CIO·RU

Вестник цифровой трансформации

№5 ИЮНЬ 2017

Директор

информационной службы

ЗОДЧИЕ ЦИФРОВОЙ ЭКОНОМИКИ

АЛЕКСЕЙ ЛЕБЕДЕВ, ПРЕЗИДЕНТ АССОЦИАЦИИ РАЗВИТИЯ КОРПОРАТИВНОЙ АРХИТЕКТУРЫ, ГЛАВНЫЙ АРХИТЕКТОР БАНКА «ОТКРЫТИЕ»

СОСЕДИ ПО ЦИФРОВИЗАЦИИ: ПРИМЕР КАЗАХСТАНА

МАРКЕТИНГ, ОСНОВАННЫЙ НА ДАННЫХ

ОНЛАЙН-КАССЫ: ЧАС «ИКС»...

ITMF 2017: В РОССИЮ – С СЕРВИСНЫМ ПОДХОДОМ

ДЕЙСТВУЮЩИЕ ЛИЦА / БАНК «ОТКРЫТИЕ»

14 ЗОДЧИЕ ЦИФРОВОЙ ЭКОНОМИКИ

АЛЕКСЕЙ ЛЕБЕДЕВ, ПРЕЗИДЕНТ АССОЦИАЦИИ РАЗВИТИЯ КОРПОРАТИВНОЙ АРХИТЕКТУРЫ, ГЛАВНЫЙ АРХИТЕКТОР БАНКА «ОТКРЫТИЕ»

АЛЕКСЕЙ ЕСАУЛЕНКО

Читайте в следующем номере

- Lattelecom: Большие Данные проживают за границей
- «Яндекс»: как работать с исследователями данных
- Благополучие сотрудников как KPI
- «Северсталь - Центр Единого Сервиса»: трансформация как сервис
- ОМК: религия ITSM
- «Райффайзенбанк»: agile-подход должен стать моделью работы всей организации, а не только ИТ-службы
- Цифровая трансформация HR в «Юлмарте»: полный переход от бумажного документооборота к ЭДО
- Поэлементный анализ себестоимости в «Трансмашхолдинге» на основе BI

ИТ-рынок

Российский рынок ИСУП начнет восстанавливаться с 2019 года

IDC опубликовала исследование, посвященное российскому рынку информационных систем управления предприятием – ИСУП. К нему аналитики традиционно относят приложения для управления ресурсами предприятия, цепочками поставок, операциями на производстве, взаимоотношениями с клиентами, а также приложения для бизнес-аналитики.

По данным IDC, в 2016 году объем рынка сократился на 1,1% – до 632,72 млн долл. При этом в рублевом выражении он вырос на 8,8%. Пятерка лидирующих поставщиков (SAP, «1С», Microsoft, Oracle, «Галактика») осталась прежней, тем не менее в целом российским поставщикам удалось немного улучшить свои позиции. В 2016 году по-прежнему две трети рынка приходилось на приложения ERP и BI.

Крупнейшими потребителями ИСУП остаются предприятия непрерывного производства и розничной торговли. Их совокупная доля на рынке составила около 44%. В 2016 году в пятерку вошли дискретное производство, сельское хозяйство, строительство и добывающая отрасль, а также энергетика.

Аналитики констатируют, что улучшение общей экономической ситуации хорошо сказалось и на всем рынке ИТ, и на этом сегменте. Как ожидается, среднегодовой темп роста рынка ИСУП до 2021 года будет положительным. Уже в 2019 году ожидается постепенное восстановление рынка.

Облака стали рассматриваться как гарантия безопасности

Объем рынка облачных сервисов в России по итогам 2016 года составил около 29 млрд руб. По оценкам TAdviser, лидирующие позиции – 46% рынка – заняли российские разработчики облачных решений, распространяющие свои сервисы как самостоятельно, так и через партнеров. Доля иностранных вендоров облачных решений составила 31%, а на долю интеграторов приходится 23% рынка.

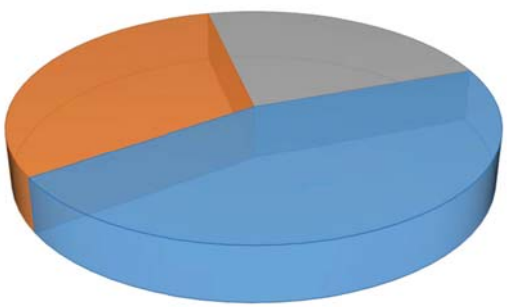
Среди западных вендоров основным игроком, по данным исследования, стал Microsoft с широким портфелем облачных сервисов Microsoft Azure, Office 365 и др., на долю которого пришлось около трети выручки (29%). Второе и третье места занимают IBM (18%) и Salesforce (14%).

Исследование также показало, что в России облако наиболее востребовано в ретейле, интернет-сервисах, FMCG и промышленности. Активно проникают облака в ИТ-компании, телеком, транспортную сферу и логистику. 64% опрошенных уже используют облачные сервисы. Те из них, кто выбрал иностранных провайдеров и готов раскрывать своего партнера, наиболее часто упоминают Microsoft (55%), Amazon (21%) и Google (16%).

Доминирующими критериями выбора поставщика в ходе опроса были названы стоимость сервисов (67%), а также опыт использования сервиса в отрасли или в аналогичной компании для решения похожих бизнес-задач (55%). Показательно, что, несмотря на все опасения по поводу риска потерять данные, 57% респондентов видят в облаках гарантию безопасности, обеспечиваемую провайдерами. В основном так думают представители среднего бизнеса (в том числе интернет-ретейла), а также поставщики интернет-сервисов и ИТ-компании, знакомые с требованиями и условиями соблюдения SLA.

Структура российского рынка облачных услуг

46% Локальные разработчики
31% Иностранные вендоры
23% Системные интеграторы



Источник: TAdviser, 2017

НЕ ПРОПУСТИТЕ

30 июня
«Шестая ИТ-ночь на Ивана Купалу – 2017»
Конференция
Ярославская область
Клуб ИТ директоров я-Ит-ы
http://ciocfo.ru/meropriyatiya/

5-7 июля
PG Day Russia
Конференция
Санкт-Петербург
PG Day Russia pgday.ru

4 августа
IT SUMMER FEST
Фестиваль
Калужская область, Никола-Ленивец
Парк «Никола-Ленивец»
itsummerfest.ru

Сентябрь
Практическая конференция «ITIL, DevOps, Agile: инструменты цифровизации»
Конференция
Москва
Издательство «Открытые системы», www.osp.ru

11 октября
«Мир ЦОД-2017. Услуги. Облака»
Конференция
Москва
Издательство «Открытые системы», www.osp.ru

26 октября
Smart Industry 2017
Конференция
Москва
Издательство «Открытые системы», www.osp.ru

29-30 ноября
«Технологии баз данных»
Конференция
Москва
Издательство «Открытые системы», www.osp.ru

Техника безопасности

Корпоративные сети Wi-Fi всегда уязвимы для хакеров

Во всех без исключения проектах по анализу защищенности исследователи Positive Technologies обнаружили проблемы с безопасностью, открывающие возможность атак через беспроводные сети компаний. Решить эти проблемы можно только путем комплексного подхода к обеспечению безопасности корпоративной инфраструктуры.

Одна из самых распространенных проблем безопасности корпоративных сетей Wi-Fi – использование словарных паролей, которые легко подобрать. С ними исследователи Positive Technologies сталкивались практически во всех проектах по анализу защищенности ИТ-инфраструктуры.

Кроме того, часто встречаются и ошибки конфигурирования сетей, расширяющие нарушителю возможности для проведения атак. К таким недостаткам безопасности относится отсутствие ограничения мощности сигнала беспроводных маршрутизаторов, в результате чего подключение к сети компании можно осуществлять вне контролируемой зоны – например, из соседнего здания или с парковки.

Часто бывает, что в компании ограничивают доступ сотрудников к Интернету, блокируют отдельные веб-ресурсы. Чтобы обойти такие ограничения, работники подключаются к нужным им сайтам со смартфонов. А для большего удобства они могут разворачивать на смартфоне беспроводную точку доступа, к которой подключают рабочую станцию и пользуются интернет-ресурсами через такое несанкционированное и никак не защищенное соединение. В ходе работ по анализу защищенности беспроводных сетей на каждом объекте в 2016 году выявлялись в среднем три несанкционированные точки доступа. В одной из компаний обнаружено сразу семь таких точек.

Как подчеркивают аналитики, отказываться от использования Wi-Fi не нужно, гораздо эффективнее – задействовать комплексный подход к обеспечению информационной безопасности. Важно заниматься повышением осведомленности сотрудников в вопросах безопасности, а также перекрывать потенциальные векторы атак на Wi-Fi – например, внедрять безопасные методы аутентификации с проверкой сертификатов, ограничивать доступ клиентов к гостевой сети, проводить регулярный анализ защищенности беспроводных сетей, выявлять и отключать несанкционированные точки доступа.

Словарные пароли делают неэффективными дорогие системы безопасности

Для атак на корпоративные информационные системы киберпреступники чаще всего используют несложные сценарии на основе известных уязвимостей. В случае успеха подобные атаки приводят к существенным финансовым и репутационным потерям. Positive Technologies выпустили исследование, в котором описали самые популярные сценарии атак.

В список вошли как простые атаки, не требующие специальных инструментов, так и более сложные – например, обход двухфакторной аутентификации, которая традиционно считается надежным методом защиты. В целом подобные сценарии атак позволяют экспертам компании получать полный контроль над локальной вычислительной сетью во всех проектах тестирований от лица внутреннего нарушителя, а при моделировании атаки внешнего нарушителя преодолеть периметр удается в 80% случаев.

Важно понимать, что используемые для атак пробелы защиты могут присутствовать в системе любой организации. При этом большинство атак вполне предсказуемы: каждый из описанных сценариев основан на эксплуатации наиболее распространенных уязвимостей, которые могут быть устранены с минимальными финансовыми вложениями, зачастую просто путем изменения конфигурации системы.

Эксперты также отмечают, что сложность компрометации ресурсов в значительной степени зависит от того, является ли подход к защите комплексным. Даже дорогостоящие решения по обеспечению безопасности могут оказаться бесполезными, если пользователи и администраторы ресурсов применяют словарные пароли. Было множество примеров, когда словарный пароль лишь одного пользователя позволял при атаке получить полный контроль над всей инфраструктурой корпоративной сети. Также было показано, что, имея привилегии локального администратора на рабочей станции или сервере, нарушитель может использовать специализированные утилиты для получения учетных данных даже при наличии антивируса.

Управление ИТ

Нестабильность порождает новое поколение CIO-инноваторов

Две трети организаций пересматривают свои ИТ-стратегии в связи с политической и экономической неопределенностью. Тем не менее, как показало исследование CIO Survey, проведенное Harvey Nash и KPMG, при этом 89% сохраняют и даже увеличивают инвестиции в инновации, в том числе в «электронных сотрудников» – искусственный интеллект в различных его проявлениях.

Хотя нестабильность делает бизнес-планирование проблематичным для многих организаций, очевидно, что цифровые стратегии проникли в компании довольно глубоко. Доля организаций, имеющих полномасштабную цифровую стратегию, достигла 52%, а у 39% появилась должность цифрового директора (Chief Digital Officer). Для осуществления комплексных преобразований компаниям чрезвычайно необходимы специалисты по архитектуре предприятия.

Вопросы кибербезопасности как никогда актуальны: 32% опрошенных признали, что их компания за последний год подверглась крупной атаке. Лишь 21% ИТ-директоров заявляют, что «очень хорошо» готовы к атакам. Несмотря на то что широкое освещение получают действия хакеров, самый большой рост наблюдался в сегменте инсайдерских атак.

Как отмечают аналитики, экономическая и политическая обстановка изменяется очень быстро, что не может хорошо отражаться на настроениях компаний и их готовности к инвестициям. Однако многие ИТ-руководители находят возможность извлечь выгоду даже в таких условиях, делая свои компании более гибкими и цифровыми. Они начинают приобретать все большее влияние на первых лиц, которым нужен доверенный специалист для освоения цифрового окружения.

ИТОГО

К числу ключевых можно отнести следующие выводы исследования:

«ЦИФРОВЫЕ ЛИДЕРЫ» ИНТЕРЕСУЮТСЯ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

- Лишь 18% ИТ-директоров считают, что им удалось разработать эффективную цифровую стратегию.
- «Цифровые» компании в четыре раза чаще инвестируют в когнитивные технологии (25%).
- 61% крупных компаний уже инвестируют в «электронную рабочую силу».

ИТ-ДИРЕКТОРА ЛЮБЯТ СВОЮ РАБОТУ

- Число ИТ-руководителей, «очень удовлетворенных» своей ролью в компании, достигло максимума и составляет 39%.
- Впервые за последние 10 лет более 70% ИТ-директоров заявили, что их роль становится более стратегической.
- 92% ИТ-руководителей за последний год участвовали хотя бы в одном совете директоров.
- Средняя «продолжительность жизни» CIO составила около пяти лет на одном рабочем месте.

CIO-ЖЕНЩИНЫ СТАЛИ ЗАРАБАТЫВАТЬ БОЛЬШЕ

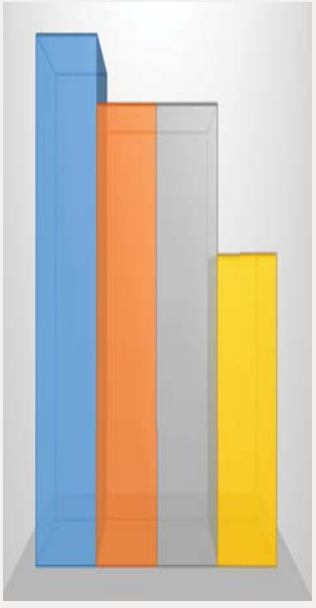
- 42% женщин получили прибавку к зарплате (среди мужчин об этом заявили лишь 32%). Однако процент женщин среди ИТ-менеджмента по-прежнему крайне мал – 9%.

СЛОЖНОСТЬ ИТ-ПРОЕКТОВ РАДИКАЛЬНО УВЕЛИЧИЛА РИСК НЕУДАЧИ

- Две трети ИТ-директоров заявляют, что нынешние проекты заметно усложнились. Отсутствие спонсора проекта, слишком оптимистичный подход и неясные цели становятся главными причинами неудач.
- 27% в качестве главной причины провала проекта называют плохого менеджера проекта, однако специалистов с требуемыми навыками в списке наиболее востребованных экспертов нет.

Главные причины проектных неудач

46% Отсутствие спонсора проекта
40% Слишком оптимистичный подход
40% Неясные цели
27% Плохой руководитель проекта



Источник: Harvey Nash, KPMG, 2017