

Директор

информационной службы



ПЛОДЫ ЦЕНТРАЛИЗАЦИИ ИТ В КРУПНОМ АГРОПРОМЫШЛЕННОМ ХОЛДИНГЕ

СЕРГЕЙ ПОТАПОВ

ДИРЕКТОР ПО ИТ ГРУППЫ
КОМПАНИЙ «РУСАГРО»

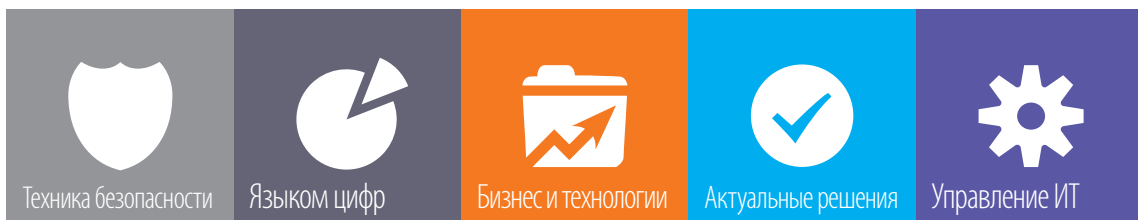
БОЛЬШОЙ ИНТЕРЕС
К БОЛЬШИМ ДАННЫМ

СИСТЕМНЫЙ ВЗГЛЯД
НА ПРИОРИТЕТЫ В ИТ

«ПОСЛЕДНЯЯ
МИЛЯ» ЛОГИСТИКИ

БЕСПИЛОТНИКИ
НАД РОССИЕЙ

3 **ИТОГО**
9 **МОНИТОР**
10 **ТРИ ВОПРОСА**
11 **ТЕНДЕНЦИИ И КОММЕНТАРИИ**



ИНТЕРВЬЮ

12 ПЛОДЫ ЦЕНТРАЛИЗАЦИИ

МИХАИЛ ЗЫРЯНОВ



СТРАТЕГИЯ

18 СІО в 2016 году:
от великого к обыденному
НИКОЛАЙ СМІРНОВ

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

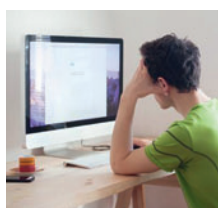
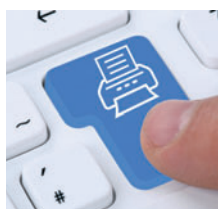
26 Большой интерес
к Большим Данным
АЛЕКСЕЙ ЕСАУЛЕНКО

30 Дроны для бизнеса:
новая «головная боль»
для ИТ-директора

ПОЛ РУБЕНС

32 Беспилотники
над Россией

ИРИНА ШЕЯН



ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

34 «Последняя миля» логистики:
конкуренция алгоритмов

ИРИНА ШЕЯН

40 Цифровая стратегия:
ИТ-директора должны быть
решительнее

ЭДВАРД КУАЛТРО

ПРАКТИКА

42 Три способа сэкономить
на печати миллионы

СТЕФАНИ ОВЕРБИ

УПРАВЛЕНИЕ ИТ-ПЕРСОНАЛОМ

44 Как наладить прочные
взаимоотношения
с удаленными сотрудниками

САРА УАЙТ

CSO

46 Чем новый директор
по информационной
безопасности должен
заняться в первую очередь

РАЙАН ФРЭНСИС

ХИТЫ

48 Прогнозы на 2016
год от поставщиков
и аналитиков в области
кибербезопасности

ТЭЙЛОР АРМЕРДИНГ

Читайте
в следующем
номере

- Шесть стратегий оценки ИТ-проектов и расстановки приоритетов
- Нефть — падает, данные — растут
- Управление проектами: когда «классика» не работает
- Ключевые аспекты безопасности Больших Данных

На правах рекламы



Техника безопасности

Больше «бумажной» безопасности и пилотных проектов

Кроме того, что в области информационной безопасности в 2016 году усилятся существующие тенденции, будут происходить заметные изменения в поведении компаний, такими прогнозами поделились эксперты Zecurion Analytics.

Говоря о своих ожиданиях относительно будущих киберугроз, аналитики выделяют несколько ключевых направлений. Первое – целенаправленные атаки. За подобными атаками – будущее киберпреступности на ближайшие несколько лет.

По словам Владимира Ульянова, руководителя Zecurion Analytics, такие атаки сложнее в подготовке и дороже обходятся, однако более результативны, а в финансовом отношении – выгоднее атак широкого спектра. Расследования громких инцидентов последних лет выявляют все большее число именно целенаправленных атак.

Самые громкие и значительные кампании оказываются хорошо спланированными и подготовленными. Часто злоумышленники используют элементы социальной инженерии и прибегают к помощи инсайдеров, чтобы обойти защиту. Тем самым минимизируются собственные риски и обеспечивается впечатляющий результат.

Вторым важным направлением, заслуживающим особого внимания, становятся Интернет вещей и связанные с ним угрозы. Техника всё больше «умнеет», но по-прежнему слабо защищена. Современные устройства в большинстве своем имеют один или даже несколько сетевых интерфейсов, но не имеют адекватных средств защиты. Вопросам безопасности устройств просто не уделяется внимания.

Внутренние угрозы продолжают оставаться одной из самых больших забот служб информационной безопасности. Повсеместное внедрение механизмов разграничения доступа – даже в рамках отдельных приложений – не решило проблему утечки информации. Наоборот,

с развитием технологий передачи информации проблема стала острее.

К утечке могут привести несколько событий, каждое из которых относительно безобидно и укладывается в рамки стандартных бизнес-процессов. Это предъявляет дополнительные требования к системам защиты информации. В любом случае те права доступа, которыми обладают собственные сотрудники, позволяют им быть эффективным инструментом в руках киберпреступников, и потому они нередко становятся одним из элементов сложной атаки.

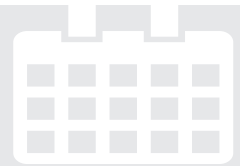
Еще одним заметным направлением в нынешних непростых условиях становится «бумажная» безопасность. Сокращение бюджетов неизбежно приведет к пересмотру приоритетов. Часть проектов придется отложить до лучших времен или вовсе отменить. Наибольшее внимание будет уделено мероприятиям, которые не требуют серьезных финансовых вложений. Прежде всего это профилактическая и бумажная работа.

«Организовать занятия и тренинги сотрудников по вопросам защиты информации – недорого, но эффективно, ведь человек остается наиболее уязвимым звеном информационной безопасности», – уверен Ульянов. Именно люди являются объектом фишинга, социальной инженерии и других видов атак.

Второе направление на 2016 год – это подготовка документации, та кропотливая и скучная работа, которую в большинстве случаев откладывали до «лучших времен». Сейчас это время пришло. Разработка документов, регламентирующих деятельность (политик информационной безопасности, регламентов, процедур и инструкций), способствует систематизации деятельности, в том числе в будущем, когда нормальное финансирование будет восстановлено.

Наконец, компании станут еще более взвешенно подходить к приобретениям. Они не откажутся от внедрений новых продуктов, для этого просто нет оснований – задача поддержания и укрепления уровня безопасности никуда не исчезнет. Финансирование будет сокращено не столь значительно – напротив, ожидается, что рынок программных средств защиты информации вырастет относительно 2015 года. Однако выбирать средства защиты станут более аккуратно.

Кроме того, в практику войдут пилотные проекты. Они не требуют больших финансовых затрат, а часто выполняются за счет вендора или его партнера, при этом позволяют опробовать решение в реальной среде.



НЕ ПРОПУСТИТЕ

23 марта

V Российский форум Big Data 2016

☞ Форум

📍 Москва

Издательство «Открытые системы», www.ospcon.ru

23 марта

SAMday 2016

☞ Конференция

📍 Москва

itSMF Россия, www.samday.org

5 апреля

«Бизнес-Видео – 2016»

☞ Форум

📍 Москва

Издательство «Открытые системы», www.ospcon.ru

19-21 апреля

EXPO COMM Russia 2016

☞ Выставка

📍 Москва

«И. Джей Краузе энд Эсоушиэнтс», expocomm.ru

24 мая

«МИР ЦОД. Инфраструктура»

☞ Форум

📍 Москва

Издательство «Открытые системы», www.ospcon.ru

7 июня

13-й Российский IT Management Forum

☞ Форум

📍 Москва

Издательство «Открытые системы», www.ospcon.ru

4 октября

«МИР ЦОД. Услуги. Облака»

☞ Форум

📍 Москва

Издательство «Открытые системы», www.ospcon.ru



Языком цифр

Цифровая экономика требует переоценки активов

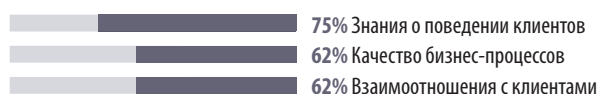
Финансовым директорам следует переосмыслить существующую практику оценки экономического благосостояния своих компаний в эпоху цифровых технологий. Большая часть современных корпоративных ценностей создается посредством нематериальных активов, таких как поведение потребителя и торговая марка, очень немногие респонденты заявили, что у них есть возможность обращаться к достоверным данным, чтобы оценить эти критически важные элементы бизнеса и вести их мониторинг.

В исследовании, проведенном Chartered Global Management Accountant, утверждается, что необходимость оценить, какие преимущества для бизнеса несут нематериальные активы, с помощью ключевых показателей эффективности (KPI) будет только нарастать по мере распространения бизнес-моделей, активно использующих цифровые технологии. Важность нематериальных активов существенно выросла за последние несколько лет, и сегодня на их долю приходится 80% от общей акционерной стоимости компаний. Опрошенные респонденты считают, что основными факторами повышения эффективности и акционерной стоимости их компаний являются поведение потребителей (его отметили 75% респондентов), качество бизнес-процессов (62%) и взаимоотношения с клиентами (62%).

Тем не менее исследование показало, что финансовые специалисты испытывают трудности с доступом к данным, связанным с нематериальными активами, и с их анализом. Так, лишь 16% респондентов заявили, что могут собирать и анализировать данные о поведении потребителя. Еще у 16% финансовых директоров, по их словам, есть доступ к данным о влиянии их бренда на их бизнес, и только 29% опрошенных подтвердили свою возможность оценивать качество бизнес-процессов компании.

На вопрос о том, в какой степени финансовая служба была преобразована для поддержки новых факторов повышения эффективности бизнеса, лишь 10% респондентов ответили, что финансовый департамент в их компании полностью участвует в предоставлении нефинансовых показателей оценки достигнутого роста.

КЛЮЧЕВЫЕ НЕМАТЕРИАЛЬНЫЕ АКТИВЫ



Источник: CGMA, 2016

«Цифровая рулетка»: проекты трансформации чрезвычайно рискованны

Успеху цифровых проектов препятствуют их сложность, конфликт приоритетов и неуверенность в результате. Исследование, проведенное Fujitsu, выявило серьезные различия в стратегических приоритетах компаний.

По мнению отраслевых экспертов, 2016 год станет «годом цифровых преобразований». Три четверти организаций согласны с тем, что цифровизация бизнеса является для них бизнес-приоритетом, но столько же сомневаются в правильности принятых решений в этой сфере.

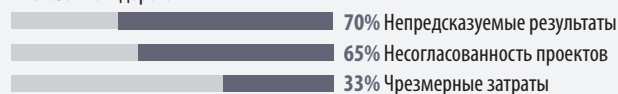
В целом исследование выявило оптимизм во взглядах на цифровые преобразования. Руководители уверены в том, что их организации способны реализовать такие проекты, подавляющее большинство высказалось за ускорение трансформации. Кроме того, большинство из них согласны с тем, что промедление чревато множеством негативных последствий, включая увеличение времени реагирования бизнеса на требования рынка, а также проблемы с удержанием клиентов и сохранением их лояльности.

Однако аналитики полагают, что на деле оптимизм бизнеса в отношении цифровых преобразований выглядит по большей части бравадой. Только одна из четырех компаний действительно уверена в принимаемых решениях в области цифровых преобразований, тогда как две компании из трех признают, что подобные проекты, реализуемые у них, скорее, являются авантюрой. Более того, треть бизнес-руководителей оценивают затраты своей организации на цифровые проекты как чрезмерные.

Ради процветания бизнеса компаниям требуется быстрее объединять технологии и новые идеи. Однако отсутствие явной заинтересованности и конфликт интересов создают барьеры на пути к успеху.

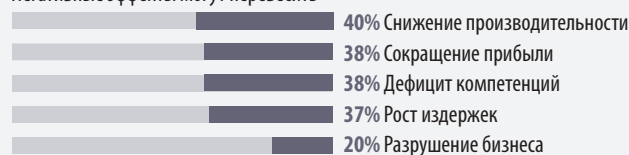
ПРОБЛЕМЫ ТРАНСФОРМАЦИИ БИЗНЕСА

Рискованно и дорого



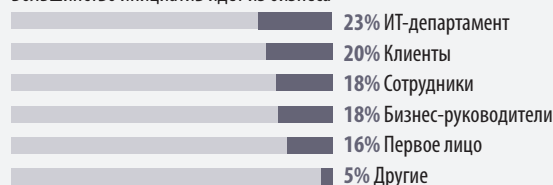
РИСКИ ЦИФРОВИЗАЦИИ

Негативные эффекты могут перевесить



ИНИЦИАТОРЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Большинство инициатив идет из бизнеса



Источник: Fujitsu, 2016

Каждая шестая российская компания в прошлом году подверглась DDoS-атаке

В прошлом году 17% российских компаний столкнулись с DDoS-атаками, а сама страна оказалась в первой пятёрке государств, чьи веб-ресурсы вызвали наибольший интерес у киберзлоумышленников. В общей сложности за 2015 год эксперты «Лаборатории Касперского» зарегистрировали свыше 120 тыс. атак, направленных на интернет-ресурсы.

В России киберпреступники чаще всего атаковали компании среднего и крупного бизнеса – от DDoS-инцидентов пострадали соответственно 20 и 17% организаций. Однако микробизнес тоже не остался без внимания: 12% мелких компаний, принявших участие в опросе, испытали на себе последствия DDoS-атак.

Атакующие старались вывести из строя не только сайт организации, хотя такая цель была в числе главных – 55% DDoS-атак были направлены именно на официальный веб-портал компании. Тем не менее

СЕРВИСЫ, ПОСТРАДАВШИЕ В РЕЗУЛЬТАТЕ DDoS-АТАК



Источник: «Лаборатория Касперского», 2016

треть инцидентов затронула коммуникационные сервисы (прежде всего почтовые серверы), а в 23% случаев пострадали страницы, предназначенные для клиентов компании. 18% атак были нацелены на файловые серверы, и еще 12% – на сервисы для совершения финансовых операций.

При этом довольно часто DDoS-атака осуществлялась одновременно с другой кибератакой, в которой использовалось вредоносное ПО, или же она служила прикрытием для кражи ценных данных. О подобных двойных инцидентах заявили 59% компаний.

В результате DDoS-атак у половины пострадавших организаций скорость загрузки веб-страниц значительно замедлялась. Однако четверть компаний имели дело с более неприятными последствиями: атаки полностью нарушили работоспособность сервисов или же стали причиной сбоя финансовых транзакций.

DNBD
marketing.dnbd.su

DIVE IN MARKETING 2016

Конференция для профессионалов
в области маркетинговых коммуникаций

На главной сцене лидеры индустрии
и создатели лучших мировых кейсов,
только практики

Более 1000 делегатов на площадке,
300 медиа-партнеров и СМИ

Активный нетворкинг

ОРГАНИЗАТОР ФОРУМА:
DNBD INTERACTIVE
FORUMS

По вопросам информационного
сотрудничества и аккредитации СМИ:
ИЛОНА АВИЛОВА
Brand-директор
+7 (903) 111 00 70
IA@DNBD.SU

Реклама