDisk, использованный в атаке, включал в себя дополнительные функции, которые не просто делали перезагрузку компьютера невозможной, но блокировали АСУ производством электроэнергии, намного усложняя

Вадим Подольный

ее восстановление. Может ли подобное случиться на наших АЭС?

В. П.: Всегда легко во всем обвинить хакеров. Если произошёл какой-либо технологический сбой, то конечно же удобно сказать, что это сделал хакер. Ведь кто такой хакер? Инженер, который решил стать злоумышленником. Хакер, способный осуществить какое-то реальное вредоносное воздействие и несанкционированный доступ к информации хотя бы на чтение, — это инженер, который, для того чтобы получить доступ хотя бы к пятому контуру, должен отлично знать, как устроены механизмы подключения к нему. А значит, это внутренний нарушитель. Или он когда-то работал у нас и получил необходимую информацию. Мы считаем, что в случае АЭС потенциальный внешний нарушитель маловероятен. Этим мы руководствуемся при разработке моделей угроз, модели нарушителя и соответственно модели защиты.

PC Week: Ну а если сисадмин станции решил поработать удаленно и кинул к себе домой VPN-канал? А его домашний компьютер уже находится под внешним управлением…

В. П.: Начиная с третьего контура сетевая структура АСУ ТП АЭС — это обычная сеть. Обычные коммутаторы, маршрутизаторы. Просто их технологическое исполнение подразумевает, что они должны выдерживать больше нагрузок с точки зрения внешних факторов, чем бытовые устройства. Но с точки зрения коммутации — это обыкновенное сетевое оборудование. Все это оборудование полностью изолировано от внешних сетей подключения, так что VPN подключать просто некуда.

PC Week: А как же с разнообразной отчетностью для регуляторов? Данные по налогам, отчеты в Пенсионный фонд. И должна же проходить на АЭС электронная почта?

В. П.: Да, на АЭС есть офисная сеть, например для документооборота и т. д. Там используется обычное бытовое оборудование. С промышленной сетью АСУ ТП она вообще никак не сопрягается. Они изолированы друг от друга на физическом уровне. Офисная сеть также изолирована от Интернета.

PC Week: А что насчет флэшек? Предположим, сотруднику АЭС пришло домой зараженное письмо, он его открыл и случайно заразил свою флэшку. А потом воткнул ее в компьютер в сети на работе. И таким образом перенес туда зловредный код.

В. П.: В контурах управления у нас используются сертифицированные операционные системы на базе Linux. Исследовать Linux на уязвимости намного проще, чем Windows, как и проще выпустить дистрибутив с отключенными теми или иными функциями. То есть снизить число уязвимостей на этапе проектирования намного проще.

Флэшку в компьютеры на АЭС просто так не засунешь. Есть специальные помещения, в которых размещается оборудование, к которому можно получить доступ только согласно установленным процедурам. Когда станция работает в режиме эксплуатации, доступ к USB-порта отсутствует. Помещения и компьютеры защищены системами физической защиты, имеются специальные организационные процедуры, которые регламентируют все работы с точки зрения информационной безопасности.

PC Week: А если это не просто хакеры, а спецслужбы других государств, использующие закладки на уровне контроллера? Такие, как при кибератаке на ядерные объекты Ирана в 2009–2010 гг., когда из 19 тыс. центрифуг по обогащению урана около тысячи было выведено из строя?

В. П.: Правильней говорить не "закладка", а "недекларированная возможность" (НДВ). Это может быть не просто закладка, приводящая к сбою, а код, приводящий к некорректной работе алгоритмов управления. Для нас важнее корректность работы программного обеспечения — платформы, прошивок контроллеров, коммутаторов, маршрутизаторов. Из-за их некорректной работы, например, может нарушиться работа промышленной сети.

АЭС — огромный объект с самым разнообразным оборудованием. Есть и иностранное, потому что не всё производится в России. Но все ключевые системы безопасности сейчас российской разработки, в том числе с использованием иностранной электронной компонентной базы.

НДВ могут быть везде. В процессоре, в контроллере, в сервере, в маршрутизаторе, коммутаторе и планшете. НДВ могут быть в более высокоуровневом ПО, в операционных системах, прошивках оборудования. Да, ПО сертифицировано, но ни один разработчик не в состоянии провести полную ревизию исходного кода. Есть ПО, которое осуществляет непосредственно управление. Мы понимаем, что и туда злоумышленник может внедрить НДВ, которые в самый ответственный момент активируются.

Страшно не то, что произойдет сбой, который приведет, например, к останову реактора, а когда специально подстроено, чтобы система неправильно себя вела таким образом, чтобы вывести из строя дорогостоящее оборудование. Когда НДВ будет завышать или занижать показатели, некорректно воспроизводить алгоритм управления. Предположим, реализована атака для занижения мощности реактора на 10%. На самом деле реактор уже достиг 100%-ной мощности, а алгоритм управления продолжает повышать её. Аварии при этом не произойдёт, реактор будет остановлен, но его простой стоит очень дорого. Падает КПД АЭС (коэффициент использования установленной мощности, КИУМ). Это фактически прямой удар по прибыли.

От НДВ можно защититься глубоким анализом исходного кода, который мы стараемся получать от производителей оборудования, а также умением самостоятельно прошивать все используемые контроллеры, коммутаторы и маршрутизаторы и прочее оборудование.

Абсолютно всё импортозаместить невозможно. Поэтому наша основная задача — сделать из недоверенных компонентов доверенную систему. Именно так ставится вопрос о кибербезопасности АЭС и подобных объектов во всем мире.

PC Week: И как можно этого добиться?

В. П.: Один из механизмов обеспечения кибербезопасности — собственная программная платформа, разрабатываемая нашей компанией для сопряжения всех устройств, транспорта данных и визуализации технологических процессов в виде мнемосхем, графиков и других графических примитивов, генерации отчетов и т. д. У нас есть и аппаратная платформа, разрабатываемая предприятиями ГК Росатом. С помощью нашей программно-аппаратной платформы мы и собираем из недоверенных компонентов доверенную систему, где есть все механизмы сопряжения оборудования, синхронизации данных, визуализации технологических процессов и т. д.

Основным плюсом является то, что нашу платформу мы можем верифицировать с помощью тренажеров и симуляторв. Кроме стандартных исследований исходного кода на кибербезопасность, статического и динамического анализа, тестов на проникновение мы еще и сравниваем в различных режимах эксплуатации реальную систему и её модель на симуляторе на предмет расхождения контролируемых параметров. Если злоумышленник захочет разместить в системе НДВ, то ему придется это сделать не только на рабочей платформе, но и на симуляторе. А они работают на разных принципах и на разном ПО. Это гораздо сложнее, чем взломать одну систему.

С точки зрения технологического развития решений мы исследуем возможность промышленного применения систем анализа большого объема структурированных данных, machine learning, систем искусственного интеллекта, предсказывающих динамику развития событий в АСУ ТП АЭС и подсказывающих оператору алгоритм действий в тех или иных ситуациях, например, экспертной системы поддержки принятия решения (СИПО).

PC Week: В чем специфика кибербезопасности АСУ ТП?

В. П.: Основная угроза кибербезопасности АСУ ТП — воздействие на технологический процесс. Если заранее знаешь, как он должен протекать, то защитить его идеологически намного проще, чем компьютер домохозяйки, которая не планирует своих действий.

Объект АЭС нельзя защитить внешней "нашлепкой". Система должна обладать естественной функцией внутренней защиты. Нельзя забывать, что технологический объект прежде всего должен работать, не должна падать скорость, снижаться эффективность из-за "нашлепок", обеспечивающих кибербезопасность. В отличие от офисных сетей никакие блокирующие воздействия на компоненты АСУ ТП подсистемы кибербезопасности осуществлять не имеют права, это может привести к аварии.

PC Week: Куда движется рынок кибербезопасности АСУ ТП?

В. П.: Рынок движется к разработке программных решений, позволяющих анализировать прошивку контроллера как черного ящика. Многие производители еще не готовы к тому, чтобы открывать исходный код прошивок своих контроллеров. Но мы обязательно придем к тому, что на критически важные объекты типа АЭС такие контроллеры покупать не будут. Хочешь поставить контроллер — покажи исходный код. Потребитель всегда должен иметь возможность прошивку перепрошить.

С точки зрения кибербезопасности программного обеспечения рынок движется к созданию систем, работающих в псевдореальном времени с такой же скоростью, с какой работает АСУ ТП, и располагающих средствами анализа промышленных протоколов. Не факт, что это спасёт, как с помощью анализа трафика понять, хороший это пакет или плохой? Тем не менее как дополнительная сигнализация такие системы могут быть использованы.

Услуги, которые сейчас могут потребоваться на атомном рынке, — наработка кейсов, необходимых для включения в такие документы, как модель угроз и модель

ПРОДОЛЖЕНИЕ НА С. 15 ▸

Электронный документооборот: конец эпохи или новые возможности?

СТАНИСЛАВ МАКАРОВ

Скорость изменений в политике и бизнесе очень велика, поэтому к системам управления сегодня предъявляются повышенные требования. От СЭД/ECM-систем, которые для многих стали привычным инструментом, клиенты ОБЗОРЫ ждут большей гибкости, динамичности, интеллектуальности. В нашем тематическом обзоре мы обсудим вопрос адекватности современных СЭД/ECM-решений как важного инструмента управленческой практики сегодняшним и завтрашним бизнес-реалиям. Примет ли индустрия вызов рынка, трансформируя популярные продукты, чтобы придать им новые качества, или на смену им придут другие системы? Своими мнениями на сей счет делятся наши эксперты.

Сможет ли СЭД изменить бюрократию?

СЭД реализуют бюрократическую парадигму управления, которая, по сути, не может быть гибкой и эффективной. С другой стороны, ИТ, на которых построены СЭД, несут в себе потенциал управленческих изменений. Как разрешается этот парадокс?

"Мы претерпеваем цифровую трансформацию, которая непосредственно влияет на подходы к управлению организациями, когда вместо управленческой вертикали строится "плоское предприятие" в виде совокупности самоуправляемых и сотрудничающих команд и СЭД должны ответить на изменение объекта управления, — уверен Владимир Андреев, президент компании "ДоксВижн". — Некоторые ростки нового мы уже наблюдаем: появилась поддержка Case Management, простое управление процессами "по шаблонам", поддержка проектных команд и рабочих групп. Но изменяться мы должны активнее".

Сама СЭД может стать катализатором изменений в организации — об этом говорит Владимир Недобой, директор центра интеграционных решений RedSys: "Парадокс на самом деле состоит в том, что избыточность и сложность своих бюрократических процессов организации, не готовые к реинжинирингу, но желающие автоматизировать свою документно-ориентированную деятельность, могут осознать только с внедрением информационной системы. Несмотря на большую сложность таких проектов, в результате у прогрессивных руководителей появляется возможность максимально объёмно показать все неоптимальности в работе и практически мгновенно продемонстрировать положительный результат от изменения процессов".

Устремляясь навстречу новому, нельзя в то же время игнорировать свой исторический багаж. СЭД возникли и развивались в целях автоматизации служб документационного обеспечения управления (ДОУ), и это продолжает оказывать влияние на их архитектуру и набор функций. "Основными пользователями и бизнес-заказчиками СЭД на протяжении многих лет являлись сотрудники служб ДОУ, поэтому системы строились на основе привычной им метафоры бумажного документооборота. Такой подход стал своего рода наследуемой особенностью СЭД, подчас тормозящей работу квалифицированного персонала и руководителей всех уровней, — признает Вадим Ипатов, заместитель генерального директора компании "ИнтерТраст" по развитию бизнеса. — Бюрократизм традиционных СЭД приводит к тому, что большая часть профессионалов предпочитает решать вопросы неформально, оставляя недокументированными важные решения и деловые активности. В итоге бизнес-процессы остаются за рамками СЭД. Чтобы изменить ситуацию, необходимо обеспечить взаимодействие пользователей в рамках сквозных деловых процессов, в границах компании, холдинга или между независимыми организациями. Это позволит сместить фокус СЭД/ECM от функций регистрации и учета к прямому участию в создании бизнес-ценностей и "научить" СЭД сохранять новые виды информации: обмен мнениями, неформальные документы, информационные материалы, документированный ход принятия решений и т. д.". Он считает, что для этого можно и нужно использовать средства персонализации контента и интерфейса, которые позволяют создавать функционально-ориентированные рабочие места с учетом профессиональной специализации сотрудников и формировать рабочее пространство с развитыми средствами решения повседневных задач и инструментами горизонтального взаимодействия, а документооборот при этом становится фоновым технологическим сервисом.

Однако отрицать полезность СЭД было бы, пожалуй, преждевременно. Многие организации еще не вступили на путь цифровой трансформации, но тем не менее они озабочены вопросами повышения эффективности бизнес-процессов и качества управления, поэтому СЭД все так же востребованы и продолжают совершенствоваться. Елена Иванова, директор по маркетингу компании ЭОС, не согласна с заявленным постулатом, что СЭД не может быть гибкой и эффективной: "Системы, реализующие функции обработки документов, давно уже вышли далеко за рамки СЭД. Сегодня системы управляют всей корпоративной информацией, данными, знаниями, и только в частности — документами. А гибкость — это как раз один из главных критериев функционирования любой ИТ-системы, тем более сегодня, когда управленческие решения принимаются быстро и так же быстро должны исполняться".

Не видит в данном случае никакого парадокса и Александр Безбородов, руководитель отдела разработки программ документооборота "1С", потому что документ и в традиционном делопроизводстве, и в бизнесе подчиняется правилам. "Без согласования и утверждения договор не будет иметь силу, не выйдет на рынок новый продукт или услуга. Современная СЭД совместима с различными моделями управления и ориентирована как на поддержание традиционной ("бюрократической") модели, основанной на вертикальной иерархии, разделении труда и четкой регламентации деятельности, так и на гибкие, адаптивные управленческие структуры, разновидностями которых являются проектные формы управления. СЭД могут концентрировать много ценной информации и предоставляют инструменты для работы с процессами, их мониторинга и оптимизации. Если компания хочет быть эффективной, то СЭД ей в этом только поможет", — заключает эксперт.

"Говорить, что СЭД реализует какую-то конкретную модель управленческих процессов, не совсем верно, — считает Артем Пермяков, руководитель проектов внедрения компании Directum. — В первую очередь СЭД является инструментом, позволяющим автоматизировать существующие бизнес-процессы предприятия. Если они бюрократичны и неэффективны и переносятся в СЭД без изменений, то тогда действительно можно говорить о реализации бюрократической парадигмы. Но такой подход к внедрению СЭД неэффективен в принципе. Внедрение СЭД неотделимо от консалтинга, направленного на изменение процессов, на отсечение всего лишнего. Совокупность технических решений, услуг по внедрению позволяет СЭД менять сложившуюся систему управления".

Особенности рынка в период зрелости

Рынку СЭД уже более двадцати лет, он достиг зрелости — функционально все системы стали довольно похожими. Тем не менее заказчики по-прежнему сталкиваются с проблемой выбора продукта, но прежние подходы, основанные на сопоставлении чек-листов наличия тех или иных функций, перестают работать. Какие критерии выходят сегодня на первый план при выборе СЭД?

На зрелом рынке человеческий фактор имеет приоритет перед чисто технологическим, но успех гарантирует только их удачная комбинация. Елена Иванова констатирует, что сегодня на первые места выходит уровень профессионализма команды внедренцев, гибкий подход вендора к заказчику и проекту, уровень сервиса, гибкое лицензирование, мобильные приложения, безопасность данных и работы, динамичное развитие системы. Ее поддерживает Владимир Недобой, он также признает, что системы во многом похожи, никакого решительного преимущества в функциональности одних перед другими нет. Для заказчиков должен быть важен опыт конкретной компании или даже конкретной команды, её подходы к решению задач, аналогичных вашим, методологии управления проектами. И если не рассматривать ценовой аспект, отбросить специфические технические требования, то можно сказать, что система в общем-то вторична, поэтому заказчикам при выборе поставщика нужно ориентироваться на опыт, который всегда уникален. При этом далеко не очевидно, что вы найдёте своего идеального поставщика среди грандов рынка, говорит он.

По мнению Александра Безбородова, основным критерием для клиентов попрежнему остается максимальная адаптация системы под требования бизнеса вкупе с реализацией традиционного делопроизводства, интеграция СЭД с любыми существующими информационными системами, в первую очередь с ERP, а также тесный контакт с вендором, чтобы получать информацию о планируемых изменениях и иметь возможность сообщить о пожеланиях напрямую разработчику программы.

Аналогичным образом думает и Владимир Андреев: "Для заказчиков сейчас на первом месте уровень готовности системы к использованию, цена и сроки внедрения. Однако не менее важна и возможность "подстройки" готового решения под свою специфику, желательно самостоятельно". Вместе с тем г-н Андреев отмечает некоторые перемены в поведении заказчиков, которые сегодня не пытаются найти решение "всё в одном" и охотно приобретают "изолированные" приложения — главное, чтобы они легко интегрировались. Роль консалтинга при внедрении снижается, поскольку предметные компетенции воплощаются в готовом продукте. Однако требования к интеграции с различными системами предприятия, в первую очередь с ERP, растут, отмечает эксперт.

Разумеется, нельзя всех стричь под одну гребенку. Артем Пермяков акцентирует внимание на разных категориях заказчиков: "Важно понимать, о каких заказчиках мы говорим. Для крупного бизнеса основное значение имеет производительность СЭД, возможность одновременной работы тысяч и десятков тысяч пользователей в распределенной среде. Важны для крупных структур и вопросы информационной безопасности. Средний и малый бизнес ориентируется в первую очередь на функциональность "коробки", благодаря чему достигается экономия на внедрении". При этом вне зависимости от масштаба общим критерием выбора для всех заказчиков является интерфейс, его современность, простота, удобство, дружелюбность и понятность, заключает он.

При прочих равных — когда технические характеристики, функциональное богатство и профессионализм консультантов достигли высокого уровня, — поведение заказчиков становится исключительно прагматичным. "Если мы уславливаемся говорить о приблизительном равенстве функций, то определяющим фактором остается цена: по-прежнему этот момент часто перевешивает все остальные", — признает Дмитрий Шмайлов, начальник отдела развития ECM-решений компании ЭЛАР. Системы часто выбираются также исходя из опыта коллег по отрасли, личных предпочтений руководителей или привычек ключевых сотрудников. При дальнейшей проработке обращают внимание на качество поддержки конкретной системы в конкретном регионе, потому что лишние затраты и простои

ПРОДОЛЖЕНИЕ НА С. 14 ▸

Наши эксперты

ВЛАДИМИР АНДРЕЕВ, *президент, "ДоксВижн"*

АЛЕКСАНДР БЕЗБОРОДОВ, *руководитель отдела разработки программ документооборота, "1С"*

ЕЛЕНА ИВАНОВА, *директор по маркетингу, ЭОС*

ВАДИМ ИПАТОВ, *заместитель генерального директора по развитию бизнеса, "ИнтерТраст"*

ЮРИЙ КОРЮКИН, *генеральный директор, "ABBYY Россия"*

ВЛАДИМИР НЕДОБОЙ, *директор центра интеграционных решений, RedSys*

АРТЕМ ПЕРМЯКОВ, *руководитель проектов внедрения, Directum*

ДМИТРИЙ ШМАЙЛОВ, *начальник отдела развития ECM-решений, ЭЛАР*

Итерационное сокращенное внедрение СЭД, или Давай сделаем это по-быстрому

ВЯЧЕСЛАВ ФИЛИППОВ

Время заставляет поставщиков и заказчиков ИТ-решений быть умнее. Реалии рынка дали толчок к развитию такого неординарного и местами рискованного варианта внедрения, как ***итерационное сокращенное:*** быстро, качественно и в рамках малого бюджета.

Подготовка

Приступая к новому проекту, мы снова оказались перед выбором, как внедрять. На входе мы имели: разнородные блоки процессов, короткие сроки, небольшой бюджет и учет затрат в еженедельных табелях, двух участников от исполнителя (руководитель проекта и бизнес-аналитик в одном лице; разработчик), заранее обученного администратора DIRECTUM, дружелюбного и открытого заказчика, а также твердое намерение сделать всё как можно лучше.

От максимального каскадного и итерационного внедрения отказались сразу — дорого и долго. Внедрение сокращенное (учесть все требования, не зная, чего хочется) — тоже нет, хотя уже ближе. В итоге приняли решение опробовать минимальный по затратам и срокам вариант — внедрение с поэтапным вводом процессов в опытно-промышленную эксплуатацию (ОПЭ).

Внедрение

Первое, что было сделано, — проведены исследование процессов и примерная оценка, насколько "коробка" справится с поставленными задачами. Параллельно рабочая группа прошла обучение основам работы в системе DIRECTUM.

Следующий этап — проектирование и адаптация системы. От тотального документирования отказались, описание решений носило минимально необходимый характер и всё делалось параллельно и попроцессно, чтобы можно было тут же приступить к настройке.

Как был выстроен процесс "подгонки" системы под заказчика.

1. Исследование процессов у заказчика. Изучались текущие процессы по каждому блоку. Результаты документировались по-быстрому, "от руки". В итоге получили первоначальные схемы процессов "как есть", общее понимание, как все устроено, и познакомились с основными исполнителями.

2. Оценка применимости "коробки" и первоначальная проработка решения. Детально прорабатывались и разбирались схемы, полученные на первом этапе. Далее они перестраивались с учетом стандартных возможностей DIRECTUM и повторно демонстрировались заказчику. Так мы выясняли, правильно ли поняли друг друга и насколько внесенные изменения "ложатся" на процессы. На выходе получали первоначальные схемы процессов "как будет".

3. Демонстрация и обсуждение схемы процессов "как будет". Главная задача — принять окончательное решение, как будут выглядеть процессы. Участникам выдавались распечатанные схемы, а сам алгоритм рисовался на доске с объяснением каждого этапа. В результате таких совещаний рождалась итоговая схема работы.

4. Настройка и адаптация системы. Полученная схема работы реализовывалась в СЭД. Параллельно готовились инструкции пользователей.

5. Демонстрация работы в системе DIRECTUM для всех участников процесса. Цель демонстраций — показать, как людям предстоит работать, и морально настроить на то, что это скоро случится. Параллельно собирались замечания, которые тут же либо отклонялись, либо брались в работу.

6. Опытно-промышленная эксплуатация. Чем больше процессов было запущенно, тем большее их количество приходилось одновременно поддерживать команде внедрения. Однако это балансировалось тем, что основные замечания по предыдущим блокам к моменту запуска следующего обычно уже были исправлены. С каждым днем и сам заказчик становился все опытнее, и "бытовые" консультации перекладывались на плечи ответственных.

По такой схеме была проведена работа по каждому из четырех блоков автоматизируемых процессов. Нам удалось значительно сократить трудоемкость и длительность проектирования за счет исключения процессов документирования и длительного согласования.

Проблемы и рекомендации

Проект был закончен раньше запланированного срока и с приличной экономией бюджета. Однако такой подход таит в себе определённые риски:

• *Ошибки в проектировании, появление новых и изменение существующих требований*. Для исключения ошибок подробно разбирали все принимаемые решения и требования. Делали всё, чтобы рабочая группа до конца поняла, что будет в результате, и продумала все варианты использования. К слову, доработок и изменений после запуска в ОПЭ было немного.

• *Разногласия с заказчиком во время ОПЭ по поводу того, что делаем, а что нет*. Чтобы нивелировать этот риск, постарались установить доверительные взаимоотношения с заказчиком. Вдобавок к этому активно прививали понимание, что всё и сразу реализовать в рамках ограничений проекта мы не сможем.

• *Замечания от пользователей из-за укороченной ОПЭ и отсутствия тестовой эксплуатации*. Проблема решалась детальным устным обсуждением на этапе проектирования, а также подготовкой заказчика к тому, что доработка и развитие системы будут продолжаться и после окончания проекта внедрения.

Несмотря на все сложности, методология может использоваться и быть эффективной, если имеем:

• небольшой бюджет и сжатые сроки;

• относительно малое количество пользователей СЭД;

• согласие заказчика подстраиваться под стандартные возможности системы, а не только адаптировать ее под процессы;

• отсутствие бюрократии и быстрое принятие решений;

• возможность предоставить удаленный доступ к СЭД (в противном случае при таком варианте внедрения выполнять работы будет затруднительно);

• возможность и желание заказчика уделять проекту не менее 50% своего времени, а также идти на компромиссы;

• способность команды внедрения на протяжении всего проекта работать в активном режиме — параллельные работы, постоянное взаимодействие с заказчиком, сжатые сроки.

Необходимость соответствовать индивидуальным ожиданиям и потребностям заказчика заставляет снова и снова придумывать новые подходы к реализации проектов, искать места, где можно сэкономить, решать, как сделать все "по-быстрому" и на достойном уровне. Поэтому к выбору варианта внедрения и путей сокращения нужно подходить с головой и индивидуально в каждом конкретном случае.

Автор статьи — руководитель проектов внедрения DIRECTUM.

Электронный...

◂ ПРОДОЛЖЕНИЕ СО С. 13

никому не нужны. А кроме того, сейчас все чаще смотрят на происхождение продукта, отмечает эксперт.

"По понятным причинам для многих заказчиков важным становится вопрос построения импортонезависимой среды для управления документами, — говорит Вадим Ипатов. — Есть организации, которым эта тема интересна исключительно в контексте сокращения издержек на приобретение лицензий, в то время как другие ставят целью создание доверенной информационной среды. Сегодня можно выделить еще один явный тренд всего российского рынка ИТ: разработка с применением СПО. В текущей экономической ситуации это логичное направление развития корпоративных систем, в том числе и СЭД".

Необходимо сказать, что на рынке СЭД импортозамещение произошло практически естественным путем: изначально в силу ориентации заказчиков на автоматизацию российской бюрократии спрос на отечественные системы был выше. Сейчас из-за курса национальной валюты и политической ситуации крен в сторону отечественных СЭД только усилился. (Справедливости ради следует отметить, что СЭД и ECM, строго говоря, синонимами не являются. И санкции распространяются далеко не на все российские предприятия. Поэтому западные вендоры по-прежнему ведут крупные проекты в России, автоматизируя различные бизнес-процессы, не всегда связанные с традиционным документооборотом.)

Ловушка морального износа

Известное правило айтишников "работает — не трогай" может сыграть злую шутку с любой ИТ-системой, в том числе и с СЭД, где к этому добавляется еще мощный консерватизм пользователей, не желающих менять процессы документооборота, чтобы двигаться в ногу со временем. Поэтому, несмотря на то, что разработчики постоянно выпускают обновления своих продуктов, через 5—10 лет после внедрения многие клиенты задумываются о замене "старой" СЭД вследствие ее морального износа. Как избежать этой ловушки?

Вадим Ипатов уверен, что избежать морального износа можно только одним способом: искать прогрессивные технологии и новые способы работы с контентом, выявлять порой еще неочевидные запросы клиентов. "Рынок СЭД уже не раз переживал технологические переломы. Появление потокового сканирования, потребность заказчиков в распределенных СЭД, развитие BPM-инструментов, бум мобильных приложений — таковы лишь некоторые вехи, — напоминает эксперт. — По нашим оценкам, технологические новшества, за которыми следует очередной этап развития рынка СЭД, появляются каждые 3—5 лет". Однако основной потенциал развития СЭД г-н Ипатов связывает с обеспечением поддержки различных моделей управления. В этой части перспективным подходом считается адаптивный кейс-менеджмент (Adaptive Case Management, ACM), позволяющий в отличие от традиционных инструментов BPM быстро реагировать на меняющиеся условия.

Но одних только усилий разработчика недостаточно, чтобы поддерживать СЭД в актуальном состоянии. Большая доля ответственности лежит и на самом заказчике — ведь нужно планировать развитие своей системы и регулярно ее обновлять. Распространённый среди автомобилистов подход "купить и пользоваться, пока работает" в случае ИТ не годится — потому что софт устаревает быстрее, чем любое "железо", и одним только техобслуживанием тут не обойтись, часто требуется глубокая модернизация.

"Парадокс состоит в том, что за 5—10 лет сама платформа, на которой функционирует СЭД заказчика, тоже очень сильно изменяется, — комментирует проблему Владимир Андреев. — Поэтому если не делать регулярных обновлений, получается, что по трудоемкости миграция "через пять версий на текущую" сравнима с внедрением новой системы. Это, наверное, нормально, это здоровая конкуренция вендоров, потому что на замороженном рынке неоткуда взяться инновациям. Ловушки морального износа можно избежать, если постоянно развивать свою систему, решать на ней новые задачи, увеличивать ROI, вовремя обновляться. Такая тактика правильна во всех случаях, даже если вы будете переходить на альтернативную платформу, то успеете амортизировать старую задолго до перехода".

Лояльный и дисциплинированный заказчик, который регулярно покупает техподдержку и устанавливает все обновления, — мечта любого вендора. Однако даже этот путь не гарантирует клиенту, что его СЭД будет адекватна реалиям нынешнего дня. Ведь при таком подходе вся ответственность за стратегию развития системы перекладывается на ее создателей, но кто может поручиться, что команда идет верным курсом?

На этот риск обращает внимание Артем Пермяков: "Некорректно выбранный вендором путь развития системы может быть источником проблем. Если при выпуске новых версий разработчик не учитывает современные управленческие и технологические тренды, то его система, пусть даже последних версий, с каждым годом все больше устаревает. Поэтому и переход заказчиков на новые версии не приносит желаемого эффекта". Второй фактор, на который указывает эксперт, — отказ заказчика от обновления системы — тоже имеет место, здесь г-н Пермяков согласен с Владимиром Андреевым. Причины отказа могут быть разные: "отсутствие ресурсов на обновление", "и так все устраивает"… Данный подход к сопровождению и развитию системы неизбежно приведет к ее моральному устареванию. Таким образом, рецепт, позволяющий избежать морального износа, — постоянное взаимодействие с вендором, направленное на передачу ему пожеланий к функциональности решения, и постоянное развитие и обновление системы внутри предприятия.

Развитие ИТ в целом не происходит строго поступательно и эволюционно. Время от времени появляются прорывные инновации, которые перекраивают весь пейзаж рынка. "Говоря о моральном износе, не всегда имеется в виду только лишь сам продукт. Даже если он меняется и обновляется, на рынке всегда появляются принципиально новые решения, с новым интерфейсом и новым концептуальным подходом, на основе более мощной платформы, что не обеспечишь модернизацией давно работающей системы", — замечает Елена Иванова. Кроме того, есть эффект привыкания: команда, которая изначально была ориентирована на завоевание клиента, со временем может расслабиться и перестать оказывать клиенту должное внимание. "Как этого избежать? На мой взгляд, нужно плотно работать с клиентом", — резюмирует она.

Тем не менее миграции клиентов с платформы на платформу неизбежны. Нет такой силы, которая могла бы их навечно привязать к одному вендору. Об объективных причинах смены поставщика СЭД рассказывает Дмитрий Шмайлов: "Внутренние процессы и их регламент в компаниях меняются, и это в любом случае требует затрат на доработку существующих систем. Новый продукт — это гарантированная адаптация к новым ▸

реалиям. К тому же конкуренция растет, и внедрение новых продуктов часто обходится даже дешевле поддержки старых. Есть огромное количество примеров, когда из-за взлета курса доллара компании, использующие зарубежное ПО, попали в "ловушку сопровождения" — цена сопровождения оказалась неподъемной, а неуплата ведет к штрафам при возобновлении отношений; если деньги не платятся, то система устаревает. В такой ситуации многие предпочли переход на аналогичное российское ПО".

Не стоит сбрасывать со счетов и субъективный фактор. Как отметил Вадим Ипатов, переход на новую систему намного чаще связан с ротацией кадров, чем с моральным износом. Меняется руководство или приходит новая ИТ-команда со своими идеями относительно того, на базе каких продуктов должны автоматизироваться те или иные процессы. Поэтому нередко технологии и прикладные системы кочуют из одной организации в другую вместе с их приверженцами.

Вообще говоря, с моральным износом не все так однозначно — тут есть определенная доля лукавства. Владимир Недобой указывает, что есть заказчики, вполне успешно работающие на системах, которые можно назвать морально устаревшими в технологическом плане: с устаревшими архитектурами, с не самыми модными технологиями. Есть и те, кто перевнедряет некоторые свои системы каждые 3—5 лет, обосновывая это в том числе моральным устареванием. В каждом случае нужно разбираться детально, но, скорее всего, дело здесь опять же не в самой системе, а в качестве и полноте внедрения. Неполное внедрение значительно повышает риск сноса системы, например, при смене руководителя, и никакие современные технологии не будут страховкой от этого. Со временем любая система, любой продукт устареют, и, конечно, нужно выпускать новые версии, инвестировать перспективные разработки, чтобы к моменту окончания жизненного цикла одного продукта у вас было что-то интересное для рынка. Чтобы управлять этим риском, нужно иметь своё решение, и компании-разработчики, ориентирующиеся только на создание решений на базе платформ и средствами, предоставляемыми платформами, рискуют потерять свой рынок, когда вендор снимет с пробега конкретную платформу, признав её морально устаревшей, или при смене лицензионной политики, или, как сейчас, в силу внешних политических и экономических факторов, которые никто и прогнозировать не мог.

Искусственный интеллект заставит СЭД поумнеть

Искусственный интеллект (ИИ) вышел из лабораторий и начинает активно использоваться в разных задачах в бизнесе. Компьютер давно обыграл человека в шахматы, но сможет ли он сделать такую простую вещь, как регистрация входящего документа в СЭД и направление его нужному исполнителю? Что вообще эта технология может дать рынку СЭД/ECM?

"Технологии искусственного интеллекта позволяют обрабатывать неструктурированные данные, то есть ту область, где привычные системы, основанные на статистике и правилах, не очень эффективны. Они могут быть настроены на конкретные бизнес-задачи, такие как извлечение и анализ информации из массивов текстовых данных, автоматическое распределение документов на основе их смысла по департаментам или ответственным внутри компании (например, обращений граждан или запросов клиентов) и конечно же улучшение корпоративных систем поиска, — говорит Юрий Корюкин, генеральный директор "ABBYY России". — Такие технологии предоставляют бизнесу наиболее точные и полные данные, чтобы принимать решения быстро и объективно, снижать финансовые и операционные риски благодаря тому, что вся необходимая информация имеется под рукой. В дальнейшем это приведет к появлению новых инструментов на рынке СЭД/ECM для решения задач контентной аналитики на принципиально ином уровне".

Другие отрасли двинулись по пути интеллектуализации раньше, чем СЭД, поэтому риски оказаться первопроходцем в этом деле не так велики, а выгоды можно получить значительные, вплоть до полной замены офисных сотрудников роботами. Так, один из крупнейших японских банков Mitsubishi UFJ Financial Group начал своего рода эксперимент, в ходе которого сотрудниками по работе с клиентами одного или двух отделений стали гуманоидные роботы Nao, созданные французской робототехнической компанией Aldebaran Robotics. Но если роботизация — дело пусть и не слишком отдаленного, но все-таки будущего, то автоматизация документооборота на основе ИИ возможна уже в наши дни.

"Сегодня в классические СЭД приходят технологии искусственного интеллекта, используемые в других сферах, где они имеют гораздо более определяющее значение. Например, технологии автоматической классификации и индексирования неструктурированных документов уже несколько лет применяются банками в кредитных конвейерах и для обработки документов операционного дня, заменяя ручной ввод", — говорит Дмитрий Шмайлов. Другое направление — встраивание в СЭД интеллектуального поиска в дополнение к реквизитному, когда система подсказывает сотруднику, что запрашиваемое наименование фигурирует в текстах других документов, в том числе за пределами СЭД.

Нас, конечно, впечатляет, что в 2013 г. шесть компьютеров IBM Watson были "трудоустроены" в клиники США в качестве диагностов, где ИИ вполне успешно справляется с задачей подбора оптимальной тактики лечения, работая вместе с врачами-людьми. Однако революция едва ли произойдет очень быстро. Искусственному интеллекту еще предстоит многому научиться, чтобы освоить разные человеческие профессии.

Да, ИИ вышел из лабораторий в сегмент B2C, но в корпоративные решения он только еще приходит, отмечает Владимир Андреев. "В ближайшие 3—5 лет, наверное, не будет ни одной СЭД, не интегрировавшей в себе технологии интеллектуальной категоризации, интеллектуального поиска и поддержки базы знаний (не просто хранилища данных, а семантических объектов, фактов и связей), — уверен он в скором техническом прогрессе. — Вендоры к этому готовы, дело за спросом со стороны заказчиков. Но поскольку современный пользователь уже привык к интеллектуальным функциям в своем смартфоне, он очень скоро начнет требовать того же самого и от приложений. Этот эффект мы наблюдали несколько лет назад в форме "дайте нам поиск, как в Google": сегодня уже почти все такой поиск своим пользователям дали".

Транзакционный документооборот — близкая задача, но уже не СЭД

Количество первичных документов, сопровождающих цепочки поставок и финансовые операции, на несколько порядков превышает число обычных документов, а бизнес-процессы здесь протекают весьма интенсивно. На первый взгляд с технической стороны вроде все то же самое — есть документы, которые надо хранить в системе, заполнять карточки реквизитами, маршрутизировать и т. д. Но при этом документооборот, связанный с обработкой транзакционных документов, имеет свои особенности. Прежде всего это тесная интеграция с ERP, обеспечение юридической значимости, необходимость извлечения данных из образов и многое другое. Нужно ли считать его отдельным рынком или это просто разновидность СЭД?

На взгляд Владимира Андреева, транзакционный документооборот — это отдельный рынок, в большинстве случаев примыкающий к ERP. Однако для ERP сам договор в виде текста вообще не является документом, никаких транзакций он не порождает. Поэтому договорной документооборот, связывание с договором переписки, истории согласования и других взаимодействий внутри предприятия и с контрагентом все-таки лучше автоматизировать в СЭД. В составе ERP обычно есть свои модули управления документами, но конкуренция между ними и СЭД искусственная, она происходит чаще всего от непонимания разницы в назначении систем. Вместо этого надо беспокоиться об интеграции, считает эксперт.

Дмитрий Шмайлов указывает еще на одно важное отличие этого класса систем от СЭД: "Транзакционность может подразумевать автоматический обмен систем данными, проведение операций без участия человека, включение в процесс третьей стороны и многое другое. Частично эти свойства используются в ЭДО, BPM, СМЭВ и т. д. Однако это отдельные задачи, отличающиеся от классического документооборота как с точки зрения их технической реализации, так и в части законодательного регулирования".

Действительно, говоря об автоматизированной обработке электронных счетов-фактур и накладных, о сдаче налоговой отчетности, электронных госуслугах или о других подобных вещах, мы подразумеваем, что документооборот выходит за границы одного предприятия. Поэтому Антон Пермяков полагает, что межкорпоративный документооборот — это отдельный динамично развивающийся рынок, назвать который разновидностью СЭД нельзя, так как здесь решаются абсолютно разные задачи. СЭД обеспечивают качественное внутреннее взаимодействие сотрудников, управление контентом предприятия, а сервисы межкорпоративного документооборота — быстрое и дешевое взаимодействие между разными предприятиями; но интеграция этих систем позволит повысить эффективность работы каждой из них и предприятия в целом.

Как обеспечивается...

ПРОДОЛЖЕНИЕ СО С. 12

защиты. Мы должны иметь возможность до проектирования системы и закупки оборудования собирать все требуемые документы из разных кусочков — базы данных уязвимостей, инцидентов, угроз. И делать это на основе общемирового опыта. Именно это позволит автоматизировать процесс анализа требований к защищенности и разработке кибербезопасности критически важных объектов (КВО).

А кроме того, надо понимать, что сама по себе система кибербезопасности АСУ ТП работать не может. Она должна иметь точки сопряжения, чтобы инженеры, разрабатывающие комплексные промышленные системы автоматизации, могли обеспечить глубокую интеграцию и взаимодействие с ней.

Еще один общий тренд — сопряжение большего количества подсистем КВО с АСУ ТП. Подсистема кибербезопасности будет плотно интегрирована с системами контроля и управления доступом, пожарной безопасности, видеонаблюдения и др. Перспективными являются системы комплексного анализа безопасности и сопряжения с компонентами защиты информации, глубоко интегрированными внутрь аппаратно-программной платформы АСУ ТП, такими как авторизация, идентификация, разграничение доступа и разработка соответствующей комплексной политики кибербезопасности.

PC Week: Спасибо за беседу.

ПОДПИШИСЬ

СК ПРЕСС

PCWEEK RUSSIAN EDITION

Подписаться на бумажную версию газеты PC Week можно в агентстве
ООО "Агентство "Урал-Пресс"" 8 (495) 789-86-39

НА 2016 ГОД

БЕЗОПАСНОСТЬ

Тематический раздел-портала PC Week Live

Блог
Форум
Статьи
Новости
События
White papers

pcweek.ru/security