

PCWEEK

UKRAINIAN
EDITION

WWW.PCWEEK.UA

ЕЖЕДНЕВНЫЕ
ГЛАВНЫЕ НОВОСТИ
И СОБЫТИЯ ИТ-РЫНКА

ГАЗЕТА ДЛЯ КОРПОРАТИВНЫХ ПОЛЬЗОВАТЕЛЕЙ ИТ

• №2 (70) • 2015 • КИЕВ



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ:

В ПОИСКАХ СОВЕРШЕННОЙ ЗАЩИТЫ

Х ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ

DATACENTERS & SECURITY DAY 2015:

ЭФФЕКТИВНОСТЬ | ОПТИМИЗАЦИЯ | БЕЗОПАСНОСТЬ



ОРГАНИЗАТОР
PCWEEK
UKRAINIAN
EDITION

ДАТА ПРОВЕДЕНИЯ:

21 октября 2015 г.



МЕСТО ПРОВЕДЕНИЯ:

**КОНГРЕСС-ХОЛЛ «КОСМОПОЛИТЬ»
г. Киев, ул. В. Гетьмана, 6**

Детальная информация и регистрация на сайте www.pcweek.ua

В УКРАИНЕ УСИЛИВАЮТ ЗАЩИТУ ИНФОРМАЦИИ В ГОССЕКТОРЕ

Государственная служба специальной связи и защиты информации (Госспецсвязь) провела тренинг для госслужащих 1-й и 2-й категорий по организации защиты информации. Сотрудников проинформировали об основных понятиях защиты информации, возможных угрозах для ее целостности и сохранности, а также важности этого процесса для обеспечения информационной безопасности страны. Также на тренинге проанализировали возможные каналы утечки данных и продемонстрировали действующие системы блокирования подобных утечек.

Первая часть мероприятия была посвящена организационно-правовым основам и общим сведениям по организации технической защиты информации (ТЗИ). Во второй части основное внимание уделили технологиям шифрования, а также провели презентацию средств ТЗИ.

Криптографическая защита

История криптографии насчитывает около 4 тысяч лет. Первые шифры использовались еще в третьем тысячелетии до н. э. В основном тогда доминировали моноалфавитные шифры, в основе которых лежала замена букв алфавита исходного текста буквами или символами альтернативного алфавита. Примерно с начала второго тысячелетия в обиход были введены полиалфавитные шифры. А уже в середине XX века начался новый период — переход к математической криптографии. При этом важным требованием создания нового шифра стало исследование его уязвимости к различным известным атакам в соответствии с линейным и дифференциальным криптоанализом. Стоит отметить, что в XX веке появились первые шифровальные машины, например, шифровальная машина Enigma, которая использовалась в коммерческих и военных целях во многих странах мира, но наибольшее распространение получила в нацистской Германии.

До 1975 года в криптографии применялись только симметричные технологии шифрования — с секретным ключом. В последние 40 лет успешно развивается новое направление — криптография с открытым ключом. Ее появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптогра-

фического алгоритма с открытым ключом RSA (1977). Стоит также отметить недавнюю отечественную разработку — блочный симметричный шифр «Калина», разработанный ЗАО «Институт информационных технологий» г. Харькова.



Ведомство Госспецсвязи провело тренинг для госслужащих 1-й и 2-й категории по организации защиты информации в государственных органах

Даниил Мялковский, заместитель директора Департамента криптографической защиты информации (КЗИ) Администрации Госспецсвязи, в своем докладе подвел основные итоги на рынке криптозащиты. Во-первых, отмечается постоянное совершенствование математических механизмов осуществления практических атак, направленных на криптографические механизмы. Во-вторых, правительственные агентства разных стран совершенствуют кибероружие, основываясь на использовании закладок (то есть, незадекларированных функций) в уже созданных системах и перспективных стандартах. В-третьих, ведущие страны для защиты классифицированной информации применяют алгоритмы ограниченного распространения. Таким образом, все криптографические приложения должны разрабатываться очень тщательно, а их исследования необходимо проводить с привлечением независимых высококвалифицированных аналитиков.

Государственная политика в сфере криптографической защиты, по словам спикера, реализуется по следующим направлениям:

- нормативно-правовое регулирование в сфере криптографической защиты информации;
- техническое регулирование в сфере криптографической защиты информации;
- поддержка функционирования и развития криптографической системы;

Сравнение криптографической стойкости блочных шифров «Калина» и AES

	AES	«Калина»
Вычислительная сложность	2 ⁴⁰	2 ⁵⁵
Длина блока	128 бит	128 бит
Метод криптоанализа	дифференциальный	дифференциальный
Количество циклов	5	5

фии для использования частными лицами. Эра современной криптографии — это применение таких криптоалгоритмов, как Data Encryption Standard (DES), взятого на вооружение в 1977 году, AES (1997), NESTIE (2000), CryptoRec, SHA-3 (2007) и

- координация деятельности органов государственной власти и органов местного самоуправления военных формирований, предприятий, учреждений и организаций в указанной сфере;
- координация деятельности субъектов национальной

инфраструктуры открытых ключей электронно-цифровой подписи (ЭЦП);

- лицензирование хозяйственной деятельности в сфере криптографической защиты информации;
- экспортный контроль в

сфере криптографической защиты информации; также государственное определение способов и порядка защиты конфиденциальной информации, которая передается в государственные органы.

Деятельность ведомства по внедрению ЭЦП

Благодаря вышеупомянутым шифрам с открытым ключом стало возможно применение электронно-цифровой подписи. ЭЦП играет важнейшую роль при построении e-government, поскольку данная концепция предполагает предоставление различных услуг гражданам страны через сайт электронных государственных услуг. В этой сфере Госспецсвязь намерена выполнять такие задачи, как техническое регулирование (процесс создания средств КЗИ и их функционирования в составе информационно-телекоммуникационных систем), и координировать деятельность субъектов услуг ЭЦП по вопросам защиты информации. Также ведомство будет выполнять государственный контроль соблюдения субъектами услуг ЭЦП требований законодательства в данной сфере.

Что касается внедрения ЭЦП в деятельность государственного органа, то здесь Госспецсвязь планирует осуществить следующие основные шаги: определить

Стандартизация в сфере КЗИ

По инициативе Минюста и Госспецсвязи Министерство экономического развития и торговли Украины приняло



Автономный комплекс, содержащий генератор виброшума с модулями блокировки утечки звуковой информации через трубы системы отопления и через оконное стекло, а также генераторы звукового шумления в вентиляционных шахтах и других возможных каналах утечки

европейские и международные нормативные документы в качестве национальных стандартов Украины. Это около 40 нормативных документов, определяющих криптографические механизмы и способы их применения, они вступают в силу с 2016 года. Кроме того, вступили в силу с апреля и июля 2015 новые национальные криптографические алгоритмы, разработанные по заказу Госспецсвязи: ДСТУ 7564:2014 «Информационные технологии. Криптографическая защита информации. Функция хеширования», а также ДСТУ 7624:2014 «Информационные технологии. Криптографическая защита информации. Алгоритм симметричного блочного преобразования» (с 1 июля 2015).

Среди новых задач в сфере технического регулирования и оценки соответствия Даниил Мялковский отметил необходимость совершенствования нормативно-правовых актов технического регулирования, описывающих применение в средствах КЗИ и ЭЦП соответствующих алгоритмов и прото-

ответственное подразделение для внедрения, администрирования и технической поддержки ЭЦП, утвердить порядок применения ЭЦП в государственном органе с учетом требований Кабмина, заключить договор с АЦСК (Авторизированным центром сертификации ключей) на получение услуг ЭЦП и обеспечить должностных лиц носителями ключевой информации и надежными средствами ЭЦП. Также Госспецсвязь собирается обеспечить выполнение должностными лицами требований по порядку применения ЭЦП.

Физические каналы утечки информации

В любом государстве есть ведомства, работающие с конфиденциальными документами, которые должны быть надежно защищены от посторонних ушей и глаз. В период же обострения политической обстановки или военного конфликта необходимость передачи информации по защищенным каналам приобретает особое значение.

ПРОДОЛЖЕНИЕ НА С. 6 >>>

PCWEEK
UKRAINIAN
EDITION

ГАЗЕТА ДЛЯ КОРПОРАТИВНЫХ
ПОЛЬЗОВАТЕЛЕЙ

Свидетельство о
государственной регистрации
печатного СМИ
Серия КВ № 21409-11209П

Издательство
ООО «ПИСИВИК УКРАИНА»

Директор
ОЛЕСЯ БАБИЧ

Редакция

Главный редактор
ОЛЕГ ПИЛИПЕНКО

Главный дизайнер
ЕЛЕНА ГАРБАР

Отдел рекламы

Тел.: +380 (44) 338-70-83
E-mail: advertising@pcweek.ua

Распространение

© ООО «ПИСИВИК УКРАИНА», 2015
04205, г. Киев, пр-т
Оболонский, 35

PC Week Ukrainian Edition.
Газета печатается по
лицензионному соглашению
с компанией
Ziff Davis Publishing Inc.
Перепечатка материалов
допускается только
с разрешения редакции.
За содержание рекламных
объявлений редакция
ответственности не несет.
Editorial items appearing in
PC Week UE that were
originally published in the U.S.
edition of PC Week are the
copyright property
of Ziff Davis Publishing Inc.
Copyright 2014 Ziff Davis Inc.
All rights reserved. PC Week
is trademark of Ziff Davis
Publishing Holding Inc.

Печать

ООО ИД «Адеф-Украина»,
ул. Б. Хмельницкого, 32,
оф. 40А,
г. Киев, 01030
тел.: +380 (44) 284-08-60
www.adef.com.ua

Периодическое издание
«PC Week Ukrainian Edition»
распространяется
по подписке.

Дата выхода:
24 сентября 2015г.

Тираж
10 000 экземпляров

Volkswagen — не единственная фирма, занимавшаяся подтасовкой тестовой информации

На днях автоконцерн Volkswagen стал фигурантом неприятной истории — выяснилось, что на экологических тестах по выбросам дизельными двигателями вредных веществ автогигант занижал данные. Это обнаружили инженеры калифорнийского комитета по надзору за выбросами вредных веществ в атмосферу. Как выяснили специалисты, ПО контроллеров дизельных двигателей TDI объемом 2,0 л могло распознавать оборудование проверки выхлопных газов и в случае его подключения включало систему фильтрации вредных выбросов на полную мощность.

Когда же автомобиль эксплуатировался в условиях повседневной городской езды, то система на полную мощь не работала. Это стало причиной повышенного выброса автомобилями VW окиси азота, который негативно влияет на озоновый слой и может быть причиной смога. Это вещество способно вызвать ряд проблем для здоровья человека, включая приступы астмы и другие респираторные заболевания.

Агентство по охране окружающей среды США (EPA) выпустило для

18 млрд. долл. — это больше, чем годовая прибыль концерна. Также вероятны многомиллиардные штрафы в связи с ведущимся расследованием минюста США и многочисленные иски от обманутых покупателей. Автопроизводитель сообщил, что «обманным» ПО снабжены 11 млн. автомобилей по всему миру.

Как пишет Уейн Реш из eWeek, в этой истории нет ничего нового, в 1980-е такое ПО было широко распространено. Впервые он столкнулся с нестандартной работой устройств, когда тестировал с коллегами Ethernet-карту одного производителя. В ходе проверки она показывала более продуктивные результаты, чем карты других вендоров, но в реальных условиях ее результаты работы были гораздо скромнее. В те времена наиболее распространенным способом проверки сетевых интерфейсных плат был тест, разработанный компанией Novell, поэтому его работа была хорошо изучена: Ethernet-карта того вендора проводила пакеты без обработки, увеличивая таким образом «производительность» во время тестирования.

По словам Реша, спустя несколько лет он обнаружил нечто подобное при тестировании гигабитных коммутаторов Ethernet в Гавайском университете, поэтому ему пришлось разработать тест, отражающий реальную работу сети. В итоге коммутатору, столкнувшемуся с обработкой фактического трафика,



VW может быть оштрафован на сумму порядка 18 млрд. долл. Это больше, чем годовая прибыль концерна

Volkswagen уведомление о допущенном нарушении, обвинив компанию в незаконной установке так называемого «defeat device», которое на сленге специалистов обозначает устройство, позволяющее обмануть систему контроля вредных веществ в выхлопных газах двигателя. Программное «шулерство» зафиксировано в 4-цилиндровых моделях марок Volkswagen и Audi 2009–2015 гг. выпуска.

Главный исполнительный директор Volkswagen Мартин Винтеркорн извинился и распорядился провести свое расследование. Кроме того, собственное расследование планирует провести правительство Южной Кореи. По информации BBC, южнокорейские власти проверяют до 5 тыс. автомобилей Volkswagen моделей Jetta и Golf, а также Audi A3s 2014 и 2015 гг. выпуска, и если в них будут выявлены проблемы, проверка коснется всех машин компании, оснащенных дизельными двигателями. О намерении проверить автомобили немецкой компании на соответствие экологическим стандартам сообщили также Франция и Италия.

В США компания фактически нарушила два пункта закона о чистоте воздуха, и по американским законам может быть оштрафована на сумму до 37,5 тыс. долл. за каждый проданный автомобиль, что в совокупности составляет порядка

так и не удалось доказать свою эффективность. «К счастью, автомобили VW являются безопасными для езды, даже если выбрасывают больше, чем положено загрязняющих веществ в атмосферу. Автопроизводитель ответит и починит эти машины, но все же проблема останется», — считает Реш.

По его словам, скорее всего, Volkswagen — не единственная компания, которая фальсифицировала результаты испытаний. «Мой опыт показывает, что создание ПО, которое может обнаружить тесты, это давняя практика. Противостоять этому можно только создав способ, когда тест не только будет имитировать работу оборудования, но создаст для его проверки условия реальной эксплуатации. Вряд ли что-то мешало и другим автомобильным компаниям обманывать тестовые программы», — делится своими мыслями Реш.

Что касается причин, которые подвигли инженеров VW подтасовать работу софта, то этим будет заниматься следствие. Возможно, что у них просто не было времени для доработки ПО, которое могло бы эффективно управлять двигателями. Не исключено также, что таким образом концерн сократил затраты на техобслуживание, экономя на AdBlue (специальный раствор мочевины, используемый для нейтрализации вредных выбросов дизельных двигателей).

СОДЕРЖАНИЕ

НОВОСТИ

3 В Украине усиливают защиту информации в госсекторе

5 ИТ все чаще определяют вектор развития физической безопасности

6 Три вещи, которые СЮ должны знать о кибербезопасности

7 Сотни маршрутизаторов Cisco инфицированы в результате атаки SYNful Knock

7 Мег Уитман: гибридная облачная инфраструктура — это будущее

8 Наиболее важные новшества Microsoft Office 2016



КОРПОРАТИВНЫЕ РЕШЕНИЯ

10 UARAY предлагает инновационную схему получения комиссионных доходов

10 Недоработки и неудобства в Windows 10

12 Риски, связанные с использованием поддельных картриджей

— Что в Вашем принтере?

ТЕМА НОМЕРА

14 Информационная безопасность: в поисках совершенной защиты

16 Актуальные киберугрозы: мнение экспертов

18 Семь шагов к безопасности интернет-банкинга

19 Три козыря Fortinet: предотвращение, обнаружение, снижение рисков

20 Проблемы построения и аудита систем управления информационной безопасностью банка



21 Как мы выбирали решение по сетевой безопасности

21 Онлайн-магазин Apple впервые подвергся крупной кибератаке

МОБИЛЬНЫЕ РЕШЕНИЯ

22 iPad Pro поистине новый планшет Apple

22 iPhone 6s вместо iPhone 6 — стоит ли переходить?

ИТ ВСЕ ЧАЩЕ ОПРЕДЕЛЯЮТ ВЕКТОР РАЗВИТИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

Выбор средства обеспечения физической безопасности сегодня в значительной степени диктуется тенденциями на рынке ИТ. IP-технологии, биометрическая аутентификация, облачная архитектура, FOG-вычисления — все это оказывает мощное влияние на развитие систем контроля физического доступа, видеонаблюдения, сигнальных систем и пр.

Тенденции на рынке

Современные средства контроля доступа тесно связаны как с развитием технологий в целом, так и с мобильными решениями. Например, для открытия дверей всё чаще используют мобильные устройства, что гораздо безопаснее и удобнее. Наблюдается тенденция замены механических ключей на карточки и телефоны. Кроме того, внедряется практика использования решений по генерации одноразовых паролей для контроля физического и логического доступа, рассказывает Артем Касьянов, инженер 1-й категории в компании «ИТ-Интегратор».

Технология Bluetooth Smart для карточек и смартфонов обеспечивает пользователям доступ к нужным объектам, приложениям и сетям. Идентификация в данном случае происходит благодаря считыванию данных с устройства или карты. Мобильные технологии развиваются настолько активно, что на сегодняшний день Bluetooth Smart может считывать информацию для открытия дверей даже на расстоянии.

Олег Саенко, инженер-консультант Internet of Things, EMEA/RCIS в компании Cisco, указывает, что на рынке средств контроля физического доступа с технологической точки зрения заметны такие тенденции, как завершение перехода на IP-технологии, увеличение масштаба систем и появление средств дополнительного контроля доступа, в том числе биометрических.

Что касается общих трендов в сегменте систем физической безопасности, то здесь можно отметить стандартизацию и

О том, что биометрические технологии стремительно завоевывают рынок, свидетельствует появление соответствующих устройств для подтверждения личности на входе в режимные здания, применение



Олег Саенко

инженер-консультант Internet of Things, EMEA/RCIS в компании Cisco

сканеров отпечатков пальцев или геометрии лица в мобильных гаджетах на базе iOS, Android и Windows Phone.

Кроме того, вышеописанная тенденция подтверждаются и недавним выпуском Windows10, где системы биометрии встроены в ОС. Это позволяют войти в систему, сканируя лицо, глаза или отпечатки пальцев. Таким образом, подобные разработки активно продвигают использование биометрии в различных устройствах.

Трансформации подвергаются и сами сканеры. В будущем они станут мультифункциональными и смогут поддерживать разные типы биометрической аутентификации, полагает Артем Касьянов.

На практике большое количество запросов от заказчиков поступает отно-

как того хотели бы производители. Ее решения сложны в настройке и поддержке, что ведет к большим затратам на внедрение при недостаточно высоком уровне надежности аналитики. В первую очередь это касается систем распознавания образов. Более простая аналитика, например, различного рода детекторы вроде входа в зону контроля, выхода из нее и так далее, достаточно популярна. Многие производители на рынке могут предложить ее как бесплатную опцию к своим камерам видеонаблюдения.

Но в целом, учитывая развитие технологической платформы, область применения аналитики ограничена, говорит Олег Саенко. Более перспективным видится направление предобработки данных на стороне конечного оборудования (камер, контроллеров): простая видеоаналитика, корреляция событий и данных для формирования тревог или информационных сообщений. То есть, речь идет о подготовке данных для последующей обработки на уровне центральной системы управления.

Внедрение аналитики должно решать задачу качественной работы системы безопасности, что повсеместно и начинает применяться. В силу глубокого проникновения видеонаблюдения в нашу жизнь и экспоненциального роста числа установленных камер, применение аналитики становится все более важным и необходимым.

Тем не менее, отрасль ждет большей простоты настройки и повышенной надежности работы алгоритмов. Ведь с появлением камер с разрешениями 4K и даже выше для видеоаналитики открываются совершенно новые и очень широкие возможности.

Интернет вещей и FOG-вычисления

Технологии интернета вещей (IoT) способны дать новый толчок развитию средств безопасности. Например, «умный дом» может предупредить хозяев о проникновении посторонних, определить утечку угарного газа или протекание воды. Ритейлеры будут отслеживать украденные товары с помощью подключенных к Интернету маячков безопасности. Некоторые эксперты считают, что развитие Интернета вещей поможет людям изменить взгляд на безопасность в целом — использование объединенных в единую сеть устройств позволит достигнуть более высокого уровня защиты в обычной жизни.

Разработка устройств с низким потреблением энергии и периодичностью передачи данных (LoRa — Low Power Wide Area Network), появление новых технологий передачи данных в схеме взаимодействия устройств дают возможность значительно увеличить количество систем контроля и мониторинга. Но с точки зрения Олега Саенко, по мере прогресса в области IoT все более важную роль будут играть так называемые распыленные вычисления — FOG-вычисления, подразумевающие обработку данных на стороне конечного оборудования (то есть, камер и контроллеров).

В своем блоге Мачек Кранц, вице-президент и генеральный менеджер отдела корпоративных технологий компании Cisco, пояснил, почему появилась такая технология. Известно, что на первом этапе развития Интернета все данные загружались в аналитические системы. Это хорошо работало для больших объемов исторических данных, например, когда нефтяной компании для внедрения новых методов добычи требовался пакетный анализ сейсмической информации за несколько лет. В определенных случаях такой подход работает и сейчас, например, когда речь идет о подключенных к сети торговых автоматах, которые передают в Интернет

всего несколько байт информации о необходимости пополнения запасов товаров. Разумеется, для такой ситуации не требуются ни большая полоса пропускания, ни быстрая обработка в режиме реального времени.



Артем Касьянов

инженер 1-й категории в компании «ИТ-Интегратор»

Появление Всеобъемлющего Интернета (Internet of Everything, IoE) потребовало массу высокоскоростных приложений реального времени. Для работы с ними необходим новый подход — использование FOG-вычислений. Распыленные (FOG) вычисления приближают средства анализа к источникам данных, делая возможными как обработку в реальном времени, так и мгновенную ответную реакцию. Вместо того чтобы перемещать массивы исходных данных, такие вычисления сортируют и индексируют информацию локально, передавая в облако лишь аварийные уведомления и сообщения о нештатных ситуациях.

Благодаря перемещению средств анализа ближе к данным, датчики транспортной инфраструктуры способны, например, определить перемещение специального транспорта и тут же скорректировать работу светофоров для быстрого и безопасного проезда

Благодаря перемещению средств анализа ближе к данным датчики транспортной инфраструктуры способны, например, определить перемещение специального транспорта и тут же скорректировать работу светофоров для быстрого и безопасного проезда. А нефтегазовая компания с помощью температурных и акустических датчиков сможет выявить аномальные условия и немедленно предпринять соответствующие меры для предотвращения выброса.

Переход к аналитике с помощью распыленных вычислений уже идет полным ходом. Во время недавнего опроса специалистов по информационным и операционным технологиям 37% респондентов заявили, что через три года большая часть IoT-данных будет обрабатываться локально, на границе сети.



В где через три года будут обрабатываться данные, генерируемые IoT-решениями?

Через три года на долю FOG-технологии будет приходиться 37% от всех IoT-вычислений

обширное проникновение IT-стандартов и протоколов, а также переход на облачную и cloud-fog архитектуру. К последней относится централизация средств управления, администрирования и мониторинга, распределение вычислений и предобработки данных на стороне конечного оборудования, о чем будет подробно рассказано ниже. Также для обеспечения физической безопасности все чаще применяют сервисную модель, в пользу чего свидетельствует появление предложений услуг Video Surveillance as a Service (VSaaS).

Биометрия для аутентификации и идентификации

Одним из наиболее важных трендов в области обеспечения физической безопасности сегодня является развитие биометрической аутентификации. По данным исследования Infiniti Research Limited, рынок биометрии будет расти в среднем на 21,83% в течение 2014-2019 г.

сительно систем контроля доступа (СКД) с использованием биометрических технологий. Даже самые современные решения со временем становятся доступными для конечного пользователя, поэтому заинтересованность заказчиков в биометрии — логичное продолжение развития технологии, утверждает спикер.

Однако биометрические технологии могут быть полезны не только с точки зрения аутентификации, но и идентификации. Например, видеонаблюдение с поддержкой функции распознавания номеров машин или идентификации прохожих по геометрии лица или радужной оболочке глаза позволяет находить угнанные автомобили или преступников. Кстати, аналитика распознавания номеров автотранспорта является де-факто уже стандартом для проектов типа «умный» или «безопасный» город.

Однако, по словам Олега Саенко, видеоаналитика не настолько популярна,

ТРИ ВЕЩИ, КОТОРЫЕ СІО ДОЛЖНЫ ЗНАТЬ О КИБЕРБЕЗОПАСНОСТИ

СТИВ ДЕРБИН

Сотрудники нашего портала Information Security Forum хорошо знают, что кибербезопасность — один из ключевых приоритетов бизнеса, и связано это со все большей его цифровизацией и ростом как количества, так и сложности киберугроз. В нынешнюю цифровую эпоху кибербезопасность является одним из главных вопросов для СІО. Чтобы их работа была успешной, они должны не только хорошо ориентироваться в постоянно эволюционирующем ландшафте киберугроз, но и выработать проактивную стратегию готовности своей организации к противостоянию сегодняшним вездесущим опасностям.

В течение многих лет СІО добивались права занять место у пресловутого «большого стола» и стать партнерами бизнеса. И, очевидно, сейчас для этого самое время, ибо технологическая связка между обеспечением условий для функционирования ИТ и управлением безопасностью и рисками диктуют необходимость партнерства СІО и CEO. По моему опыту успешное взаимодействие этих двух руководителей повышает вероятность того, что компания сумеет достичь целей своих стратегических инициатив. Эффективное взаимодействие позволяет организациям выгодно использовать возможности, открываемые киберпространством и современной технологией, и вместе с тем быть защищенными от сопутствующих рисков.

СІО необходимо знать тенденции в использовании личных устройств и облаков в рабочих целях, новые нормы защиты личной информации и ответственности за утечку данных, а также новые угрозы безопасности

Функция СІО пребывает в процессе значительных изменений, но то же самое происходит и в бизнесе. Роль СІО

со временем существенно выросла — от концентрации на самих ИТ до фокуса на бизнес-рисках, умения разговаривать на языке бизнеса и четкого изложения своей позиции на совете директоров, которые наверняка менее сведущи в технологиях. Что касается инцидентов с безопасностью, современный СІО обязан досконально понимать, что произошло, и уметь правильно осмыслить и отреагировать на причинные риски. Без этого понимания анализ рисков и принимаемые решения могут содержать ошибки, на которые руководство будет реагировать неадекватно.

Три сферы безопасности

Хочу обратить внимание на три специфические сферы информационной безопасности, о которых, как мне кажется, надо знать всем СІО. Заметим, что сферы эти не являются взаимно изолированными и могут сочетаться, порождая опасности еще более высокого уровня. И хотя это не единственные проблемы, о которых должен помнить СІО, их надо постоянно держать под пристальным вниманием.

1. ВУОх и личные облака на рабочем месте

С усилением тенденции использовать для рабочих целей приносимые сотрудниками личные мобильные устройства, приложения, персональную облачную память и собственное облачное рабочее пространство (Bring Your Own Everything, ВУОх) организации всех масштабов сталкиваются с фактами злонамеренного использования рисков информационной безопасности. Эти риски проистекают как из внутренних, так и из внешних угроз, включая неправильное обращение с самим устройством, манипуляции извне с уязвимостями ПО и развешивание плохо протестированных, ненадежных бизнес-приложений.

Если СІО чувствует, что риски ВУОх слишком высоки, ему следует контролировать разработки и вносить в них необходимые коррективы. Если эти риски находятся в приемлемых рамках, он должен напрямую взаимодействовать с CEO и советом директоров, чтобы программа ВУОх была хорошо структурирована и правильно реализована. Необходимо помнить, что плохо реализованная стратегия использования

персональных устройств на рабочем месте может приводить к случайным утечкам информации из-за размывания границы между рабочими и личными данными, а также из-за того, что значительная часть бизнес-данных будет плохо защищена.

К заботам СІО в этой области относится также продолжающийся переход к использованию облаков и связанная с этим проблема оценки безопасности как сервиса для облачных приложений, часть которых может сосуществовать с экосистемой организации вне сферы компетенции или без разрешения ИТ-группы. Использование собственного облака является новым вектором угроз, который требует постоянного внимания и контроля.

2. Законодательное регулирование безопасности данных

Правительства большинства стран уже выпустили или разрабатывают правила, содержащие гарантии безопасности и условия использования персональных данных и предусматривающие наказания для предприятий, не обеспечивающих надлежащую защиту. Поэтому защиту личной информации следует рассматривать как юридическую норму и одновременно как бизнес-риск, который надо устранять, чтобы организация не попала под санкции и не понесла коммерческого ущерба (например, в виде репутационных потерь или прямой потери клиентуры из-за утечки данных).

При этом заметно, что планы правительства, особенно стран Европейского союза, по регулированию сбора, хранения и использования информации вместе с жесткими взысканиями за утечку данных становятся все шире. Этот тренд, по всей видимости, будет продолжаться и усиливаться, и это потребует дополнительной работы по управлению соблюдением законодательства в более широком аспекте, чем функция безопасности, и с обязательным участием СІО, CEO и советов директоров.

Для СІО многонационально рассредоточенной организации это крайне запутанная задача, так как подчиненная ему инфраструктура должна функционировать во многих зонах с разными законодательными требованиями. Совет директоров заинтересован во взаимосвязности и эффективности бизнеса

в масштабе всего предприятия, и СІО должен обеспечить условия, при которых всё будет работать эффективно и рационально, не спотыкаясь о новации законодательства о защите информации и управлении данными.

3. Угрозы безопасности данных

Хакеры стали более организованными, атаки — более изощренными, угрозы — более опасными, и всё это создает больше рисков для репутации компаний. А репутация бренда и динамика доверия со стороны поставщиков, покупателей и партнеров сегодня стали прямыми мишенями киберпреступников и хактивистов.

При буквально ежедневном изменении частоты атак и сложности их ландшафта бизнес нередко страдает от репутационного и финансового ущерба. СІО надо взаимодействовать с CEO, чтобы организация была полностью готова к этим постоянно обновляющимся вызовам и хорошо оснащена против кибератак на данные. В большинстве цепочек поставок присутствуют уязвимости, позволяющие хакерам завладеть интеллектуальной собственностью и секретными корпоративными данными через доступ к сторонним системам, что является настоящей головной болью для СІО, которым приходится строить стратегию управления своими системами с учетом множества многосторонних факторов.

Главное — в подготовленности

Сегодня ставки как никогда высоки, и мы говорим не только о персональной информации и краже личных данных. Под острием атак постоянно находятся высокоуровневые корпоративные секреты и жизненно важная инфраструктура. Предприятия должны знать важные тренды, связанные с последними или давними, но измененными атаками, и понимать, к чему надо быть готовым в ближайшем будущем.

Сегодня СІО пора проявить инициативу и начать работать с CEO и советом директоров, чтобы лучше подготовить свою организацию к постоянно меняющимся вызовам. Разобравшись в возможностях кибербезопасности, СІО могут существенно повысить свой авторитет в руководстве и свою роль в масштабе всей организации, что является важной целью большинства честолюбивых СІО.

компьютер или монитор во время работы излучает подобные электромагнитные сигналы. Современные методы разведки с использованием ПЭМИН позволяют перехватить информацию, которая обрабатывается в компьютере, и скрыто передать ее, не оставляя следов местонахождения разведчика.

Защита от «прослушки»

На сегодня в Государственной службе введена система организации и проведения научных исследований, которые осуществляются в основном в формате научно-исследовательских и опытно-конструкторских работ. Одним из ключевых исполнителей научных работ является Государственный научно-исследовательский институт специальной связи и защиты информации, созданный распоряжением Кабина в 2006 году.

Работы, которые выполняет институт, в основном охватывают создание современных отечественных средств криптографической и технической защиты информации, а также специализированного коммутационного, заключительного и вспомогательного оборудования. Инженерно-технические решения, применяемые в служебном процессе, позволяют внедрять весь технологический цикл создания специальных разработок — «от эскизно-технического решения до опытного образца».

За последние годы специалисты института разработали ряд средств, которые перекрывают пути утечки информации как акустическим способом, так и посредством перехвата электромагнит-



Универсальное автоматизированное рабочее место, защищенное от утечек по каналам ПЭМИН

ных излучений. В большинстве случаев принцип их действия построен на создании избыточного «шума» в возможном канале утечки, который сможет полностью перекрыть полезный сигнал.

Так, мобильный комплекс «Гарант-КТЗИ» предназначен для защиты речевой информации от утечки по акустическим и виброакустическим каналам при использовании в помещениях, которые временно служат для конфиденциальных переговоров. Комплекс помещается в небольшом чемодане и содержит моду-

ли, генерирующие виброакустический и акустический шум. Все модули являются автономными, работают на батарейках и не требуют внешнего питания. Комплекс «Гарант-КТЗИ» блокирует утечку виброакустической информации через оконное стекло, трубы системы отопления или водоснабжения. Есть также модули, предназначенные для установки в вентиляционных трубах и у дверей, то есть, в любых местах, через которые возможно подслушивание. Принцип их действия основан на генерировании акустического шума в канале.

Для защиты от утечки информации по каналам ПЭМИН предназначен генератор пространственного электромагнитного зашумления «Гарант-ПГШ-У». Данное изделие устанавливается у незащищенного электронного оборудования и создает мощный электромагнитный шум, который блокирует возможную утечку полезной информации.

Другой способ надежной защиты от утечек информации по каналам ПЭМИН — это применение компьютеров в защищенном исполнении. Речь идет о специальных экранящих футлярах для электронной техники, блокирующих любое электромагнитное излучение. При этом качество защиты должно быть проверено лабораторией, которая имеет соответствующий сертификат на право выполнения таких работ.

СОТНИ МАРШРУТИЗАТОРОВ CISCO ИНФИЦИРОВАНЫ В РЕЗУЛЬТАТЕ АТАКИ SYNFUL KNOCK

Количество инфицированных маршрутизаторов Cisco продолжает расти: специалисты обнаружили уже почти 200 IP-адресов в более чем 30 странах, которые были атакованы через внедренное вредоносное ПО в ПЗУ, известное как SYNful Knock. Это намного превышает первоначальное количество — 14 инфицированных маршрутизаторов FireEye, о которых было сообщено на прошлой неделе.

VAR'ы говорят, что новые сообщения о количестве выявленных атак не сказались на их продажах маршрутизаторов Cisco, но окажут влияние на сам процесс продажи клиентам.

«Это не проблема для канала в смысле самих продаж. Проблема для канала в том, что это затормозит продажи традиционной технологии маршрутизации, поскольку заказчики пересматривают теперь, как устанавливается оборудование на периметре сети», — пояснил руководитель VAR-компании, «золотого» партнера Cisco, попросивший об анонимности.

Mandiant, дочерняя фирма FireEye, подтвердила в своем блоге на прошлой неделе, что обнаружила 14 случаев внедрения вредоносного ПО в маршрутизаторы Cisco. Представитель Cisco пояснил в ответе на запрос CRN, что хакеры либо украли подлинные регистрационные данные администратора, либо сумели получить физический доступ к самим маршрутизаторам и вручную установили вредоносное ПО. Внедренный код дает им лазейку, которая может сохраняться и после перезагрузки.

Cisco уже обратилась к Shadowserver Foundation, партнеру в своей экосистеме, специализирующемуся на киберпреступности, и, согласно информации, опубликованной в понедельник, выявлено,

что были атакованы 199 постоянных IP-адресов в 31 стране.

«Важно подчеркнуть всю опасность этой вредоносной деятельности, — указывает Shadowserver в своем блоге в понедельник. — Инфицированные маршрутизаторы должны быть выявлены и очищены в срочном порядке».

Согласно информации от Shadowserver, самое большое количество инфицированных маршрутизаторов в США — 65; далее идут Индия (12), Россия (11), Польша (9) и Китай (8). Cisco ответила на запрос CRN, что три модели маршрутизаторов, которые

считалась возможной раньше, и оборона против нее — это следование передовым методам, прежде всего».

«Мы подчеркиваем с нашими командами поддержки клиентов, насколько важно просвещать заказчиков относительно передовой практики и предложить им содействие. Так что речь не о продажах оборудования Cisco; мы действительно просим наши команды сбыта пойти и помочь заказчикам обеспечить, что они защитили свою сеть всеми теми средствами, которые уже имеются», — пояснил представитель.



были инфицированы, — 1841, 2811 и 3825 — больше не выпускаются и не продаются уже «несколько лет». Поддержка данного оборудования истекает в следующем месяце, говорится на сайте Cisco.

«Это не уязвимость в нашей технологии, — пояснил представитель Cisco. — Это новый тип угрозы, которая не

VAR'ы говорят, что канал должен вести себя так же в отношении с клиентами, чтобы полностью понимать всю внутреннюю сеть заказчика, ее архитектуру и уровень защиты, дабы предотвратить такие атаки в будущем.

«Мы как партнер в канале не можем теперь просто прийти и сказать: вот

наша группа [продуктов] подключения, и давайте внедряйте эти маршрутизаторы», — говорит Джейми Шепард (Jamie Shepard), старший вице-президент по стратегии и системам для здравоохранения VAR-компании Lumenate, партнера Cisco. «Вы должны войти в это, поговорить со специалистами в безопасности, изучить архитектуру у заказчика, — сказал он. — Мы наблюдаем, что заказы на поставку при таком подходе откладываются, но они становятся крупнее, потому что мы вводим в это больше консалтинга».

Другие поставщики решений соглашались, что нужен более консалтинговый подход к продажам, чтобы понимать внутреннюю архитектуру и технологию у заказчика, что поможет исключить новые атаки. Также, говорят партнеры, хакеры с успехом взламывают старые модели оборудования, как это было с маршрутизаторами Cisco, потому что заказчики заняты внедрением новой облачной технологии, забывая при этом про «дыры» в унаследованном оборудовании.

«Эта атака SYNful Knock касается лишь некоторого такого унаследованного оборудования, которое не в полной мере интегрируется с новыми процессами, и хакеры используют эти уязвимости, — говорит «золотой» партнер Cisco. — Можно сказать: VAR'ы и канал в целом должны стать еще более ценными для своих заказчиков, лучше узнавая их [сеть] изнутри».

Cisco сообщает, что предлагает свое содействие заказчику конкретно по атакам SYNful Knock, объясняя, как предотвратить, обнаружить и устранить эту угрозу. В частности, предлагается инструмент «Snort Rule», который проводит анализ сети заказчика, чтобы определить, есть ли риск и не инфицирована ли сеть таким вредоносным ПО.

МЕГ УИТМАН: ГИБРИДНАЯ ОБЛАЧНАЯ ИНФРАСТРУКТУРА – ЭТО БУДУЩЕЕ

СТИВЕН БЕРК

Главный управляющий Hewlett-Packard Мег Уитман заявила аналитикам Уолл-стрит, что новая компания корпоративных решений, которая войдет в список Fortune 50, имеет сильные предположения гибридного облака в рамках своего облачного бизнеса с доходом 3 млрд. долл., который будет расти на 20% ежегодно в ближайшие несколько лет.

«Облако — это крупный бизнес с высокими темпами роста, который мы монетизируем в объеме всего портфеля Hewlett Packard Enterprise», — заявила Уитман, сообщая первый прогноз облачных продаж новой компании корпоративных решений с оборотом 52,7 млрд. долл., которая официально станет отдельной с 1 ноября. «У нас очень ясная точка зрения: что гибридная инфраструктура — это будущее и та среда, которая больше всего отвечает потребностям наших заказчиков во всем мире. Мы действительно хорошо позиционированы», — подчеркнула она.

Сославшись на данные исследования рынка фирмы Bain & Co., которая оценивает совокупный среднегодовой темп роста частного облака в 24% в течение ближайших трех лет против 17% у общедоступного облака, Уитман подчеркнула, что рынок гибридных облачных решений гораздо больше и богаче возможностями, чем рынок общедоступных облачных услуг.

Это наступление HP на рынок гибридного облака — своего рода вызов гиганту Amazon Web Services, чей бизнес общедоступных облачных услуг с доходом 7,2 млрд. долл. вырос на феноменальные 81% в последнем финансовом квартале.

Операционная прибыль AWS составила 21% в том же квартале против 17% за предыдущий период.



Мег Уитман

Уитман подчеркнула, что HP, спектр предложений которой охватывает стратегический консалтинг, серверы, СХД и сетевое оборудование, а также ПО, имеет полный портфель корпоративных гибридных решений. Она указала на сделку облачного аутсорсинга с Seadrill Management Limited, глобальной компанией шельфового бурения для добычи нефти, как пример такой возможности, делающей HP самым привлекательным стратегическим партнером в облаке.

Seadrill Ltd. переносит свою штаб-квартиру из Норвегии в Великобританию, и HP выиграла контракт на миграцию ее тридцати двух важнейших приложений в управляемое виртуальное частное облако, что должно занять менее шести месяцев. «Эта платформа дает пристанище всем критически важным корпоративным приложениям и данным

компании в рамках защищенной среды без высокой стоимости владения и управления собственным центром обработки данных», — отметила Уитман.

Также HP берет на себя управление сотнями серверов Seadrill Ltd. в других сегментах ИТ-среды, включая 56 серверов на буровых платформах по всему миру. «Мы обеспечиваем себе особое место на рынке, являясь поставщиком исчерпывающих решений для крупных заказчиков, таких как Seadrill, а не просто одним пунктом их общего ИТ-решения», — подчеркнула Уитман. «Это дает вам понятие о возможностях Hewlett Packard Enterprise и о том, как мы выигрываем в финансовом отношении от всеобщего перехода в облако», — сказала она аналитикам.

Майк Строл (Mike Strohl), главный управляющий VAR-компании Entisys (№ 227 в списке CRN «Solution Provider 500» 2015 года), говорит, что наблюдает кардинальный сдвиг на рынке — всё больше заказчиков переходят из общедоступного в частное облако, выстраивая свою долгосрочную стратегию в облаке.

«Заказчики начинают более стратегически относиться к облаку и смотрят на общую стоимость и доставку услуг с гибридными решениями и рабочими нагрузками, — сказал он. — Заказчики, тратившие много денег на общедоступное облако, начинают изучать предложения Flex Capacity от HP. Раньше у этих заказчиков не было выбора. Общедоступное облако было единственным предложением. Теперь они переносят свои рабочие нагрузки из общедоступного в частное облако».

Строл сравнил этот массовый переход в частное облако с другим похожим переходом, когда заказчики начали столь же

массово оценивать возможности СХД и перемещать данные с систем стандартного одноуровневого хранения на системы двух- и трехуровневого хранения исходя из критичности данных для всего их бизнеса.

Эта платформа дает пристанище всем критически важным корпоративным приложениям и данным компании в рамках защищенной среды без высокой стоимости владения и управления собственным центром обработки данных

В целом, говорит Строл, Hewlett Packard Enterprise гораздо агрессивнее продвигается на рынок частного облака в преддверии окончательного разделения, которое произойдет 1 ноября. «Это сделает бизнес Hewlett Packard Enterprise гораздо более гибким и позволит им быть более конкурентоспособными и вводить больше новаций в будущем», — сказал он.

Келли Айрленд (Kelly Ireland), учредитель и главный управляющий VAR-компании CB Technologies, платинового партнера HP, также наблюдает массовый переход корпоративных заказчиков в частное облако. «Мег права, — говорит Айрленд. — Частное облако — возможность гораздо большего масштаба. Она нацелена прямо на корпоративного заказчика. Мы ожидаем, что за следующий год наш облачный бизнес удвоится»

НАИБОЛЕЕ ВАЖНЫЕ НОВШЕСТВА MICROSOFT OFFICE 2016

ТОМ СПРИНГ, СРН/США

Функции коллективной работы, использование мобильных устройств и облака занимают центральное место в новой версии одного из главных программных пакетов Microsoft, Office 2016.

Добро пожаловать в MS Office 2016!

Пакет Microsoft Office 2016 теперь официально доступен для загрузки домашними и профессиональными пользователями. Список новшеств включает приезд на коллективную работу и мобильные устройства, всемерное использование облака, а также интеграцию обратной связи и данных в реальном времени в главные приложения Office.

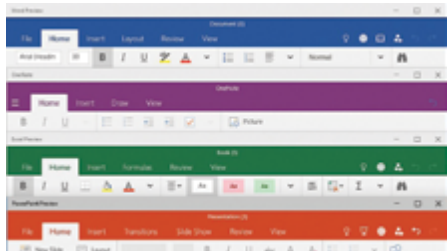


В очередной версии пакета компания привносит обновления в Word, Excel, PowerPoint, Publisher, Outlook, OneNote, Skype for Business, Access, Project и Visio. Помимо функциональности, в новой версии Microsoft берет приезд на безопасность, администрирование и изменения в интерфейсе для использования пакета на различных устройствах.

Пакет Office 2016 доступен для загрузки начиная с 22 сентября. Итак, главный вопрос: следует ли решаться на апгрейд? Попробуем помочь вам с ответом.

Еще красивее!

Office 2016 включает красочные новые темы, больше соответствующие темам Windows 10, а также последние релизы приложений для Mac OS, iOS и Android. Цветовые опции показаны на лентах приложений: синий у Word, зеленый у Excel и красный у PowerPoint. Сами ленты также слегка перестроены, чтобы освободить место для постоянно присутствующего поля поиска «Tell Me».



Окошко поиска «Tell Me»

Чтобы помочь пользователям работать в приложениях Office 2016 с максимальной продуктивностью, Microsoft добавила окошко «Tell Me», которое непрямо сидит в центре панели заголовка в программах Word, Excel и PowerPoint. Поле поиска встроено в ленту панели заголовка справа от символа лампочки и выводится с готовой подсказкой «Tell me what you want to do...».

Если пользователю нужна помощь — например, чтобы понять, как вывести изображение экрана на второй монитор, создать графики в Excel или поместить водяной знак в документ Word, — достаточно спросить об этом в окошке «Tell Me». Просто начните вводить свой вопрос обычным языком — и Microsoft постарается сузить для вас варианты поиска до наиболее подходящего ответа.

«Закулисные» меню

Меню второго уровня (backstage menu) — это те, которые обычно появ-

ляются, когда вы пытаетесь открыть, закрыть, сохранить, переслать или экспортировать документ. В Office 2016, к примеру, панель «Info» показывает больше сведений о файле, так что пользователю не нужно щелкать мышью снова, чтобы увидеть все сведения. Можно посмотреть и дополнительные сведения о файле, которые обычно не показаны и требовали еще пары кликов мышью: это дата создания файла, последнего изменения, последнего вывода на печать и размер в байтах.

Упрощение вызова файлов

«Задние» меню в Office 2016 дают также упрощенный доступ к сохранению или открытию файлов с облачного диска OneDrive или OneDrive for Business. Суть в том, что Microsoft старается охватить все различные версии Office, работающие в среде Windows, Mac OS, iOS и Android. Вам нужен последний файл, который вы редактировали? Просто войдите в меню второго уровня на вашем iPad и загрузите его.

Вся история версий

Акцент на пересылке и хранении файлов в новом Office 2016 включает также улучшенные инструменты для обнаружения истории версий файлов. Теперь можно очень просто узнать, какая версия файла хранится на SharePoint и на OneDrive for Business. Просто щелкните мышью на команде «History» в меню «File» — и увидите текущую версию или сможете восстановить более раннюю версию файла.

Редактирование — в реальном времени!

Microsoft добавила также функцию, которую пользователи Google Docs давно уже полюбили, — совместное редактирование в реальном времени в документах Office. Пока что она предложена в Office Online, но вендор говорит, что эти возможности будут расширены на приложения Office 2016 начиная с Word. Microsoft заверяет, что коллективная работа станет проще для групп удаленных пользователей, помогая всем участникам «быть на одной и той же странице».

Быть в курсе в каждый момент

Один из аспектов коллективной работы в Word — видеть, что делает другой участник, в процессе того как он это делает. Чтобы достичь этого, Microsoft добавила функцию «Real Time Presence», которая позволяет каждому участнику видеть, где именно в документе другие вводят правку.

Sway — новый онлайн-инструмент презентаций

Sway преподносится как новая классная программа презентаций — лучше, чем дедовский PowerPoint. Она позволяет «перетащить» фотографии, видео и другие файлы из YouTube, Facebook, Twitter, с компьютера или OneDrive в веб-браузер, в приложение на смартфоне или планшете. После этого можно организовать контент удобным образом и общаться «в нелинейной манере» (по типу PowerPoint), говорит Microsoft.



Да, программа OneNote — тоже «собирает контент». Но Sway, говорит Microsoft, это программа для показа

готовых идей, тогда как OneNote — это окошко, в которое мы складываем идеи до того, как ими поделиться.

Sway, с которой можно познакомиться начиная с октября, будет предложена в Office 2016, а также бизнес-пользователям и клиентам в сфере образования в Office 365 ближе к концу года.

Меню стали умнее

Меню в Office стали умнее, говорит Microsoft, упростив сохранение, открытие и поиск файлов. К примеру, в окошке «Browse» в Word теперь лучше видно файлы, и стало гораздо проще найти нужные. Вкладки «Open» и «Save As» также упрощены и стало проще выбрать место, куда сохранить файлы — на локальный диск или в OneDrive.

Встроенная бизнес-аналитика

В новом Excel 2016 Microsoft решила встроить функцию «Power Query» в саму программу, так что теперь не нужно загружать этот модуль отдельно. Этот инструмент позволяет комбинировать собственные данные пользователей и сторонние данные прямо из самой программы, что, в свою очередь, дает возможность решать довольно сложные задачи, касающиеся обнаружения, комбинирования и очистки данных из самых разных источников.



С помощью Power Query можно импортировать в Excel структурированные или неструктурированные данные из общедоступных источников, в том числе таблиц Википедии, с сайтов Azure Marketplace и Data.gov, после чего, используя встроенный синтаксический анализатор JSON, создавать визуализации данных, построенные на Big Data или Azure HDInsight.

Полезные новшества в Outlook

В приложении Outlook особенно порадовало обновление меню. В версии Outlook 2016 когда пользователь добавляет вложение в электронную почту, опция «Attach File» включает теперь пункт «Recent Items», где перечислены любые документы Office, которые были недавно закрыты. Благодаря этому не нужно заниматься разыскиванием только что отредактированного файла через «Browse», чтобы переслать его коллеге.

• **Новый подход к вложениям почты.** Чтобы избавиться от случаев, когда общие документы, отправленные нескольким получателям, редактируются или рецензируются в устаревшей версии, Microsoft добавила новую функцию под названием «Modern Attachments». Эти вложения привязаны к электронной почте через облако. Это означает, что когда прикрепленный файл сохраняют или извлекают, он автоматически отправляется в облако.

• **Создание групп в Outlook.** Согласно концепции сегодняшней рабочей среды, как видит ее Microsoft, коллективная работа строится главным образом через электронную почту, видео, мгновенный обмен сообщениями (IM), а также виртуальные и «живые» совещания. Чтобы еще больше способствовать этому сотрудничеству и взаимодействию, Microsoft добавила специальные группы, названные «365 Groups», «Outlook Desktop Groups» и «Office 365 Enterprise Mailboxes».

Очевидно, окончательное название пока не придумано. С помощью этой функции пользователи «настольной» версии Outlook 2016 могут создавать группы и управлять ими. Прямо из программы Outlook можно отслеживать всю деятельность в группе, вызывать предысторию переписки и управлять

файлами и заметками группы, хранимыми на OneDrive.

• **Хлам — отдельно!** В новом Office 2016 Microsoft вооружает пользователя новыми средствами внутри Outlook, чтобы противостоять натиску электронной почты, которую мы получаем сегодня ежедневно. Эта функция носит название Clutter; она перемещает письма с низким приоритетом из ящика входящей почты в специальную папку, также красноречиво названную «Clutter» (Хлам).



Компания поясняет, что функция Clutter — интеллектуальный инструмент, анализирующий поступающий поток писем. Если она определит, что те или иные письма будут скорее всего проигнорированы получателем, то помещает их в папку «Clutter» внутри Outlook. Когда эта функция активирована в настройках программы, одноименная папка появляется во всех установленных экземплярах Outlook — на смартфоне, планшете и т. д.

• **Умный поиск.** Outlook обрел более интуитивные функции поиска писем в ящике входящей почты. Если программа видит, что пользователь производит поиск по имени, то «догадывается», что он ищет прошлую переписку с этим человеком, и покажет отфильтрованные результаты по мере набора имени.

Новый уровень безопасности

Microsoft повышает уровень безопасности в Office 2016, вводя специальные средства для предотвращения утечки данных и управления правами доступа к файлам. Администраторы могут теперь активировать и задать политики «Data Loss Prevention» для Word, Excel и PowerPoint.

С точки зрения администрирования, политики должны препятствовать утечке данных, позволяя администратору задать ограничения: какие файлы можно послать и кому, а также запретить «копировать» данных за пределами приложения Office 2016.

ИТ-администраторы могут ввести ограничения в диапазоне от «уведомлений» о нарушении (разрешив пользователям «отменить» правила с достаточным на то основанием) до полной блокировки распространения контента. Также, Microsoft добавила шифрование на уровне файлов в Outlook, Word, Excel и другого контента. Кроме того, можно задать сохранение данных в Customer Lockbox, чтобы исключить доступ самой Microsoft к конфиденциальной информации.



Защита в Word

В новой версии пакета функции «Data Loss Prevention» включены теперь в Outlook, Word, Excel и PowerPoint. Пользователь получит предупреждение прямо внутри программы при попытке сохранить файл, содержащий конфи-

денциальную информацию, в каталог, папку или сервис, где он может оказаться незащищенным.

Об обновлениях...

Как и в новой Windows 10, Microsoft изменила процесс обновления для Office 2016 в том, что касается доставки критичных заплат, устраняющих уязвимости, исправлений багов, не связанных с безопасностью, а также новой функциональностью.

Потребительская версия Office 2016 должна устанавливать обновления автоматически, когда они присылаются. Для бизнес-пользователей компания следует тем же курсом, что и с Windows 10 — «делайте апгрейд, а не то...».

Обновления для бизнес-пользователей Office 365 и Office 2016 будут выпускаться с разными интервалами. Первый будет обновляться ежемесячно, по плану «Current Branch». Второй — «Current Branch for Business» — будет доставляться каждые четыре месяца. Клиенты программы «Current Branch for Business» могут отложить обновление на четыре месяца, но по истечении этого срока они будут полностью исключены из списка рассылки патчей.



Упрощение администрирования

«Click-to-Run» — известная всем технология, призванная сократить время на загрузку, установку и запуск нового ПО.

В новой версии Office 2016 добавлены расширения, о которых давно звали ИТ-администраторы: улучшено управление трафиком в сети (при развертывании Office в среде с ограниченной полосой пропускания), расширены возможности управления дистрибуцией ПО (более тесная интеграция с ConfigMgr), гибкое управление обновлениями (для багов, уязвимостей и новой функциональности) и упрощено управление активацией (новый инструмент Admin Portal для активации устройств).



Инструмент SmartArt

Для пользователей, работающих над документами со значительным объемом графики, добавлен инструмент SmartArt; он применим к документам, хранящимся в облаке. SmartArt позволяет открыть файл Word, Excel или PowerPoint 2016 без диаграмм и изображений — то есть пользователь может открыть и редактировать файлы большого размера, не загружая документ целиком. Строка состояния показывает, сколько придется ждать для загрузки остальной части документа, если это потребуется.

Это должно быть удобно для тех, кто работает с Office 2016 в условиях ограни-

ченной полосы пропускания — например, по сотовой сети.

Skype — внутри приложений

В новой версии Microsoft более тесно интегрировала Skype в пакет Office. Теперь можно инициировать речевые и видеозвонки, а также чат мгновенных сообщений прямо из документов приложений Office.

Справочный поиск через Bing

В новый Word, PowerPoint, Excel и Outlook встроена также функция под названием «Smart Lookup». Идея такова: если нужно быстро проверить какой-то факт или провести быстрый поиск в Web слова или фразы, содержащихся в документе, то достаточно просто выделить их в документе. Используя Bing, Office 2016 сам проведет быстрый поиск и даст просмотреть результаты запроса в отдельном окне внутри редактируемого документа, так что не нужно будет метаться между веб-браузером и самим приложением.

Веб-приложения

Есть еще инструмент, который Microsoft обещает, но пока не предложила пользователям, — это веб-приложения. Одно из таких веб-приложений под названием

Planner Hub — это информационная панель (dashboard), которая показывает графику планов, проектов и заданий в организации. Этот инструмент — воплощенная мечта менеджера проектов, она дает обзор всех проектов и состояния дел «с высоты птичьего полета».

Для каждого проекта есть отдельная «корзинка» или карточка, которая показывает срок исполнения, статус, кто руководитель проекта, а также имена всех членов команды. Достаточно щелкнуть мышью на карточке и затем выбрать те или иные пункты, чтобы узнать, на какой стадии исполнения находятся те или иные части проекта, идут ли они в графике или просрочены.

Стоимость

Сколько он будет стоить? Автономная версия пакета Office 2016 Home & Student (включает Word, Excel, PowerPoint и OneNote) стоит 149 долл., а версия Office Home & Business (добавлен Outlook 2016) — 229 долл. Еще один вариант — Office 365, который стоит 7 долл. в месяц (тарифный план Personal с установкой на одно устройство) либо 10 долл. в месяц (Home Plan с разрешенной установкой на пять устройств и пять смартфонов). Версия Microsoft Office Professional 2016 стоит 400 долл. за один ПК.

Как купить

Office 2016 продается в розничных салонах или с сайта. Владельцы подписки на Office 365 могут просто подождать — им будет автоматически загружен апгрейд в ближайшие недели. Организации с корпоративной лицензией, в том числе по программе Software Assurance, смогут загрузить новый код начиная с 1 октября.



С 2003 г. Softkey.ua сохранила 894 дерева, потому что продает софт online!
Программное обеспечение online не требует изготовления коробок.

Береги лес – покупай софт online!

www.softkey.ua

+380 (44) 377-77-16



UAPAY ПРЕДЛАГАЕТ ИННОВАЦИОННУЮ СХЕМУ ПОЛУЧЕНИЯ КОМИССИОННЫХ ДОХОДОВ



СЕРГЕЙ САВКА, АЛЕКСАНДР ШУЛЬГА

В последние несколько лет банковский сектор столкнулся с резким падением доходов. Платежный сервис UAPAY предлагает банкам инновационные продукты, которые позволяют им получить альтернативные источники прибыли.

В связи с кризисной экономической ситуацией в стране банки и финансовые учреждения испытывают непростые времена: привычные для них направления бизнеса и источники получения доходов в виде кредитования существенно сузились или полностью закрылись. Кроме того, дополнительное давление оказывают вопросы операционной эффективности, конкуренция и падение покупательской способности. В этих условиях банки вынуждены искать альтернативные источники доходов, способные компенсировать спад в кредитовании.

UAPAY — уникальный сервис, позволяющий потребителям оплачивать огромный спектр услуг по всей Украине (коммунальные платежи, Интернет, телевидение, мобильная и телефонная связь, ЖД-билеты и многое другое) по самым выгодным тарифам в широчайшей сети точек приема. Подключаясь к UAPAY, банк переходит от стандартной схемы обслуживания клиентов к инновационной и не затратной схеме получения комиссионных доходов, увеличивая при этом спектр предоставляемых услуг и средний чек.

На сегодняшний день платежи можно делать практически везде — на почте, через платежные терминалы или в офисах компаний, предоставляющих различные платные услуги. К последним, например, относятся операторы мобильной связи, интернет- и ТВ-провайдеры и т. д.

Когда основным источником дохода было кредитование, банки часто не предоставляли услуги по приему коммунальных платежей либо устанавливали очень высокие тарифы за их оказание. В нынешних же условиях банки делают упор на увеличение комиссионных доходов, одним из источников формирования которых являются операции по приему

платежей. Поэтому сейчас данную услугу начинают предлагать даже те банки, которые ранее ее не предоставляли.

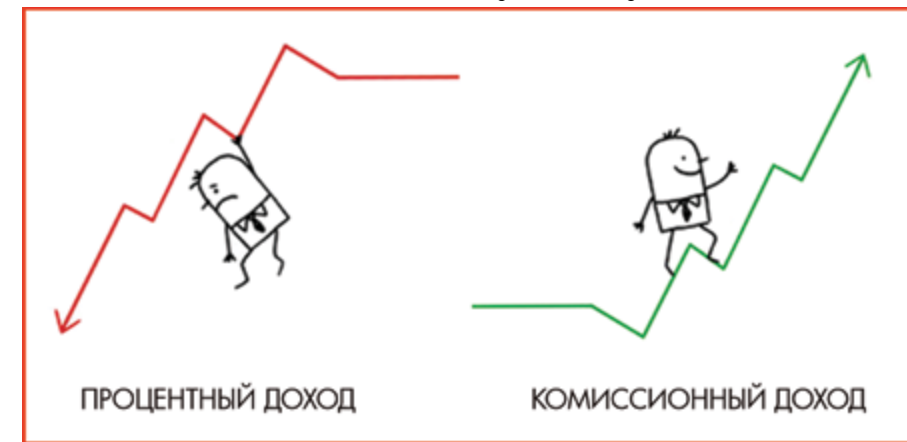
Учитывая вызовы времени и потребности партнеров, UAPAY приняла решение об активном развитии альтернативных продуктов и сервисов, которые могут предлагаться банкам в дополнение к «классическим». Речь идет о приеме платежей или валютнообменных операциях, совершаемых сотрудниками кассы банка.



Сергей Савка

директор по альтернативным продуктам и сервисам

Основная задача при внедрении таких продуктов и сервисов заключается в том, чтобы сохранить существующий подход, исповедуемый компанией UAPAY — работа сотрудника кассы в едином окне и в сжатые сроки по SLA (Service Level Agreement), связанному с приемом платежей от клиентов.



Среди дополнительных услуг можно отметить:

- реализацию альтернативных сервисов (страхование, assistance-продукты) в едином окне АРМ UAPAY совместно с основными сервисами;
- таргетирование альтернативных сервисов, исходя из типа транзакции, которую осуществляет клиент;
- «продающую» фронт-систему, нацеленную на активную продажу альтернативных сервисов;
- активные кросс-продажи альтернативных сервисов;

простые сервисы, реализация которых не требует много времени для их продаж.

Сегодня UAPAY предлагает своим партнерам сотрудничество по двум типам услуг: продукты на сдачу и домашний assistance «Мастер-Сервис». Стоит отметить, что уже в ближайшем будущем перечень услуг для сотрудничества будет значительно расширен.

Продукты на сдачу — это предложение страховать риски клиента (личное, движимое и недвижимое имущество, пр.) на выбранную им сумму за счет сдачи (включая копейки), которая остается у него после совершения основной операции, такой как оплата коммунальных и прочих платежей. Общее количество договоров, которые может заключить клиент, не ограничено.

Преимущества для клиента:

- Наличие договора страхования — это требование времени. Медицинские услуги, лекарства, восстановление поврежденного имущества достаточно затратны. Приобретая страховую полис, клиент минимизирует возможные расходы в случае наступления страхового события.
- Полезное вложение «незаметных денег» — покупка страхового полиса никогда не бывает лишней, однако она часто откладывается клиентом «на потом». Это происходит в силу отсутствия в данный момент необходимой суммы денег. Именно тогда на помощь приходит страхование на небольшие

суммы за малые и часто «незаметные» деньги.

Домашний assistance «Мастер-Сервис» — уникальное на рынке Украины предложение от UAPAY, которое объе-

диняет страхование ответственности владельца квартиры перед третьими лицами (соседями) и сервис по оказанию услуг ремонта (слесарные, сантехнические, электротехнические) в случае возникновения непредвиденных ситуаций в процессе эксплуатации жилья.

UAPAY предлагает своим партнерам ряд инновационных продуктов, которые позволят им расширить перечень оказываемых услуг, продавать их макси-



Александр Шульга

директор по развитию и продажам

мально эффективно и зарабатывать там, где ранее партнер этого не делал. Среди таких продуктов:

- «продающая» IT-платформа. Система сама предлагает сервисы клиенту;
- отсутствие платы за разработку при внедрении альтернативных сервисов;
- отсутствие необходимости согласовывать отдельные договоры на внедрение сервисов, в том числе с поставщиками альтернативных сервисов;
- финансовые взаимоотношения Вы — UAPAY;
- отсутствие НДС;
- отсутствие необходимости аккредитации поставщиков альтернативных сервисов и проведение длительных процедур согласования внутри банка;
- минимальный документооборот;
- ежедневная аналитика;
- большинство договоров с поставщиками альтернативных сервисов производится с использованием факсимильной печати и подписи;
- поддержка любого типа мотивации продавцов.

А теперь задумайтесь, сколько времени и сил у вас займет самостоятельное внедрение подобных сервисов, включая доработку со стороны IT-службы, согласование с back-офисом, бухгалтерией и прочими службами?

Авторы статьи —
директор по альтернативным продуктам и сервисам UAPAY, Сергей Савка,
директор по развитию и продажам UAPAY, Александр Шульга

НЕДОРАБОТКИ И НЕУДОБСТВА В WINDOWS 10

Прошло уже несколько месяцев тех пор, как стартовала Windows 10. Новая ОС успела заслужить многочисленные похвалы экспертов отрасли и партнеров в канале. Не обошлось, конечно, без багов и недочетов, но к чести компании нужно сказать, что Microsoft устраняет их со всей возможной быстротой. Тем не менее, новая ОС всё еще не идеальна: с каждым релизом нового прикладного ПО или аппаратного компонента выявляются те или иные нестыковки.

Скажем сразу: самое большое недовольство связано с отсутствием прозрачности при автоматической установке обновлений в Windows 10. Замечены и откровенные баги: пользователи после апдейда жалуются на мерцающий экран в некоторых программах, капризный Wi-Fi и почти уже забытый «синий экран смерти».

Вот главные из проблем и неудобств, о которых сообщили первые пользователи Windows 10 на текущий момент.

В своей новой операционной системе Microsoft изменила подход к доставке плановых обновлений. В прежних версиях Windows 8.1 и Windows 7 компания сообщала больше подробностей, какие именно обновления устанавливаются. В Windows 10 ИТ-менеджеры остаются в неведении относительно того, что именно устанавливается; они требуют, чтобы компания предоставила более подробные сведения о содержании обновлений.

С момента старта новой ОС компания предоставляла лишь ограниченные описания при устранении обнаруживающихся недочетов. В сентябрьском обновлении для Windows 10 в качестве описания было предложено следующее: «Данное обновле-

ние включает улучшения, чтобы облегчить процесс апдейта на Windows 10».

Неудивительно, что на сайте предложено для улучшения ОС (Windows Feature Suggestions) одно из самых популярных звучит так: «Нам нужны более содержательные пояснения базы знаний (knowledge base articles) к релизам обновлений Windows 10». К таким предложениям присоединяются многие члены сообщества.

Просматривая страницы поддержки на сайтах каждого из ПК-вендоров, приходится сделать вывод, что при апдейте на новую ОС на системах Dell, Hewlett-Packard и Lenovo могут возникнуть проблемы с Wi-Fi.

Если вы испытываете повторяющиеся зависания или сбои браузера Chrome на своем ноутбуке с Windows 10, то знайте: не вы одни. Поначалу многие думали, что






проблема связана с обновлением браузера, предложенным некоторое время назад. Однако новейшая версия Google Chrome (v.45.0.2454.85) продемонстрировала те же симптомы. Официального исправления пока не предложено, но есть временное решение: удалить текущую версию Chrome и затем загрузить более раннюю (не сбойную) версию браузера — например, с сайта FileHippo.

Тех, кто перешел на Windows 10 или приобрел новый ПК с этой ОС, встречает теперь новый браузер Edge от Microsoft; он же используется для чтения PDF-документов и служит окном в Web для Cortana. Чтобы изменить браузер по умолчанию, используемый ассистентом Cortana, следует открыть меню «Пуск» и ввести запрос «default app settings», в показанном списке найти Microsoft Edge и изменить его на желаемый.



pay

НАЦІОНАЛЬНИЙ ПЛАТІЖНИЙ СЕРВІС

-  Комунальні платежі
-  Інтернет, телебачення
-  Мобільний та стаціонарний зв'язок
-  Фінансові послуги
-  Альтернативні сервіси

1600+
сервісів

20+
банків
партнерів

2000+
точок
обслугову-
вання

БІЛІНГ

КЛІРИНГ

ПРОЦЕСИНГ

- ◆ **ВИСОКА ШВИДКІСТЬ ОБСЛУГОВУВАННЯ**
- ◆ **БЕЗКОШТОВНЕ ПІДКЛЮЧЕННЯ** ◆ **ВИГІДНА КОМІСІЯ**

www.uapay.ua ◆ +38 044 364 11 22 ◆ salles@uapay.ua

РИСКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ ПОДДЕЛЬНЫХ КАРТРИДЖЕЙ – ЧТО В ВАШЕМ ПРИНТЕРЕ?



Не дайте підробкам вас ошукати
hp.com/anticounterfeit

Производство и реализация контрафактной продукции оказывают огромное влияние на рынок: компании теряют значительную часть прибыли и репутацию, а потребители получают низкокачественный поддельный товар, а не тот, за который заплатили.

«Производители контрафактной продукции попросту обманывают потребителей: потребители думают, что покупают оригинальные фирменные товары, тратя свои с трудом заработанные деньги на некачественные изделия», — поясняет Дэйв Купер, директор службы по корпоративным решениям продукции Hewlett-Packard и Программы по борьбе с контрафактной продукцией. «Компания HP очень серьезно относится к подделке производимой ею продукции, поэтому мы являемся ведущей в отрасли глобальной командой специалистов по борьбе с контрафакцией, работающих над ее устранением с рынка, чтобы каждый клиент, имел возможность получить подлинное изделие».

Однако усилий со стороны компаний и правоохранительных органов недостаточно. Сами потребители должны принимать активное участие в обнаружении подделок, которые обманным путем лишают их собственных денег в обмен на низкое качество в «подлинной обложке».

Аналоги продукции не являются незаконной имитацией оригинала в случае, если компания не использует имя торговой марки, а товары производятся и реализуются в упаковке, не копирующей оригинал

По оценкам Всемирной таможенной организации (WCO) и Международной Торговой Палаты (ICC), мировой объем реализуемых товаров на 10% состоит из контрафактной, пиратской и продукции «серого» рынка, а ежегодный экономический и социальный ущерб мировой экономики составляет до \$775 млрд. Согласно прогнозам, эта цифра достигнет \$1,7 трл. к 2015 году. Кроме того, статистика утверждает, что в результате производства поддельной продукции на территории стран «Большой двадцатки», оказалось потеряно около 2,5 млн рабочих мест.

Масштабы пугающие, однако, экспертов Hewlett-Packard по борьбе с контрафактной продукцией это не останавливает. «Война против производителей контрафактной продукции набирает обороты, и в этих условиях компания HP объединяется с другими мировыми брендами и международными организа-

циями в поисках новых способов борьбы. Нашим приоритетом является защита клиентов компании от незаконных мошеннических действий организаций, производящих некачественную и потенциально опасную продукцию для получения легкой прибыли за счет средств ничего не подозревающих клиентов», — отмечают они

Что такое контрафактная продукция? Контрафактная деятельность — несанкционированное применение или использование зарегистрированного товарного знака на продукции, произведенной без лицензии владельца бренда. Поддельный товар имитирует оригинальную продукцию без соответствующего на то разрешения с целью получения максимальной прибыли.

Важно отметить, что аналоги продукции не являются незаконной имитацией оригинала в случае, если компания не использует имя торговой марки, а товары производятся и реализуются в упаковке, не копирующей оригинал. Незаконным является полное или частичное копирование продукции, вводящее клиентов в заблуждение относительно того, приобретают они оригинальную или не оригинальную продукцию.

Так, поддельные картриджи могут с огромной вероятностью поломаться или протечь, что в итоге приведет к поломке принтера или аннулированию гарантии на него. Возможно, придется платить за ремонт печатного оборудования или даже покупать новое. В отличие от подделок, оригинальные расходные материалы производства Hewlett-Packard не только обеспечивают стабильную работу оборудования и более высокое качество печати, но и позволяют эффективнее использовать чернила. Результаты недавнего исследования, проведенного организацией Buyers Laboratory, позволяют сделать вывод о том, что в среднем, оригинальные картриджи для струйных принтеров производства компании HP позволяют напечатать до 50 процентов больше страниц, чем заправленные или переработанные альтернативные изделия.

Исключительными эксплуатационными характеристиками и возможностью обеспечения стабильных результатов печат-

ни подлинные картриджи для принтеров HP обязаны масштабным инвестициям и испытаниям, что в совокупности гарантирует качество и надежность по конкурентоспособной цене. Именно по этой причине результаты недавнего комплексного исследования, проведенного агентством QualityLogic подтвердили факт отсутствия каких-либо дефектов в картриджах HP. С другой стороны, у более 40% картриджей сторонних поставщиков в ходе исследования были выявлены те или иные неисправности.

На контрафактные товары, представляющие собой продукцию, изготовленную в нарушении законов и перевозимую через границу контрабандным путем, не распространяется действие законов в области охраны окружающей среды и обеспечения безопасности потребителей, строго соблюдаемых производителями лицензионной продукции. Использование при неле-

не менее, существуют и другие признаки, которые могут указывать на то, что картридж не является подлинным изделием. Оригинальные расходные материалы HP всегда поставляются в новом виде — без каких-либо повторных заправок или переработок — в запечатанных упаковках высокого качества.



Для того чтобы потребителям было еще проще защитить себя от подделок, компания HP разработала инновационное программное обеспечение для проверки подлинности продукции (Authentication Software), которую пользователи могут установить на свой ПК. Данное бесплатное программное обеспечение запускается автоматически при установке нового картриджа, и при обнаружении чего-либо необычного в картридже, предупреждает пользователя соответствующим сообщением и выдает дальнейшие инструкции.

Оригинальные картриджи также снабжаются сложными голографическими контрольными марками и штрих-кодом быстрого реагирования (QR), который клиенты могут легко проверить с помощью смартфона или в режиме онлайн через сайт www.hp.com/go/ok. При сканировании QR-кода генерируется мгновенное сообщение:

если этикетка действительно, система генерирует сообщение, подтверждающее подлинность изделия. Сообщение о недействительной этикетке указывает на то, что изделие не является подлинным. Таким образом, компания HP старается максимально защитить своих потребителей, помогая сохранить их время и деньги.

Основным признаком, отличающим оригинал от подделок, является высокое и стабильное качество печати. Тем



Відскануйте код. Захистіть свій бізнес.



Не дайте підробкам вас обшукати.

Підроблені видаткові матеріали – це серйозна проблема, ніж гадає більшість людей. Вони псують ваші принтери, ваші фінансові показники та навколишнє середовище. Вони можуть виглядати як справжні. Відскануйте QR код та переконайтеся, що в ваших руках якість Original HP. Тому що захищати свої інвестиції – це важливо. Дізнайтеся більше на hp.com/go/anticounterfeit

Make it matter.



Переконайтеся, що ви отримуєте справжні тонери та чорнила Original HP

Крок 1

Завантажте програму для зчитування QR кодів



Крок 2

Відскануйте QR код на коробці HP тонера та чорнила



Крок 3

Після сканування на екрані вашого телефону з'явиться підтвердження від HP



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: В ПОИСКАХ СОВЕРШЕННОЙ ЗАЩИТЫ

Согласно отчетам аналитиков Gartner, затраты на ИБ в этом году возросли на 8,2%, а общий объем глобального рынка кибербезопасности в 2015 году составил 77 млрд долл. В 2018 году объем этого рынка достигнет 101 млрд долл., а к 2020 году данная цифра вырастет до 170 млрд долл.

В соответствии с прогнозами Markets and Markets, совокупный годовой темп роста рынка ИБ в последующие пять лет составит 9,8%. Авиакосмическая индустрия, оборонная промышленность и некоторые наиболее ИТ-зависимые отрасли станут крупнейшими потребителями решений по кибербезопасности.

Северная Америка и Европа являются главными регионами для рынка кибербезопасности, отмечают анали-

тики из TechSci Research. Азиатский-тихоокеанский регион быстро развивается как потенциальный рынок для провайдеров решений по кибербезопасности. Драйверами этого тренда являются ведущие экономики региона, такие как Китай, Индия и Юго-Восток Азии, которые в последнее время подвергаются мощному киберинфильтрации со стороны других стран, что стимулирует построение качественно защищенного киберпериметра.

По мнению аналитиков IDC, среди наиболее быстро растущих сегментов ИБ можно отметить аналитические и SIEM-решения (10%), системы защиты и аналитики вторжений (свыше 10%), защитное ПО для мобильных устройств (18%) и облачную безопасность (50%).

Согласно отчету Markets and Markets, рынок облачной безопасности вырастет к 2019 году до 8,7 млрд долл.

Рынок «песочниц» для сетевой безопасности (network security sandbox market), который практически не существовал еще несколько лет назад, сейчас испытывает бурный рост. Это обусловлено стремительным расширением АРТ-угроз и влечет за собой поведенческий подход к детектированию вредоносного ПО. Новый отчет от Frost & Sullivan — «Network Security Sandbox Market Analysis» — указывает, что этот рынок увеличится с 537 млн долл. в 2014-м до 3,5 млрд долл. в 2019-м.

Эксперты IDC прогнозируют, что до конца 2015-го около 20% проприетарных данных в облаке будет размещено в зашифрованном виде, а к 2018 году эта цифра

увеличится до 80%. Рынок систем шифрования к 2019 году составит 4,82 млрд долл., полагают в компании Markets and Markets.

Увеличение рынка облачных вычислений, виртуализация и растущее число атак на дата-центры стимулируют развитие рынка безопасности ЦОДов. Прогнозируется, что он достигнет планки в 8,13 млрд долл. к 2020 году.

Рынок страхования от киберугроз за последние два года вырос с 1 млрд долл. до 2,5 млрд долл. При этом 2014 год стал важной вехой для него, поскольку число компаний, предлагающих услуги страхования от киберугроз, равно как и число их заказчиков, резко увеличилось. Спрос на подобные страховые услуги вырос на 21% во всех индустриях, а в банковском секторе рост составил 29%.

ОСНОВНЫЕ ТЕНДЕНЦИИ НА РЫНКЕ ИБ В УКРАИНЕ

По мере того, как ИТ утверждает свое значение для развития бизнеса, растет и роль информационной безопасности. При этом государственный сектор, к сожалению, не является образцом для подражания, скорее наоборот — ряд кибератак прошлого года и несколько громких взломов первого полугодия 2015-го показали, что государство все еще уделяет очень мало внимания защите своего киберпространства.

Внедрение новых технологий — среди которых облачные вычисления и использование мобильных устройств для бизнеса — ведет к расширению диапазона решений для киберзащиты. Однако бюджеты на ИБ в условиях экономического кризиса не только не увеличиваются, а скорее повсеместно сокращаются.

Как ведет себя бизнес в ответ на вышеописанные вызовы? Какие тенденции сегодня можно выделить на украинском рынке информационной безопасности и каковы прогнозы по его развитию? Насколько украинский рынок ИБ отличается от западного и в чем именно заключается это отличие? Об этом мы решили спросить экспертов ведущих отечественных компаний.

По мнению Владислава Радецкого, Technical Lead, ВАКОТЕСН Group, новая реальность, в которой оказалась Украина, диктует существенно более высокие требования к безопасности. В том числе это относится к построению защиты информационных систем и данных. Множество инцидентов в области ИБ, которые произошли в течение последних двух лет, показывают слабую эффективность ранее существовавших подходов к обеспечению информационной безопасности, особенно в государственном сегменте.

На данный момент отмечается возросший интерес к широкому спектру решений ИБ: DLP, межсетевым экранам нового поколения, защите веб-приложений, системам управления уязвимостями, инцидентами информационной безопасности и т.д. К сожалению, развитию этого рынка не способствует ситуация в экономике — у многих заказчиков есть задачи, но нет ресурсов для их решения.

«Вариантом выхода из данной ситуации может быть появление в стране сильных компетентных партнеров, предоставляющих управляемые сервисы (Managed Services) в сегменте информационной безопасности. Если заказчики смогут получить необходимые инструменты для решения своих задач без капитальных затрат — это может быть интересно для рынка», — говорит Владислав Радецкий.

ОСОБЕННОСТИ ОТЕЧЕСТВЕННОГО СЕГМЕНТА ИБ

США и Европа находятся далеко впереди с точки зрения глубины проникновения технологий, уверен Владислав Радецкий. Там конечные заказчики хорошо понимают, зачем нужна информационная безопасность. И что это не только технологии, но также люди и процессы — всё в комплексе. Интеграторы в свою очередь уже давно работают в условиях жесткой конкуренции — постоянно совершенствуют как компе-

вторым заметным трендом является миграция с продуктов российских производителей, особенно в сегменте решений для защиты конечных точек. Их место занимают решения американских и европейских производителей, изначально недооцененные на нашем рынке.

Александр Фрасинюк, технический директор, Active Solutions, отмечает, что на рынке безопасности по-прежнему в тренде продукты, связанные с защитой корпоративных данных и безопасностью инфраструктуры, защитой от DDoS-атак и утечек данных в корпоративной среде.

С ним согласен Виталий Зарицкий, руководитель направления информационной безопасности компании, ITbiz Solutions: «Актуальными трендами ИТ-безопасности являются решения по защите от DDoS-атак корпоративного клиента, в том числе со стороны оператора связи, решения по защите от целенаправленных атак (АРТ), обеспечение безопасности систем онлайн-банкинга и мобильных платежей». Также есть движение к совместному использованию программных и аппаратных средств обеспечения безопасности: системы безопасности трансформируются в аппаратно-программные комплексы, выполняющие совокупные функции по защите охраняемого периметра, анализу контента и предотвращению вторжений.

Касательно прогнозов на будущее Виталий Зарицкий отмечает, что сегодня заказчики хоть и экономят, но все же осознают, что тенденции развития киберугроз становятся все более угрожающими. И понимая весь перечень рисков, с которыми они могут столкнуться (финансовые, репутационные и другие), они стараются более ответственно подходить к вопросам обеспечения информационной безопасности. Поэтому в ITbiz прогнозируют активизацию и рост рынка на следующий год.

В Украине исторически сложилась недооценка сегмента информационной безопасности как по значимости, так и по объемам финансирования, уверен Сергей Кишкурно, руководитель направления информационной безопасности и аудита, CISA, АМИ. Однако сейчас ситуация выравнивается: заказчики стали чаще уделять внимание аудитам ИБ, тестированию на уязвимости. Повышается и грамотность: больше руководителей компаний-заказчиков задумываются о потенциальных угрозах для корпоративной информации, ведь одних организационных мер при этом явно недостаточно, поскольку уровень киберугроз в мире

постоянно растет. Эти тренды работают на расширение рынка ИБ.

С другой стороны, в кризисное время чаще возникают трудности с финансированием проектов. Поэтому эффект расширения рынка ИБ не столь очевиден, зато формируется значительный отложенный спрос. И если в Украине действительно начнется обновление экономики, то через год можно будет говорить о реальном увеличении объемов рынка ИБ.

Николай Коцурский, архитектор решений ИБ, БМС Консалтинг, считает, что на текущее развитие рынка ИБ в Украине, помимо основных требований бизнеса по защите своих информационных активов, достаточно сильно влияют внешние процессы, связанные с общим реформированием информационного пространства страны на государственном уровне. Сюда относится развитие электронных реестров, торговых площадок — все, что является результатом движения в сторону концепции e-government. Если запросы коммерческих организаций остались достаточно консервативными (в основном, укрепление сетевого периметра и предотвращения угроз инсайдерского раскрытия информации), то в государственном секторе наблюдаемая активность существенно шире. В первую очередь, это связано с концептуальностью задач и необходимостью разработки стратегии и механизмов защиты практически «с нуля».

Эксперт выделяет следующие основные направления в области ИБ, которые будут актуальны в ближайшем будущем:

- **Защита от атак для доступных публичных сервисов.** Данное направление останется актуальным как для бизнеса, так и для государственных структур.

- **Защита коммерческих данных от утечек.** При этом область применения защиты будет все время расширяться за счет размывания границы между внутренним периметром организации и публичным сектором Интернета. В связи с этим традиционный инструментальный систем защиты от утечек данных (DLP) дополнится сторонними решениями.

- **Повсеместное сокращение бюджетов повлечет за собой трансформацию подхода к обеспечению ИБ.** Уже сейчас коммерческие структуры обращают внимание на концепцию управляемых услуг, то есть пытаются перевести капитальные затраты на ИБ в операционные расходы путем привлечения сторонних подрядчиков (провайдеров услуг информационной безопасности).

- **Распространение и консолидация электронных каналов** государственных услуг требуют внедрения надежных средств идентификации личности и механизмов их аутентификации. Как результат, в ближайшем будущем предполагается повышенный интерес к инфраструктуре PKI и связанным концепциям («единый вход», многофакторная аутентификация, биометрия) в рамках государственных проектов.

Об усилении атак на мобильные платформы сообщает Александр Георгиев, начальник отдела решений ИТ-безопасности, Softprom: «Массовое использование в бизнесе мобильных устройств влечет за собой определенные риски, которые связаны с атаками на данные устройства. Наибольший интерес вызывают решения класса Mobile Security и MDM (Mobile Device Management — управление мобильными устройствами)». Также в тренде остаются системы класса DLP, Web Security и E-mail Security, однако рынок постепенно насыщается. Отдельно стоит отметить резко возросший интерес к решениям класса WAF (Web Application Firewall) и решениям для защиты от DDoS-атак. Это обусловлено тем, что бизнес активно двигается в сеть, а злоумышленники, как обычно, не дремлют.

О криминализации кибератак говорит Александр Руденко, ведущий инженер решений безопасности и кампусных сетей, ИТ-Интегратор. С его точки зрения, злоумышленники стали более ориентированы на получение прибыли (profit oriented), о чем свидетельствуют отчеты безопасности компаний Cisco, Sophos, Verisign, и это одна из основных тенденций 2015 года. Так, возросло количество атак на платежные системы, на системы интернет-банкинга. При этом тот же DDoS или вредоносное ПО на пользовательских ПК являются лишь инструментами для атак на различные платежные системы. Стоит отметить, что у разработчиков вредоносного ПО (malware) иногда получается обходить анализ их кода в «песочницах» (sandbox), что значительно усложняет его обнаружение.

Представители «Майкрософт Украина» прогнозируют более активное внедрение облачных сервисов в области ИБ. Дело в том, что облако позволяет снизить расходы на закупку серверов и их обслуживание, кроме того, облачные ресурсы более эффективно реагируют на кибератаки. В Microsoft отмечают, что их облачные технологии обеспечивают защиту сразу на нескольких уровнях, а такие инструменты защиты зачастую лучше, чем у многих коммерческих компаний и госструктур.

тенцию, так и бизнес-модель. То есть, можно говорить о четком выстроенном механизме, которого в Украине пока нет. Необходимые технологии и квалифицированные специалисты доступны ограниченному количеству заказчиков. То же самое относится к внедрению правильных процессов.

«Таким образом, для интеграторов в этом сегменте очень много работы, притом пока на рынке ИБ относительно небольшая

конкуренция. У компаний, которые смогут воспользоваться моментом, появятся хорошие перспективы», — заявляет эксперт.

По мнению Николая Коцурского, главное отличие украинского рынка заключается в отсутствии адаптированных отраслевых стандартов и рекомендаций в сфере ИБ. В результате — фрагментарный подход в обеспечении защиты информации. Типичное решение украин-

ского заказчика: безопасность и изоляция своей внутренней ИТ-инфраструктуры с применением жесткого административного контроля для персонала. В итоге наблюдается ситуация, когда принятие позитивных мировых тенденций, повышающих эффективность бизнеса и гибкость его процессов, конфликтует с внутренними регуляторными нормативами. Отсюда проистекает тотальное недоверие

к преимуществам концепций BYOD и облачных технологий (SaaS, IaaS, PaaS). При этом глобальный рынок средств ИБ движется в сторону гибридных решений, направленных на обеспечение целостности, доступности и конфиденциальности данных, независимо от места их создания и хранения, с переносом средств мониторинга и аналитики «в облака».

В то же время Сергей Кишкурно имеет другое мнение: «По большому счету, эти рынки не отличаются. Конечно, на Западе выше ставки и больше экспертов высшего эшелона, потому что им платят солидные деньги. Но и требования к результатам там зачастую жестче. Но это объемные показатели. А в Украине есть эксперты, которые западным не уступают, и при этом «стоят» дешевле».

Более того, когда речь идет о реагировании на инциденты, о предотвращении целенаправленных хакерских атак и противодействии АРТ-угрозам, то украинские специалисты могут иногда и фору западным дать. Так, не является новостью тот факт, что ряд отечественных экспертов специализируется на противо-

действию российским хакерским атакам. И они знают этот тип работы гораздо лучше западных коллег.

С этим согласен и Виталий Зарицкий: «Мы не можем сказать, что украинский рынок ИБ отстает в развитии, просто он формируется согласно потребностям и возможностям, учитывая ситуацию в стране».

В сегменте больших компаний (банков, государственных организаций и т.д.) уровень осознанности угроз и рисков в области информационной безопасности гораздо выше, чем в сегменте SMB. Малый и средний бизнес, к сожалению, еще не готов выделять средства на обеспечение безопасности, поскольку у многих таких компаний отсутствует процедура оценки рисков относительно ИТ в целом, а не только в области безопасности.

Александр Фрасинюк добавляет, что в условиях нестабильной политической и экономической ситуации даже крупные компании Украины используют универсальные решения, направленные на защиту от наиболее часто встречающихся угроз.

ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ

Какие законы и стандарты нужны Украине в сфере информационной безопасности? Что уже сделано в этой области, а что предстоит сделать в ближайшее время? По мнению Владислава Радецкого, нашей стране необходимо как можно быстрее избавиться от устаревших ГОСТов, упразднить процедуру сертификации ПО и сосредоточиться на введении нормативных актов, более точно формализующих различные виды киберпреступлений, для которых будут предусмотрены суровые меры наказания. В этом вопросе очень важна работа с доказательной частью. Кроме того, необходима доработка тех положений, которые отвечают за контроль защиты персональных данных.

Самое главное — при составлении законов нужно привлекать экспертов, чтобы принятые нормы коррелировали с техническими реалиями.

Из достижений можно отметить попытки работы над законопроектом «Про засади інформаційної безпеки України», проведение круглых столов с целью обсуждения концепции законопроектов и появление выводов ДСТСЗИ на шифр AES. Но все это лишь малые шаги. Необходима четкая позиция государства по отношению к защите информации, которая будет учитывать интересы не только государственных и частных структур, но и простых граждан.

Важно, чтобы нормы КСЗИ не являлись препятствием для внедрения решений, которым доверяют в развитых странах. Нормативные акты в первую очередь должны подталкивать организации к использованию передовых технологий, а не устаревших/закрытых систем.

Сергей Кишкурно отмечает, что в Украине уже около двух лет идет обсуждение законопроекта «Об основных мерах по обеспечению кибербезопасности Украины» и соответствующей Стратегии. Недавно была отредактирована военная доктрина Украины. Но на этом пути очень много трудностей. Ведь такие документы затрагивают целый ряд ведомств и органов, включая СБУ, СНБО, АПУ, Госспецсвязь. А у каждого ведомства свой круг интересов и обязанностей.

Если бы Украина была готова к созданию кибервойск, то «силовики» могли бы этот процесс сильно продвинуть вперед. Но, видимо, Министерству обороны Украины самому еще надо пройти не одну степень преобразований и модернизации, чтобы эффективно заниматься настолько в сущности инновационным для него направлением.

С точки зрения Александра Фрасинюка, основными проблемами информационной безопасности компаний и государственных структур остаются низкий уровень компьютерной грамотности сотрудников и урезанные бюджеты. Финансовые ограничения не позволяют использовать продукты информационной безопасности, ориентированные на комплексную защиту. В лучшем случае это будет защита периметра. Кроме того, низкая грамотность конечных пользователей зачастую приводит к установке сомнительного ПО.

Главное — не изобретать велосипед, утверждает Николай Коцурский. В качестве примера он называет принятый в Украине ДСТУ ISO/IEC 27001. По сути это адаптированный международный стандарт, который, в свою очередь, основывался на британском стандарте BS 7799,

Комплексными решениями относительно информационной безопасности пользуется крайне незначительное количество корпоративных заказчиков. К сожалению, 85-90% компаний-заказчиков за минувший год совершенно не продвинулись в этой сфере и используют продукты 2-3-летней давности. Это вызвано прежде всего экономическими факторами, а также тем, что именно ИТ по-прежнему остаются первоочередной сферой экономии для украинских компаний.

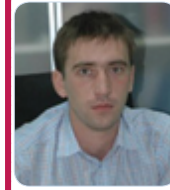
С этим согласен Александр Георгиев: «Ключевым отличием украинского рынка ИБ от западного является разница в отношении бизнеса к информационной безопасности. Не все компании уделяют должное внимание защите данных. Однако стремительный рост атак постепенно меняют точку зрения топ-менеджмента». Еще одно отличие — степень использования облачных сервисов и решений. Этим обуславливается более активное внимание западного рынка ИБ к защите именно облачных решений, а также использование облачных технологий защиты для локальных ресурсов.

позаимствовавший значительную часть контента из еще более раннего нормативного документа Министерства обороны США (т.н. Orange Book). Аналогично нашему правительству и соответствующим отраслевым институтам необходимо адаптировать и другие стандарты, используемые странами НАТО. В первую очередь нужно наконец «легализовать» международные криптостандарты (AES, RSA, SHA), что откроет возможность полноценного применения средств киберобороны от ведущих спецслужб отечественными силовыми ведомствами.

Очевидно, что в этой сфере важно также поддерживать отношения с ведущими коммерческими производителями, тем более что последние поощряют такое сотрудничество. Так, в «Майкрософт Украина» отмечают, что компания уже более 20 лет сотрудничает с европейскими правительствами, государственными учреждениями и бизнесом. А за последний год она подписала два важных соглашения с украинским правительством. В декабре 2014 года — соглашение о программе сотрудничества по вопросам безопасности (Government Security Program). В рамках этой программы корпорация Microsoft предоставляет соответствующему уполномоченному государственному органу доступ к исходному коду своих продуктов. Используя эту информацию, украинские специалисты могут, например, создавать и развертывать местные безопасные ИТ-инфраструктуры.

Второе важное соглашение было подписано в апреле этого года — Меморандум о взаимопонимании с Министерством внутренних дел Украины. Он станет фундаментом для подписания после-

НАШИ ЭКСПЕРТЫ



АЛЕКСАНДР ФРАСИНЮК

Технический директор, Active Solutions



ВЛАДИСЛАВ РАДЕЦКИЙ

Technical Lead, BAKOTECH Group



ВИТАЛИЙ ЗАРИЦКИЙ

Руководитель направления информационной безопасности, ITbiz Solutions



АЛЕКСАНДР САВУШКИН

Управляющий директор в регионе Сев.-Вос. Европы, советник коммерческого директора по развитию бизнеса, Kaspersky Lab



АЛЕКСАНДР ГЕОРГИЕВ

Начальник отдела решений ИТ-безопасности, Softiprom



СЕРГЕЙ КИШКУРНО

Руководитель направления информационной безопасности и аудита, CISA, АМИ



НИКОЛАЙ КОЦУРСКИЙ

Архитектор решений ИБ, BMC Консалтинг



АЛЕКСАНДР РУДЕНКО

Ведущий инженер решений безопасности и кампусных сетей, ИТ-Интегратор

дующих соглашений, в рамках которых специалисты Microsoft совместно с сотрудниками МВД Украины будут работать над усилением кибербезопасности министерства. Кстати, ни одно из подписанных соглашений не обязывает государственные органы покупать у корпорации Microsoft или ее авторизованных партнеров программное обеспечение.

КИБЕРВОЙНЫ: ТОЛЬКО РАЗГОВОРЫ ИЛИ НЕОСПОРИМЫЕ ФАКТЫ?

Утром 25 мая 2014 года, в день президентских выборов, команда CERT-UA, специализированного структурного подразделения Государственного центра защиты информационно-телекоммуникационных систем Госспецсвязи, получила информацию о начале кибератаки на одно из нескольких зеркал официального сайта ЦИК. В результате принятых мер специалистам CERT-UA удалось быстро обезвредить источник атаки, физическое местонахождение которого было зафиксировано в Москве. По всей видимости, основной целью киберпреступников являлась база данных реестра избирателей — в случае ее уничтожения само проведение столь необходимых для страны внеочередных президентских выборов было бы поставлено под угрозу. В Госспецсвязи отмечают, что это была далеко не первая кибератака на

веб-ресурсы государственных органов. Так, в январе 2014 года были детектированы мощнейшие DDoS-атаки на веб-сайт президента, который размещен на серверах Государственного центра защиты информационно-телекоммуникационных систем. Пик нагрузки доходил до 2 Гбит/с. Кроме того, 25 октября минувшего года, в день парламентских выборов, DDoS-атака на сайт ЦИК (cvk.gov.ua) повторилась.

Александр Фрасинюк отмечает, что рост числа DDoS или целенаправленных атак на госучреждения со стороны России носят постоянный характер. Проблема в том, что в наших государственных структурах о лицензионных программных продуктах «слышали» очень мало, и на рабочих местах часто установлены взломанные ОС, скачанные в 95% случаев с российских торрент-сетей. А если к этому добавить еще и тот факт, что в свое время

именно российским специалистам попали в руки все исходные коды операционной системы Windows, то иллюзии о низких шансах взлома и вовсе тают. Все это начинает напоминать целенаправленную политику по распространению заранее подготовленного программного продукта.

Кибервойны — это войны будущего. Специалистам в области ИБ давно очевидно, что это не миф, а новый способ политических и финансовых разбирательств, средство для ведения информационных войн, часть так называемой гибридной войны, утверждает Александр Георгиев. С учетом нынешнего уровня развития информатизации населения такие войны могут стать разрушительными для человечества.

Сколько бы не нагнеталась ситуация, информационное пространство Украины еще пока только реформируется на запад-

ный манер, говорит Николай Коцурский. Одно дело, когда мы слышим о взломе системы управления комплексами Patriot, и совсем — другое, когда в результате DDoS недоступны информационные ресурсы первых лиц страны либо на региональном сайте местного самоуправления объявлено создание очередной «народной республики». То есть, эти ситуации и ущерб от них несоизмеримы. При этом не стоит переоценивать возможности нашего северного соседа, его основная тактика — «игра мускулами»: он может сформировать миллионную армию ботов социальных сетей, заложить программные закладки в код разрабатываемого им ПО, рассказывать о собственном внутреннем «Интернете», «поисковике» и т.п. Но технологически он будет только отставать. Главная угроза, так или иначе, происходит только со стороны инсайдеров.

АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ: МНЕНИЕ ЭКСПЕРТОВ

Около 10 лет назад защита корпоративных данных сети была хоть и не простой задачей, но вполне понятной и «обкатанной»: достаточно было надежно защитить корпоративную сеть по периметру, а также от внутренних угроз, включая инсайдеров, чтобы гарантировать практически полную безопасность важной информации и бесперебойность работы систем. Но с появлением мобильных гаджетов, тренда BYOD и активного внедрения облачных вычислений сетевой периметр начал размываться. Задача защиты корпоративной сети резко усложнилась. Популяризация носимой электроники и постепенное внедрение технологии Интернета вещей еще более повысили уровень киберугроз как для организаций, так и для обычных пользователей.

Что думают о новом фронте в сфере кибербезопасности наши эксперты? Какие направления кибератак будут наиболее актуальны в ближайшем будущем? Чем угрожает обычному пользователю взлом «подключенного» автомобиля, холодильника или кардиостимулятора? Ответы на эти и другие злободневные вопросы читайте ниже.

Какие основные киберугрозы вы можете отметить: что изменилось за последний год, чего должен опасаться бизнес?



Александр Фрасинюк, технический директор Active Solutions: Рост числа целенаправленных DDoS-атак, кража и компрометация корпоративных данных выросли в разы.



Владислав Радецкий, Technical Lead, BAKOTECH Group: Среди инструментов и технологий, применяемых злоумышленниками в последнее время, стоит отметить следующие ключевые моменты:

- В первую очередь бизнесу стоит подумать о безопасности социального канала (это то, о чем многие руководители ИБ не любят вспоминать). Имеется ввиду возросшее количество инцидентов, в которых для обхода механизмов защиты так или иначе применялись методики социальной инженерии (Social engineering) и получения информации из открытых источников (OSINT). Как только бизнес начал понемногу выделять бюджеты и приобретать технические средства защиты, злоумышленники стали уделять больше внимания работе с персоналом компаний-жертв, ведь общеизвестно, что человеческую логику «пропатчить» сложнее, чем антивирус на рабочей станции. Для устранения такого дисбаланса следует в обязательном порядке объединять проведение периодического обучения сотрудников (вплоть до того, что можно публиковать в Сети, а что не стоит) с тестами на проникновение, которые должны затрагивать работу с людьми. Пользователей нужно учить грамотно использовать высокие технологии, иначе эффективность внедренных технических контрмер будет падать.

- Браузер и раньше был своеобразной точкой входа, путем легкого проникновения в инфраструктуру жертвы. Но за последний год ситуация резко ухудшилась. Наиболее уязвимые точки — это использование Adobe Flash Player, Microsoft Silverlight, отображение PDF-документов в окне браузера.

- К сожалению, случай с утечкой наработок Hacking Team показал, к чему приводит ажиотаж на рынке эксплойтов в частности, и монетизация киберпре-

ступности в целом. Речь идет о том, что на сегодняшний день использование обновленного ПО никак не гарантирует отсутствие 0-day, о которых разработчики даже не подозревают. Тут я могу дать следующие рекомендации: во-первых, провести ревизию ПО и запретить использование мультимедиа-плагинов там, где это не продиктовано производственной необходимостью. Во-вторых, если избежать применения наиболее часто атакуемых компонентов нельзя, следует, помимо регулярных обновлений, внедрять системы контроля поведения приложений/HIPS.

- Безопасность корпоративных веб-ресурсов. По причине того, что сайты многих организаций изначально проектировались как «визитки», их техническое исполнение возлагалось на низкокачественных специалистов. Но сейчас они начинают обрастать различными функциями и становятся своеобразными точками обмена клиентской информацией, в результате чего представляют легкую добычу для злоумышленников. Компаниям следует начать с аудита безопасности таких веб-ресурсов, для чего хотя бы пройтись по списку OWASP Top 10. Ложку дегтя в этот вопрос добавляют серьезные уязвимости, обнаруженные в протоколах SSL/TLS: Heartbleed, POODLE, FREAK, Logjam.

Компаниям, веб-сайты, которых используются для хранения и обработки информации, стоит в первую очередь обратить внимание на выявление и устранение этих уязвимостей. К сожалению, хотя информация об этих уязвимостях уже давно является общеизвестной, в сети по-прежнему много уязвимых серверов, что на примере банков было доказано австралийским исследователем Troy Hunt.

- Разгул вирусов-вымогателей, подобных STB-Locker, который мы отслеживаем с начала года и по сей день, служит ярким индикатором недостаточного качества фильтрации почты, с одной стороны, и доверчивости/невнимательности пользователей — с другой. Об отсутствии резервных копий я уже молчу. Бизнесу стоит подумать о должном уровне защиты электронной почты и об обучении пользователей.



Виталий Зарицкий, руководитель направления информационной безопасности, ITbiz Solutions: Мы можем выделить несколько основных угроз, которые на протяжении многих лет практически не изменились: вредоносное ПО, спам, удаленный взлом компьютеров, фишинговые атаки, при которых пользователь ПК «попадает на крючок» поддельного веб-сайта, полностью имитирующего, скажем, сайт банка, в котором он держит свой депозит.

И конечно же в разы выросло количество и частота DoS/DDoS-атак, которые зачастую используются лишь как «дымовая завеса» для похищения конфиденциальной информации, денежных средств и других данных.



Александр Савушкин, управляющий директор Kaspersky Lab в регионе Северо-Восточной Европы, советник коммерческого директора по развитию бизнеса: Последний год показал прогнозируемое увеличение количества как сложных целевых атак на организации, так и разнообразных угроз для конечных пользователей. При этом киберпреступники уже давно нацелены не только на

компьютеры, но и на смартфоны и планшеты. Только за второй квартал 2015 года с помощью продуктов Kaspersky Lab для защиты мобильных устройств было обнаружено более 1 млн установочных пакетов и почти 300 тысяч новых мобильных вредоносных программ. Уязвимы как устройства на широко распространенной платформе Android, так и на iOS и Mac.

Основная цель киберпреступников — быстро заработать, поэтому мы наблюдали очередную волну программ-вымогателей, в том числе зашифровывающих данные пользователей уникальными для каждого компьютера ключами, а также банковских «троянцев». Получившие широкое распространения технологии, такие как виртуализация, BYOD и др. делают ИТ-инфраструктуру организаций более сложной, затрудняя тем самым и задачу ИТ-специалистов по защите всех ее элементов. Каждый незащищенный элемент дает возможность злоумышленникам проникнуть в ИТ-систему. Наши эксперты все чаще раскрывают киберкампании, нацеленные на получение информации в определенной сфере или у определенных компаний, и они нередко используют такие бреши и человеческий фактор.



Александр Георгиев, начальник отдела решения ИТ-безопасности, Softprom: Наблюдается увеличение числа атак практически по всем направлениям, начиная от fraud-мошенничества и заканчивая промышленным шпионажем с применением самых современных технологий.

В целом атаки становятся все ухищренней, их стоимость снижается, при этом суммы ущерба растут.



Сергей Кишурно, руководитель направления информационной безопасности и аудита, CISA, АМИ: С течением времени необходимость в высокой квалификации хакеров существенно снизилась, а вот сложность и реальная опасность хакерских атак заметно возросла. Основные страны-источники киберугроз — Россия и Китай — за последний год лишь усилили свое сомнительное «лидерство». Кроме того, растут показатели мошенничества в финансовых системах и количество взломов носимых устройств.



Николай Коцурский, архитектор решений ИБ, BMC Консалтинг: Новые киберугрозы связаны в первую очередь с размыванием границ корпоративной сети: разнесением вычислительных возможностей между физическими ЦОДами и облаком, «просачиванием» коммерческой информации в мобильных устройствах пользователей и используемые ими веб-сервисы. Бизнесу стоит уделить особое внимание именно этим векторам и планировать усиление ИБ за счет инвестиций в решения по защите веб-сервисов (связка ADC-WAF-DDoS), организации безопасного доступа к ресурсам (SSL VPN) и контроля над использованием этих ресурсов (mobile security, cloud security).

«Майкрософт Украина»: 83% программного обеспечения в Украине установлено нелегально — такие данные последнего исследования по уровню пиратства, опубликованного в июне 2014 года международной ассоциацией Business Software Alliance (BSA). При этом каждый третий компьютер с неле-

гальным ПО заражен вредоносными программами. Согласно отчету Microsoft Security Intelligence Report (SIRv17), где проанализированы уязвимости и угрозы, с которыми сталкивались более миллиарда систем по всему миру, на каждые 1000 интернет-хостов в Украине расположено 29,9 фишинговых сайтов. По этому показателю Украина заняла первое место в мире во втором квартале 2014 года.

Существует целый ряд рисков, которые угрожают компаниям, использующим нелегальное программное обеспечение. По статистике, около 75% ИТ-директоров сталкивались с различными техническими проблемами вследствие установки сотрудниками пиратского ПО на свой рабочий компьютер. Кроме того, согласно результатам совместного исследования международной компании IDC и Национального университета Сингапура, компании тратят около 500 млрд долл. в год на решение проблем с вредоносными программами вследствие установки нелегального программного обеспечения. Избежать этих проблем можно, используя лицензионные программы, которые гарантируют техническую поддержку и своевременные обновления.

Мобильные устройства, BYOD и личные облака на рабочем месте — в чем заключаются основные риски?



Александр Фрасинюк, Active Solutions: Мобильные устройства — одни из наиболее подверженных взлому, ведь именно в таких гаджетах у многих пользователей хранятся их корпоративные данные (пароли для доступа к почтовым и интерактивным сервисам) и персональные данные (платежных карт и почтовых сервисов)



Владислав Радецкий, BAKOTECH Group: По сути, в данном вопросе сотрудникам подразделения ИБ приходится иметь дело с частичной либо полной потерей контроля над обрабатываемыми данными. Что имеется ввиду? Когда мы затрагиваем тему BYOD — то говорим о разнообразии мобильных платформ, что существенно усложняет соответствие принятым политикам ИБ. Кроме того, как правило, в каждой компании рано или поздно появляется каста привилегированных пользователей, которым в силу занимаемых должностей разрешается обход ограничений политик ИБ. Несмотря на то, что это больше проблема административного характера, она напрямую связана с желанием топ-менеджеров хранить важную информацию на своих устройствах.

При использовании облачных вычислений стоит учитывать риски несанкционированного доступа к оборудованию сервис-провайдеров, атаки типа DDoS, доступ пользователей с потенциально скомпрометированных устройств. Важно понимать, что при миграции в облачные сервисы (особенно если мы говорим о public cloud), данные должны храниться и обрабатываться в зашифрованном виде, иначе компрометация одного из компонентов может повлечь за собой частичное или полное раскрытие клиентских данных. К сожалению, зачастую, вынося те или иные службы в облака, ИТ-службы прорабатывают вопросы отказоустойчивости, но не безопасности. Бизнесу необходимо подумать о выделении средств на MDM-системы, двухфакторную аутентификацию, построение VPN-подключений, безопасную публикацию корпоративных сервисов.



Александр Савушкин, Kaspersky Lab:

Предоставляя доступ к корпоративным данным с мобильных устройств, будь то смартфон, планшет или ноутбук, важно изначально учитывать риски их использования, утери или кражи. Это могут быть заражение, передаваемые при подключении к корпоративной сети, потеря и утечка данных. Мы советуем применять комплекс из качественного проверенного защитного решения и политик безопасности, объясняющих сотрудникам, что можно и нельзя делать в той или иной ситуации.

Использование облачных решений, как правило, связано с сервисами третьих сторон, от которых во многом зависит сохранность данных. Также большую роль играет человеческий фактор (например, использование сотрудниками простых паролей, одинаковых для разных сервисов). Все это необходимо объяснять персоналу, а также, если речь идет о конфиденциальной информации, применять такие технологии, как шифрование. Ведь даже в случае кражи данных без специального ключа прочитать их будет невозможно.

Мы понимаем важность таких рисков для организаций любого размера, поэтому и в решениях Kaspersky Security для бизнеса, и Kaspersky Small Office Security предусмотрели соответствующие средства защиты. Например, возможность найти утерянные устройства, удаленно заблокировать их или удалить данные в случае кражи.



Александр Георгиев, Softprom: Среди основных рисков стоит отметить неграмотность пользователей и отсутствие средств защиты.



Сергей Кишкурно, АМИ: Использование BYOD создает дилемму: либо отстранить на персональных гаджетах сотрудника большое количество ограничений, что приведет к резкому снижению популярности этого подхода, либо разрешить почти все, но одновременно повысить риски ИБ из-за невозможности фактически контролировать конфигурацию устройств, имеющих доступ в корпоративную сеть. Эта дилемма не решена и по сей день. Возможно, нынче одним из наилучших решений является использование агентов DLP-системы, разворачиваемых на BYOD, что позволяет детально контролировать работу именно с корпоративной информацией. Это не решает проблемы полностью, но существенно снижает риски. Правда, для этого в компании надо внедрить систему DLP правильно, что означает зачастую поднятие всей ИБ организации на новый уровень зрелости. Каждый конкретный заказчик решает сам, что выбрать.

Хранение личной информации в облачном сервисе, безусловно, будет выбором сотрудника. Но если он размещает ее, скажем, с персонального устройства через корпоративную сеть, это должно стать объектом контроля, в стиле того, как процесс протекает в DLP-системе. Здесь ступень риска определяется эффективностью классификации критических информационных активов и имеющихся превентивных контролей, конкретных технических средств, которые, используя такую классификацию, смогли бы проследить все неправомерные действия пользователя и вовремя их заблокировать.

В корпоративном масштабе использование закрытых частных облаков можно лишь приветствовать. Применение же компанией коммерческих сервисов имеет фундаментальную проблему: информация физически покидает пространство

организации (обычно это управляющий офис). И тут нужен индивидуальный и очень взвешенный подход. Никакие правовые условия не компенсируют потерю жизненно важной информации. Разве что речь может идти о страховании, но этот аспект все еще в зачаточном состоянии.



БМС консалтинг

Николай Коцурский, БМС Консалтинг: «Мобилизация» бизнеса закономерно влечет за собой ряд рисков, завязанных на основных принципах работы мобильных платформ. В первую очередь, это концепция открытости этих систем. Современные смартфоны и планшеты не разрабатываются как изолированные среды, а, наоборот, предлагают широкие (часто слабо контролируемые) каналы внешней коммуникации, постоянно синхронизируя свое состояние с встроенными и подключаемыми облачными сервисами Google, Apple, Microsoft. Именно здесь и заложен основной конфликт: к мобильным устройствам невозможно применить классическую парадигму защиты традиционных ПК — запретить все, что не используется в бизнес-процессе. Производители профильных решений ИБ используют другой подход — максимальная регламентация процесса получения доступа к корпоративным ресурсам с мобильных устройств, контроль жизненного цикла данных, хранимых на них, применение средств оперативного блокирования и удаления.

IT INTEGRATOR

Александр Руденко, ведущий инженер решений безопасности и кампусных сетей, ИТ-Интегратор. Доступ к корпоративной сети и ресурсам через мобильные устройства с использованием подхода BYOD имеет ряд больших потенциальных угроз, если не строить систему комплексно. Возможность копирования конфиденциальных данных и взломанные (jailbroken, root) устройства — это источники вредоносной активности в сети. При этом, защищая периметр корпоративной сети, мы фактически даем всю свободу для распространения вредоносного ПО внутри через те же взломанные устройства. В данной ситуации продукты класса MDM во многом снижают риски, давая доступ только проверенным устройствам и используя защищенные хранилища данных.

Если сравнивать private cloud с public cloud, то безопасность доступа к данным и самих данных лежит в зоне ответственности владельца private cloud, и это опять-таки должно находить отражение в стратегии обеспечения безопасности

Что касается облаков, то тут сразу возникает другой вопрос — обеспечение безопасности личных облаков (private cloud). Если сравнивать private cloud с public cloud, то безопасность доступа к данным и самих данных лежит в зоне ответственности владельца private cloud, и это опять-таки должно находить отражение в стратегии обеспечения безопасности.

Проблемы защиты носимой электроники (wearable devices): эксперты фиксируют пер-

вые случаи взлома носимых электронных устройств, таких как фитнес-браслеты, кардиостимуляторы и т.д. С вашей точки зрения, насколько эти проблемы будут актуальны в будущем? Стоит ждать их усиления или наоборот?



Александр Фрасинюк, Active Solutions:

На мой взгляд, это наименее защищенная категория устройств, хотя и самая мобильная и универсальная. Ведь именно в мобильных персональных устройствах находится масса личной и корпоративной информации.



Владислав Радецкий, BAKOTECH Group:

Наибольшее опасения здесь представляют устройства, встраиваемые в человеческое тело (как пример кардиостимуляторы). Такие устройства сегодня не слишком широко распространены, но ряд компаний действуют на опережение и активно занимаются поиском решения будущей проблемы. В данном случае это абсолютно оправдано, поскольку повсеместное применение этих технологий без предварительного решения вопроса их безопасности — потенциальный риск для жизни и здоровья большого числа людей в будущем.



Александр Георгиев, Softprom:

Безусловно, эти проблемы актуальны, но вопрос в том, будет ли у злоумышленников возможность получить выгоду при взломе данных устройств. Все зависит от того, насколько носимая электроника интегрируется в платежные системы (например, для оплаты товаров и услуг) и как обрабатывает конфиденциальную информацию. Вот что станет основными факторами, которые повлияют на количество атак/взломов устройств.



Сергей Кишкурно, АМИ: Если популярность этих гаджетов вырастет, то риски усилятся. Такие устройства являются носителями, можно сказать, глубоко персональной информации. Это не адрес, не номер телефона и не почтовый ящик, но значительное дополнение к перечисленному. Если потенциальные злоумышленники будут знать о человеке гораздо больше, чем раньше, то лишь вопрос времени, когда они найдут этому противоправное применение. Причем здесь мы имеем весьма интересный эффект, когда киберугроза, сама по себе выглядящая почти нейтрально, может иметь продолжение в физическом пространстве, в виде опасностей, существующих в реальном мире. И надо говорить о совокупности этих гроз, чтобы увидеть всю картину по рискам и что-то с этим сделать.

IT INTEGRATOR

Александр Руденко, ИТ-Интегратор:

Всё, что будет иметь хоть какую-то ценность для взломщика с точки зрения денег и прочего, всегда будет находиться в центре его интересов. В этой связи любое ИТ-устройство является целью, и вопросы безопасности актуальны как никогда, особенно учитывая ожидаемые масштабы распространения таких персональных устройств.

Концепция Интернет вещей еще больше усугубляет этот вопрос, поскольку по прогнозам к 2020 году к сети будет подключено более 30 млрд устройств, которыми можно управлять удаленно из любого места. И любая брешь в безопас-

ности в масштабах всей сети окажется потенциальной катастрофой.

Именно поэтому продуманная стратегия защиты, которая постоянно совершенствуется, может значительно снизить риски. На наш взгляд, такие системы безопасности должны строиться на решениях от нескольких производителей, опять-таки, для увеличения общего уровня безопасности и получения эффекта эшелонирования.

Многие аналитике в сфере ИБ открывают новый фронт для борьбы с киберугрозами — Интернет вещей (Internet of Things (IoT)). Насколько вы согласны с этой точкой зрения, в чем заключается основная опасность и чего можно ожидать в ближайшем будущем?



Александр Фрасинюк, Active Solutions:

Безусловно, Интернет вещей — новый фронт для борьбы с киберугрозами. В нашей реальности многие заказчики защищены только от наиболее часто встречающихся уязвимостей, поэтому теперь им добавляется еще одна потенциальная брешь.



Владислав Радецкий, BAKOTECH Group:

В вопросе IoT я целиком разделяю точку зрения одного из признанных корифеев ИБ Брюса Шнайера. Когда на недавней конференции Black Hat 2015 репортер задал вопрос о том, что Брюс думает о защите конечных точек, эксперт ответил, что его больше беспокоит состояние защиты IoT-устройств, поскольку защищать обычные компьютеры мы более-менее научились. Недавние новости о взломе Jeer и обнаружение уязвимости Stagefright в Android — лишнее подтверждение опасениям Брюса. Проблема в том, что зачастую производители таких устройств думают о рисках кибератак в последнюю очередь. Как следствие, мы получаем огромное количество уязвимых устройств, менеджмент обновлений для которых весьма сложен, если вообще реализуем (Android 2-й и 3-й версий).



Виталий Зарицкий, ITbiz Solutions:

Новая среда порождает новые угрозы и риски. Об инцидентах использования холодильников, телевизоров, мультимедийных центров, подключенных к Интернету, в качестве точек ботнет-сетей все чаще пишут в СМИ. Но гораздо опаснее случаи взлома автомобилей, которых в последнее время становится все больше, ведь такие атаки представляют непосредственную угрозу для жизни человека. Поэтому с приходом в нашу жизнь значительного количества «умных» устройств нам приходится больше заботиться не только о физической безопасности.



Александр Савушкин, Kaspersky Lab:

Появление все большего числа подключенных к сети устройств, в том числе и носимой электроники — повод для более широкой дискуссии о безопасности и сохранности личных данных. Чем более распространенными будут эти устройства, тем больше они будут привлекать внимание злоумышленников. Если их взлом будет им выгоден, это может породить новые киберугрозы. Эксперты Kaspersky Lab уже не раз поднимали вопросы в этой области.

СЕМЬ ШАГОВ К БЕЗОПАСНОСТИ ИНТЕРНЕТ-БАНКИНГА

ВИТАЛИЙ ЗАРИЦКИЙ

Благодаря росту своей популярности дистанционное банковское обслуживание (ДБО) чаще становится объектом внимания киберпреступников. И поскольку злоумышленники изобретают все новые и новые способы атак на деньги вкладчиков, банки должны своевременно и адекватно реагировать на увеличившиеся киберугрозы.

Чтобы получить доступ к банковским счетам пользователей, киберпреступники используют широкий спектр технологий — от изощренных атак с использованием вредоносного кода до методов социальной инженерии, основанных на знании психологических тонкостей поведения клиентов. Мы рассмотрим типы атак для получения доступа к чужим банковским счетам, которые используют киберпреступники, а также способы противостояния этим атакам.

• **Фишинг** — одна из самых распространенных атак. Суть ее в том, что при помощи сообщения по электронной почте, социальной сети или SMS пользователя перенаправляют на ложный веб-сайт, который выглядит как оригинальный ресурс банка. Пользователь, не подозревая о подвохе, вводит персональную информацию (имя, пароль, номера кредитных карт, СМС-код), которая и попадает в руки мошенника. Данный вид мошенничества особо развит в сегменте интернет-банкинга.

В качестве «противоядия» рекомендуется пользоваться онлайн-услугами банка, который применяет многофакторную аутентификацию (поскольку преступники вряд ли смогут реализовать такую функцию на фишинговом сайте). Вообще многофакторная аутентификация считается наиболее безопасной системой для предоставления доступа. Хотя зловерное ПО, если оно уже присутствует на компьютере, может функционировать и после аутентификации пользователя. Однако в данном случае ущерб будет ограничен лишь текущей сессией, поскольку после ее закрытия хакер не сможет зарегистрироваться заново.

• **Кража базы паролей.** Применяя зловерное ПО и другие технологии, хакеры воруют учетные данные пользователей для перепродажи другим преступникам либо эксплуатируют их сами для получения доступа к чужим банковским счетам.

Чтобы застраховаться от утечки конфиденциальной информации, важно регулярно проверять компьютер на наличие вирусов.

• **Атака «человек посередине» (Man-in-the-Middle).** Очень распространенная некогда атака, посредством которой злоумышленник внедряет собственные сообщения в трафик между компьютером пользователя и сервером аутентификации. Таким образом, данные о платеже могут перехватываться на этапе, когда клиент их уже отправил, но они еще не дошли в банк. Мошенник изменяет данные под свои требования и только после этого отправляет их в банк.

На сегодня практически все банки, предоставляющие услуги интернет-

банкинга, для передачи данных от клиента в систему банка и обратно используют SSL-протокол, то есть вся информация шифруется. Такая мера безопасности позволяет защититься от распространенного ранее вида мошенничества.

• **Атака «человек в браузере».** Одна из самых изощренных тактик: с помощью троянской программы инфицируется веб-браузер пользователя, что позволяет перехватывать и модифицировать всю отправляемую информацию. Такой вид атаки дает возможность изменять веб-страницы и содержание операций таким образом, что пользователь этого не замечает. Весь процесс протекает скрытно, без каких-либо внешних признаков.

Для защиты от этой атаки на компьютере клиента должен быть установлен регулярно обновляемый антивирус.

• **Кража личности.** Если мошенник накопит достаточный объем персональной информации о клиенте банка, то сможет использовать эти данные для совершения различных преступлений. Например, он звонит в контакт-центр банка и, представляясь чужим именем, называет различные ключевые слова, чтобы сменить пароль доступа на сайт с услугами онлайн-банкинга или выполнить другие операции. Кражу личности или сбор персональных данных можно осуществлять различными способами: от поиска информации в социальных сетях до внедрения на компьютер клиента вредоносного ПО, способного шпионить за пользователем.

Чтобы застраховаться от таких атак, надо поменьше делиться личной информацией на публичных ресурсах и следить за антивирусным гигиеной на своем ПК.

Мобильный банкинг

Многие банки предоставляют клиентам услуги мобильного банкинга, то есть возможность работы со своим счетом через специальное мобильное приложение на смартфоне или планшете. Несомненно, это очень удобно, поскольку позволяет выполнять операции со своим банковским счетом «на ходу», в любом месте, где есть Интернет. Проблема заключается в том, что для каждой популярной сегодня мобильной ОС (Android, iOS, Windows Phone и т.п.) характерны свои уязвимости. По мнению экспертов, эти потенциальные бреши присутствуют и в приложениях для мобильного банкинга.

Например, согласно исследованиям, около трети мобильных приложений для iOS и 15% для Android содержат уязвимости, ведущие к некорректной работе SSL-протокола, а это означает возможность перехвата критичных платежных данных с помощью атаки Man-in-the-Middle. Свыше 20% приложений для iOS потенциально уязвимы к SQL-инъекции, что создает риск похищения информации о платежах. Также свыше половины программ для мобильного банкинга для платформы iOS и 20% для Android потенциально уязвимы к атакам типа межсайтовый скриптинг, что позволяет использовать авторизацию пользователя

в веб-системе для получения расширенного доступа к ней или для получения авторизационных данных пользователя. Почти половина приложений для iOS потенциально уязвимы к атакам типа XHE (XML eXternal Entity). Особо опасны эти атаки для столь популярных в нашей стране «разблокированных» смартфонов (jailbreak). Кроме того, свыше 20% приложений для Android некорректно работают с механизмами межпроцессного взаимодействия, тем самым предоставляя доступ сторонним приложениям к критичным банковским данным.

Способы защиты

Принимая во внимание стремительный рост угроз в сегменте интернет-банкинга, производители продуктов для информационной безопасности отреагировали выпуском соответствующих продуктов для защиты пользователей от мошенничества. Например, компания IBM представила серию решений под названием IBM Security Trusteer, которые помогают предотвратить атаки, одновременно позволяя финансовым учреждениям обеспечить строгое соблюдение нормативных требований.

Среди возможностей решения IBM Security Trusteer стоит отметить многоуровневую защиту пользовательских устройств от заражения вредоносным кодом и фишинговых атак; защиту сеансов веб-браузера для предотвращения взлома клиентских транзакций; защиту от хищения идентификационных данных. Также решение предохраняет компьютер пользователя от заражения вредоносным кодом, тем самым обеспечивая безопасную работу клиентов с электронными банковскими системами.

Кроме того, на глобальном рынке популярно решение от компании Easy Solutions — Total Fraud Protection. Это комплексная технологическая система для защиты от кибермошенников при проведении финансовых онлайн-транзакций. Total Fraud Protection содержит средства для противодействия фишингу, фармингу (процедуре скрытного перенаправления жертвы на ложный IP-адрес) и вредоносному коду. Единое решение защищает клиентов банка от перехвата доступа к банковскому счету и сокращает возможные потери от мошенничества с дебитовыми и кредитными картами. Вся информация о возможных фрод-атаках немедленно выводится в окне мониторинга программы.

Стоит акцентировать на том, что безопасный интернет-банкинг — это процесс, который затрагивает обе стороны: клиента и банк. На стороне клиента должно стоять качественное антивирусное ПО, а на стороне банка — специализированные системы антифрода, которые смогут отслеживать нетипичное поведение пользователя на сайте с услугами интернет-банкинга. К слову, любой банк заинтересован в предоставлении максимально качественных услуг. Но, как показывают наши наблюдения, в настоящее время рынок систем для безопасного интернет-банкинга только начинает зарождаться.

ВАЖНО

Ключевые требования к построению безопасной системы интернет-банкинга

1. Банк постоянно осуществляет мониторинг поведения пользователей в системе интернет-банкинга, отслеживает все операции со счетом и сообщает клиенту о подозрительных переводах.

2. Банк использует многофакторную аутентификацию. Кроме того, при каждом входе в личный кабинет или при проведении платежа необходимо ввести дополнительный пароль, а пароль для подтверждения платежа или входа в личный кабинет запрашивается через мобильный телефон или через специальный «токен».

3. Между банком и пользователем установлен защищенный канал по протоколу HTTPS, рядом с адресной строкой банка указан сертификат безопасности, подтверждающий защищенность канала.

4. В банке ограничено число операций за один день и применяется система автоматического выхода из личного кабинета после короткого периода бездействия.

5. Сотрудникам техподдержки банка не нужно спрашивать ваш постоянный пароль, чтобы помочь вам в работе со счетом.

6. Банк постоянно предупреждает пользователя о новых типах мошенничества, которые могут ему угрожать.

7. Кроме того, банк время от времени высылает свод рекомендаций по безопасной работе с системой интернет-банкинга, в котором, в частности, есть советы: не работать на компьютере, с которого выполняется работа с системой интернет-банкинг, с правами системного администратора, не оставлять свой компьютер или мобильное устройство без присмотра во время открытой текущей сессии и пр.

Кроме того, никакие технические средства безопасности не спасут клиента от злоумышленников, если он сам не будет соблюдать правила безопасности. Пользователь должен избегать посещения сайтов сомнительного содержания, регулярно проверять компьютер на наличие вирусов, также не рекомендуется хранить информацию о личном ключе и пароле на своем ПК или на каких-нибудь других носителях в нешифрованном виде. И, конечно же, необходимо очень внимательно читать присылаемые банком сообщения. В случае сомнений лучше лишний раз позвонить в контакт-центр банка и удостовериться в подлинности полученного письма. Фактически любое нетипичное поведение системы ДБО — повод для дополнительного повышения бдительности.

Автор статьи — руководитель направления информационной безопасности ITbiz Solutions

поскольку пренебрежительное отношение к мерам кибербезопасности может привести к достаточно серьезным последствиям. Также Kaspersky Lab поддерживает инициативу Securing Smart Cities, направленную на то, чтобы помочь ответственным за разработку «умных» городов делать свою работу, не забывая о кибербезопасности.



Александр Георгиев, Softprom: Основная опасность заложена в самой концепции, «исключающей из части действий и опера-

ций необходимость участия человека». Это может привести к непредвиденным последствиям, которые будут зависеть от степени глобализации Интернета вещей и могут касаться как отдельного человека, так и целых стран.



Сергей Кишкурно, АМИ: В этом вопросе верны те же рассуждения, что приведены и для носимой электроники выше.



БМС консалтинг

Николай Коцурский, БМС Консалтинг: Это два тесно связанных вопроса, на которые можно дать унифицированный ответ: любое устройство, обладающее вычислительными мощностями, набором логических инструкций и средствами внешней сетевой коммуникации может быть взломано и использовано злоумышленником. Исходя из принципа дальнейшей миниатюризации микросхем и увеличения скоростей пере-

дачи данных, риски, присущие Интернету вещей, будут только увеличиваться. Бот-сети из холодильников, кража токенов аутентификации с носимой электроники и последующие их неправомерное использование — это не фантастика, а вполне вероятные сценарии векторов атак в ближайшем будущем. Уже сегодня пользователи плохо контролируют активность своих ПК (бот-активность, генерация бит-коинов) и слабо понимают ценность данных, хранимых на мобильных устройствах. Имея доступ к последним, злоумышленник без труда сможет узнать «всю подноготную» человека, используя OAuth-токены.

ТРИ КОЗЫРЯ FORTINET: ПРЕДОТВРАЩЕНИЕ, ОБНАРУЖЕНИЕ, СНИЖЕНИЕ РИСКОВ

О том, как изменился технический ландшафт в обеспечении информационной безопасности и какие киберугрозы сегодня представляют наибольшую опасность для корпоративного бизнеса рассказывает Мирослав Мищенко, менеджер по работе с ключевыми клиентами компании Fortinet.

PC Week/UE: Какие основные тренды вы можете отметить на рынке ИБ в Украине? Как изменились требования клиента за последний год? Чем это обусловлено?

МИРОСЛАВ МИЩЕНКО: В первую очередь стоит сказать о бюджетах заказчиков, большая часть которых в конце прошлого года формировалась в национальной валюте и не пересматривалась в течение последнего времени в сторону увеличения. Поскольку проекты все равно нужно реализовывать, заказчики готовы рассматривать альтернативные решения от производителей, которые не указаны в их корпоративных стандартах. Вследствие этого они все больше и больше предпочитают проводить тестирования решений, прежде чем совершить покупку.

Нам комфортно работать в таких условиях, поскольку за счет широкого портфеля решений, высокой производительности и гибкой ценовой политики появилось больше возможностей удовлетворить требования заказчиков.

PC Week/UE: Как эволюционируют киберугрозы? Что нового произошло в последние годы в этой сфере? Чего должен опасаться бизнес?

М.М.: Ни для кого не секрет, что в последнее время количество угроз крайне возросло как на международном уровне, так и в Украине. Утечка данных — это

серьезный и прибыльный бизнес. За последние два года на мировом уровне было зарегистрировано более 1,3 млрд инцидентов. Эволюция угроз происходит крайне быстро, каждый день наши исследователи из научного центра FortiGuard сталкиваются с ранее несуществующими и всё более сложными угрозами.



Мирослав Мищенко
менеджер по работе с ключевыми клиентами

Думаю, многие коллеги согласятся со мной, что на сегодняшний день самыми разрушительными являются целенаправленные продвинутое угрозы (APT). Современная киберпреступность — это очень тонкий и долгий процесс. Цель киберпреступника — проникнуть в сеть компании и извлекать данные, оставаясь как можно дольше незамеченным.

Сегодня не существует универсального средства защиты от целенаправленных продвинутых угроз. Наиболее эффективную защиту обеспечивает комплексная и расширенная инфраструктура безопас-

ности. Так, например, инфраструктура защиты от продвинутых угроз Fortinet состоит из трех важных элементов: предотвращение, обнаружение, снижение рисков.

PC Week/UE: Тенденции последних лет — глобальная виртуализация ИТ-инфраструктуры: серверов, хранилищ, сетей. Как это меняет ландшафт информационной безопасности и технологии защиты и какие появляются новые угрозы?

М.М.: В 2014-м половина нагрузки в ЦОДах уже выполнялась на виртуальных машинах. Прогнозы на 2016 год — она составит более 80%.

Соответственно наблюдается и рост east-west трафика (трафик между виртуальными машинами в пределах физического сервера), который сложно контролировать традиционными аппаратными средствами инспекции/филтрации. Проблему возникающего пробела в безопасности можно решить, используя виртуальные аналоги традиционных средств. Инспекцию north-south трафика (трафик между физическими хостами) по-прежнему более эффективно выполнять с помощью устройств, в которых применяются специализированные аппаратные компоненты обработки трафика.

PC Week/UE: Какие типы решений сегодня наиболее часто используются для защиты ЦОДов? И как меняются требования заказчиков в этой сфере?

М.М.: ЦОДы развиваются с использованием доступных на рынке технологий, таких как виртуализация, облачные вычисления, программно-определяемые сети. Это и является определяющим при проектировании и внедрении сетевой безопасности. Заказчикам стоит учитывать следующие решения и факторы.

При построении системы безопасности в периметре ЦОДа, в первую очередь, необходим классический брандмауэр. Важно обратить внимание на производительность брандмауэра на мелких пакетах, которые генерируются мобильными устройствами, и на низкую задержку при обработке трафика. Нельзя забывать и об устройстве для защиты от DDoS-атак.

Если мы говорим о ядре сети ЦОДа, то необходим внутренний брандмауэр (Internal Network Firewall) с портами 40 Гбит/с и 100 Гбит/с для сегментирования сети, очень важна также высокая скорость обработки IPv6-трафика.

В настоящее время все большую популярность набирают технологии виртуализации. Это использование виртуальных устройств безопасности для контроля обмена трафика между виртуальными машинами. Они становятся одним из ключевых компонентов современной ИТ-инфраструктуры ЦОДа. Сегодня практически невозможно представить построение нового серверного узла организации без использования технологии виртуализации. Она позволяет усовершенствовать инфраструктуру безопасности ЦОДа, а также сэкономить средства и время.

PC Week/UE: Сегодня бизнес массово мигрирует в облака. При этом обязанности по защите корпоративных данных как минимум частично возлагаются на облачного провайдера. Как это влияет на общий уровень информационной безопасности компании? Какие новые угрозы появляются, какие возможные бреши закрываются?

М.М.: Это право заказчика — выбрать облачного провайдера, который удов-

ПРОДОЛЖЕНИЕ НА С. 21 >>>

ВАМ УГРОЖАЮТ КИБЕРАТАКИ – МЫ ЗАЩИТИМ ОТ ИЗВЕСТНЫХ И НЕИЗВЕСТНЫХ УГРОЗ!

С каждым днём риски, связанные с защитой активов вашей компании, растут. Целенаправленные современные угрозы — это утечка конфиденциальных данных, кража интеллектуальной собственности и другой важной информации. Традиционных способов защиты сети уже недостаточно для борьбы с кибератаками этого уровня.

Fortinet предлагает комплексное решение для защиты от современных продвинутых атак. Основанная на трёх элементах: предотвращение, обнаружение и снижение рисков, инфраструктура защиты от продвинутых угроз Fortinet сочетает в себе передовые фирменные технологии и опыт экспертов по кибербезопасности из исследовательского центра FortiGuard. Каждая компания, независимо от ее величины, является потенциальной мишенью для киберпреступников.

Не рискуйте — защитите вашу сеть с помощью решений Fortinet!

www.fortinet.com

FORTINET

ПРОБЛЕМЫ ПОСТРОЕНИЯ И АУДИТА СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ БАНКА

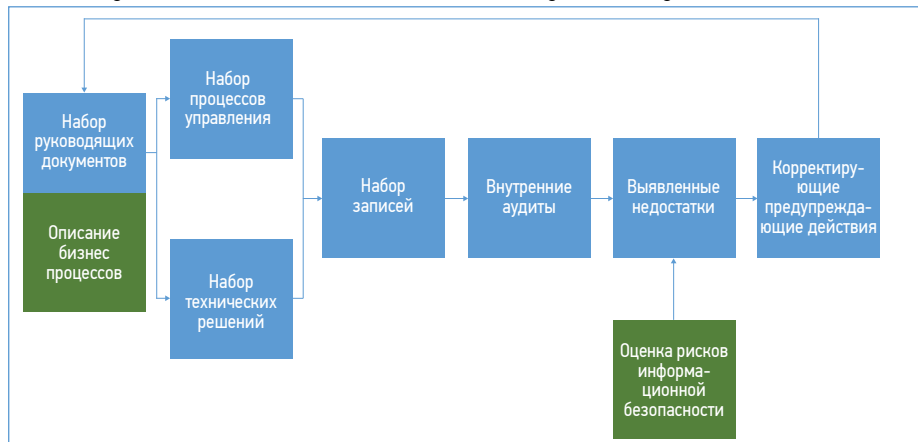
ВАЛЕРИЙ ЕРМОШИН

С момента выхода первой версии стандарта по управлению информационной безопасностью ISO/IEC 27001 прошло уже девять лет. За это время и в нашей стране, и за ее пределами в данной области произошло многое. Ключевые моменты были следующими: приняты в 2011 году стандарты как отраслевого для банковской системы Украины, выход в 2013 году второй версии стандарта, наработка большой практики построения систем управления информационной безопасностью (далее — СУИБ) в банковском секторе.

Если учитывать количество отечественных банков и требование Национального банка Украины об обязательном построении СУИБ, таких проектов уже должно быть более 150. Поэтому вроде бы теория и практика построения СУИБ является достаточно понятным и изученным направлением, но при этом здесь до сих пор остаются актуальные вопросы. Прежде чем приступить к их рассмотрению на базе существующего опыта в банковском секторе, хотелось бы перейти от несколько формального определения СУИБ, которое дает стандарт, к его неформальному представлению.

Что собой представляет СУИБ

Согласно стандарту, СУИБ (Information security management system — ISMS) — это часть общей системы управления, основанной с учетом бизнес-рисков и предназначенной для разработки, внедрения, функционирования, мониторинга, анализа, поддержания и совершенствования информационной безопасности. ИБ



в свою очередь реализуется циклически через повторяющийся процесс принятия решения PDCA (Plan-Do-Check-Act — планирование-действие-проверка-корректировка), известный как цикл Деминга (Deming Cycle).

С практической точки зрения СУИБ на начальных стадиях — это набор руководящих документов, которые порождают набор процессов управления и набор технических решений, а они в свою очередь порождают набор записей. В последующем проводятся внутренние аудиты, по результатам которых выявляются недостатки. Для устранения недостатков запускают корректирующие и предупреждающие действия, по результатам которых вносятся изменения в управляющие документы. Таким образом замыкается циклический процесс функционирования системы.

Немного в стороне от основного процесса находится описание критических бизнес-процессов (как способ инвентаризации активов) и оценка рисков информационной безопасности (как дополнительный элемент выявления недостатков), которые иногда оказываются проблемными для банка, но в этой статье не рассматриваются. Проблемным может быть и проведение стресс-тестирования СУИБ. Относительно него необходимо отметить следующее — в классическом понимании стандарта стресс-тестирование СУИБ отсутствует. Выходом являются варианты тестирования в режимах, отличающихся от тестирования

обеспечения непрерывности. При этом элементом стресса должны быть провокации на уровне действий и условий.

Циклический процесс функционирования СУИБ

Элементы циклического процесса функционирования СУИБ (представлены на рисунке) имеют следующее значение.

Руководящие документы содержат такие блоки:

- управленческий — обеспечение физической и информационной безопасности (в том числе, управление физическим и логическим доступом, сетью, антивирусной, парольной и криптографической защитой, безопасностью рабочих станций);
- управление персоналом в разрезе обучения ИБ;
- информация с ограниченным доступом и управлением документацией, в том числе вопросы, связанные с классификацией информации и правилами работы с носителями этой информации;
- управлением критическими бизнес-процессами;
- оценка рисков информационной безопасностью и их управлением;
- управление оборудованием, разработкой, тестированием, изменениями;
- управление непрерывностью бизнеса и резервированием информации;
- управление инцидентами ИБ;
- управление отношениями с третьими сторонами;
- «классика» систем управления (анализ со стороны руководства, корректирующие и предупреждающие действия, оценка эффективности);
- внутренние аудиты СУИБ;
- стресс-тестирование СУИБ.

Каждый из руководящих документов запускает от одного до четырех управляющих процессов, реализация которых осуществляется как в ручном, так и в автоматизированном (с использованием технического решения) режиме.

Эти блоки, как правило, так или иначе реализованы банками, хотя в некоторых случаях и возникает потребность в приведении систем в соответствие требованиям стандартов Национального банка Украины по управлению ИБ в банковской системе.

Набор записей — это в основном результат работы, который зависит либо от прилежности ответственного за процесс исполнителя, либо от функционала, реализующего процесс технического решения, и особых вопросов не вызывает.

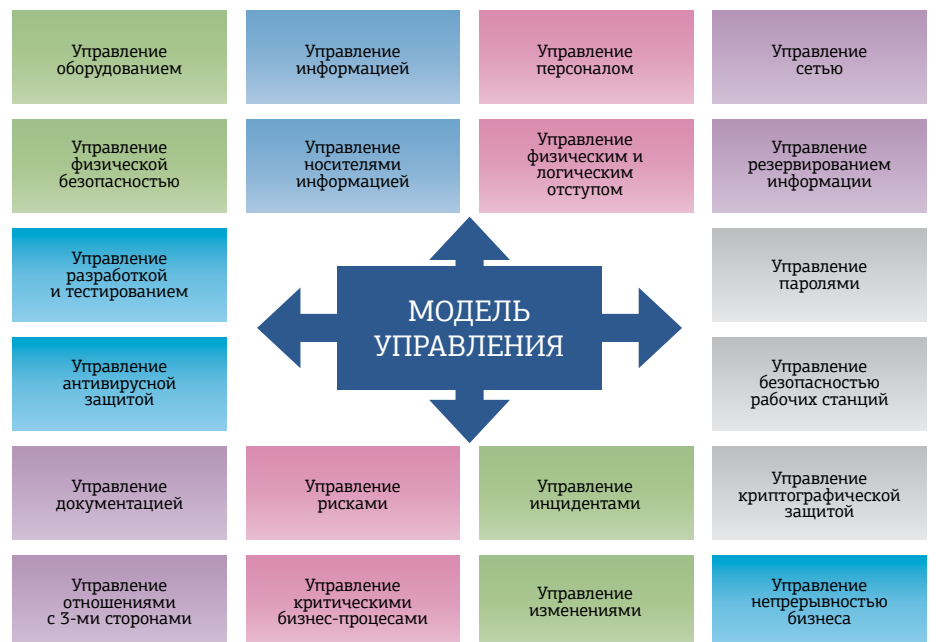
В соответствии с разделом восемь Методических рекомендаций по внедрению системы управления информационной безопасностью и методики оценки рисков (письмо НБУ от 03.03.2011 № 24-112/365) банк должен в запланированные сроки проводить внутренние аудиты СУИБ. Отбор аудиторов и проведение аудитов должны быть объективными и беспристрастными. Аудиторы не должны проводить аудит собственной работы. Когда у банка нет собственного подразделения по аудиту ИБ, привлекаются внешние аудиторы. Специалисты по вопросам ИБ могут выполнять только аудит персонала относительно выполне-

ния всех требований и процедур информационной безопасности.

Требования к аудитору

Сказанное выше не противоречит требованиям ISO 19011: 2011 «Руководящие указания по аудиту систем менеджмента», согласно которому аудит первой стороны — это аудит, проводимый самой организацией или от ее имени. И здесь банку может понадобиться сторонняя помощь. Данная потребность вызвана тем, что не больше 15% украинских банков имеют подразделение аудита информационной безопасности и вынуждены обращаться за помощью к внешним специалистам. Также аудитор должен обладать специальными знаниями, примерный перечень которых представлен в приложении А стандарта ISO 19011: 2011, а именно:

- руководящие указания таких стандартов, как ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004 и ISO/IEC 27005;
- идентификация и оценка требований потребителей и других заинтересованных сторон;
- законы и нормативные акты по ИБ (интеллектуальная собственность; содержание, защита и сохранение записей; защита персональных данных; правила управления криптографической информацией; антитерроризм; электронная торговля; электронные и цифровые подписи; надзор за рабочими местами; эргономика рабочих мест; телекоммуникационный перехват и мониторинг данных (например, e-mail), компьютерные атаки, сбор электронных свидетельств, тестирование проникновений и т.д.);
- процессы, научные и технологические основы менеджмента ИБ;
- оценка рисков (идентификация, анализ и определение уровня риска) и тенденции в технологиях, угрозы и уязвимость;
- риск-менеджмент в области ИБ;
- методы и средства управления информационной безопасностью (электронные и физические);
- методы и практики информационной целостности и доступности;
- методы и практики измерения и оценки результативности ИБ и соответствующие методы управления;
- методы и практики измерения, мониторинга деятельности и ведения записей (включая тестирование, аудиты и анализ).



Кроме этого, аудитор должен знать:

- характеристики информации, которая обрабатывается на объекте, технологии и требования к ее защите;
- правила обращения с информацией с ограниченным доступом на объекте, в том числе условия ее хранения;
- о носителях информации и порядке работы с ними;

- географическое и территориальное расположение объекта;
- пропускной и внутренне-объектовый режим на объекте аудита;
- внедренную на объекте аудита защиту помещений с ограниченным доступом, принципы контроля доступа к таким помещениям;
- топологии корпоративной сети объекта аудита;
- внедренную систему управления сетью;
- виды и характеристики каналов связи;
- принципы построения узла доступа к ресурсам Интернета;
- принципы построения элементов беспроводной связи;
- внедренные средства защиты сети от внешнего и внутреннего несанкционированного доступа, в том числе управление паролями, антивирусной защиты и защиты веб-сайта;
- принципы резервного копирования информации;
- порядок внедрения, внесения изменений, тестирование и сопровождение программного обеспечения;
- внедренные на прикладном уровне системы защиты информации (включая криптографическую защиту и отдельные вопросы генерации и распространения ключей, типы носителей ключевой информации, порядок работы центра сертификации ключей);
- распорядительные документы, регламентирующие деятельность по управлению персоналом;
- функции и полномочия подразделения ИБ;
- порядок работы пользователей на персональных компьютерах;
- принципы аутентификации пользователей и организации доступа к программно-техническим комплексам;
- порядок обслуживания пользователей и управления инцидентами ИБ;
- порядок отношений с третьими сторонами;
- порядок обучения персонала вопросам информационной безопасности.

Модель управления

При этом объектом проверки будет работа модели управления, схематически представленная на рисунке.

Подтверждением работы модели управления является: наличие управляющих документов; реальность существования управляющих процессов; наличие

предусмотренных моделью управления записей в трактовке версии стандарта ISO/IEC 27001 от 2005 года.

Объекты проверки

Исходя из типовой организационной структуры банка, один цикл внутреннего аудита должен охватывать следу-

ПРОДОЛЖЕНИЕ НА С. 22 >>>

КАК МЫ ВЫБИРАЛИ РЕШЕНИЕ ПО СЕТЕВОЙ БЕЗОПАСНОСТИ

АЛЕКСАНДР САПУРА

Угрозы сетевой безопасности — это такая вещь, к которой в большинстве случаев серьезно начинают относиться только после того, как она превратилась в свершившийся факт. Но когда гром грянул, креститься уже поздно. Поэтому не будет лишним еще раз напомнить о том, к чему может привести беспечность, и рассказать, как можно защититься от угроз максимально эффективно.

Для начала краткий ликбез — врага ведь надо знать в лицо. Что такое угроза сетевой безопасности и чем она может быть опасна?

Угроза — это потенциально возможное событие, которое способно причинить ущерб посредством воздействия на компоненты информационной системы. Для реализации угрозы злоумышленники в основном используют уязвимости (чаще всего сетевых протоколов, операционных систем, систем управления базами данных, приложений и т.д.) — именно на них направлены атаки.

Кстати, мы не раз сталкивались с тем, что клиенты (особенно далекие от ИТ) не понимают, зачем кому-то атаковать их информационную систему, какая от этого польза злоумышленникам и в чем состоит их мотивация?

В большинстве случаев мотивация самая простая — деньги, поэтому целью атаки могут быть:

- нарушение нормального функционирования объекта атаки (отказ в обслуживании) — например, DDoS-атака сайта конкурента;
- получение контроля над объектом атаки — к примеру, для рассылки спама;
- получение конфиденциальной и критичной информации — например, кража данных банковских карт;
- модификация и фальсификация данных — к примеру, для затруднения работы конкурента.

Если с вопросом «зачем» разобрались, стоит уделить немного внимания самим механизмам реализации атаки. Злоумышленники могут применять:

- перехват трафика сетевого сегмента (прослушивание);
- сканирование портов (служб) объекта атаки, попытки подбора пароля;
- создание ложных объектов и маршрутов;

- рассылка пакетов определенного типа на атакуемый объект (для отказа объекта или работающей на нём службы);
- вирусы, черви, трояны.

И теперь самый главный вопрос нашего ликбеза — как защищаться от атак? Основные меры предосторожности из категории «must have» включают: сегментацию сети; использование учетных записей с пониженными привилегиями; использование сложных паролей и их регулярная смена; ограничение доступа к конфиденциальным данным; регулярная установка обновлений для приложений и ОС.

Но всего этого может быть недостаточно, и тогда на помощь приходят специальные решения. О своем опыте их выбора и использования мы и расскажем дальше.

Ты помнишь, с чего начиналось...

Начиналось все с переезда в новый офис, в каком-то смысле даже с новой жизни ИТ-инфраструктуры компании. В прежнем офисе границу сети охранял виртуальный шлюз Kerio Control (и свои обязанности выполнял целиком и полностью), но при переезде в новый офис мы столкнулись с требованиями, который старый добрый Kerio не смог потянуть.

Во-первых, хотелось обеспечить большую отказоустойчивость всей системы, то есть продублировать функции. Например, мы планировали подключить двух интернет-провайдеров. В прежнем офисе это было сделать невозможно ввиду монополизации провайдера в бизнес-центре.

Во-вторых, мы столкнулись с трудностями «физического» характера. При проектировании сети офиса на каждое рабочее место было заложено по одной Ethernet-розетке, а для работы сотруднику нужно два IP-адреса из разных подсетей (один для телефона, другой — для ПК), то есть без VLAN (виртуальной локальной сети) нам было не обойтись.

Итак, задача понятна, осталось лишь найти необходимое решение. После первичного анализа в шорт-лист попали следующие разработки:

- Cisco (ASA с подпиской FirePOWER);
- WatchGuard;
- Juniper;
- Check Point;
- FortiGate.

Помимо двух указанных выше критериев нам, как и любой компании, при

выборе был очень важен критерий «цена/производительность». Мы протестировали решения («сделав дырку» в головах поставщиков и вендоров соответственно), и остановили свой выбор на американской компании Fortinet и их решении FortiGate. И вот почему.

Осознанный выбор

Во-первых, FortiGate — это целый комплекс сетевой безопасности, который выполняет массу функций (некоторые из них доступны по подписке, что также сыграло в его пользу): антивирус, IPS, web- и Spam-фильтр, контроль приложений, защита от DoS-атак, DLP, маршрутизация/коммутиция, VPN...

Во-вторых, FortiGate работает как VLAN-коммутиатор и сегментирует офисную сеть (что позволило решить проблему с розетками, заложенную при проектировании).

В-третьих, FortiGate имеет на борту два порта WAN, при помощи которых мы и подключили двух провайдеров Интернета, и таким образом обеспечили бесперебойный доступ во всемирную сеть для наших сотрудников. При этом все критичные сервисы всегда остаются он-лайн. Также есть выделенный DMZ-порт для безопасного подключения внутренних web-серверов.

В-четвертых, в выбранном решении поддерживается также Site-to-Site VPN для организации безопасного соединения филиалов компании (в нашем случае, например, для безопасной удаленной работы сотрудников).

В-пятых, все сервисы безопасности предоставляет одна компания, что гарантирует их консолидацию и слаженную работу. К примеру, если взять устройства компании Juniper, то антивирусная защита там предоставляется на выбор.

Далее, устройства Fortinet поддерживают так называемые виртуальные домены, то есть можно поделить физическое устройство на несколько независимых виртуальных устройств, и обслуживать/настраивать их будут независимые друг от друга администраторы.

Аргументов в пользу этого решения уже, в общем-то, немало, но сомнения оставались, и главное из них — нераспространенность решения на нашем рынке. Мало ли что?... Окончательной соломинкой, сломавшей спину верблюду, стал «user experience» — мы, команда

инженеров, по достоинству оценили удобство работы с решением.

Александр Сапура, инженер компьютерных систем Softkey.ua: «Самое главное достоинство устройства — видимость всего происходящего в сети, что для администратора является важной функцией. Мы постоянно мониторим, какими приложениями пользуются сотрудники, какие web-сайты посещают, сколько трафика расходуют. А потом, на основании анализа логов и отчетов, просто блокируем ненужные сервисы/сайты либо всем, либо только тем, кто злоупотребляет рабочим временем. Имеется множество настроек блокировки приложений. Например, можно заблокировать использовать Skype или просто запретить пересылку файлов посредством Skype, а чат и видеозвонки — разрешить.

Очень удобно предоставлять удаленный доступ сотруднику по VPN. Устройство поддерживает протоколы IPSec и SSL VPN. Есть бесплатный VPN-клиент для устройств на Mac, iOS, Windows, Android. Удаленный доступ настраивается для сотрудника/группы сослуживцев к конкретной сети/серверу (так называемый Policy-Based VPN), то есть на основании политик фаервола каждому сотруднику предоставляется доступ только к необходимым ему ресурсам. С помощью токенов и сертификатов также поддерживается усиленная двухфакторная аутентификация.

Для администратора доступны удобные функции обновления прошивок в два клика, создания бэкапов конфигурации устройства в шифрованный файл. В общем, очевидно, что эти решения создавались администраторами для администраторов».

Вместо заключения

Собственно, вот таким вердиктом и закончились наши муки выбора, о чем мы совершенно не жалеем. Конечно, это совсем не означает, что наш выбор подойдет для любой компании — у всех разная структура, требования к безопасности, тем более что стоимость подписки зависит от определенного устройства, на которое она покупается, а также от количества сервисов безопасности. Но поделиться полезным и позитивным клиентским опытом мы были просто обязаны.

Автор статьи — инженер компьютерных систем Softkey.ua,

ОНЛАЙН-МАГАЗИН APPLE ВПЕРВЫЕ ПОДВЕРГСЯ КРУПНОЙ КИБЕРАТАКЕ

На электронный магазин приложений AppStore совершена первая в его истории масштабная кибератака со стороны неизвестных хакеров. Об этом сообщили в воскресенье представители Apple, уточняя, что компания проводит очистку ресурса от вредоносных программ. Таким образом, можно констатировать, что хакеры изменили методы «работы». Впервые киберпреступники нанесли удар не по пользователям, а по разработчикам, сумев внедрить вирус в программу разработки приложений.

Компания Apple была вынуждена объявить о своих действиях после того, как ряд компаний в сфере кибербезопасности сообщили о появлении вредоносной программы XCodeGhost, встроившейся в сотни легальных приложений. По сообщению Apple, хакеры внедрили вирус, замаскированный под название официального инструмента XCode, используемого разработчиками для создания приложений, что позволяло автоматически внедрить в создаваемую программу лишний код.

Эксперты отмечают, что хакерам впервые удалось столь широко распространить вирусный код в приложения, обойдя строгую систему защиты. Сколько уже удалено из AppStore — неизвестно. Apple также отказались уточнять, как много приложений было скомпрометировано. По данным источников, речь идет как минимум о 344 программах, зараженных XcodeGhost. Среди инфицированных приложений были мобильный чат WeChat, приложение по вызову такси Didi Kuaidi и

музыкальное приложение от интернет-портала NetEase.

Компания не сообщила, какие меры следует предпринять пользователям iPhone и iPad, чтобы определить, заразились ли их устройства в результате кибератаки.

До этого в AppStore было выявлено всего лишь пять зараженных вирусами приложений. Таким образом, нынешний случай является самой крупной из всех зафиксированных ранее угроз безопасности данного магазина приложений.

>>> НАЧАЛО НА С. 19

летворяет его требованиям по защите корпоративных данных. Например, если заказчик уже использует устройства Fortinet для защиты своей внутренней сети, он может продолжить защищать свои корпоративные данные в облаке тоже с помощью решений Fortinet. Мы заключили партнерские соглашения с Amazon AWS и Microsoft Azure, и мы предлагаем заказчикам приобрести защиту как сервис в облаке на основе решений Fortinet.

PC Week/UE: Многие аналитики в сфере ИБ называют новый фронт для борьбы с киб-

ругрозами — «Интернет вещей». Насколько вы согласны с этой точкой зрения, в чем здесь заключается основная опасность и чего можно ожидать в ближайшем будущем?

М.М.: «Интернет вещей» — тренд, который набирает обороты. С точки зрения ИБ — это действительно новый фронт для борьбы. В корпоративном сегменте можно установить определенные правила работы и заставить пользователей им следовать. В случае же с «Интернетом вещей» будет большое количество подключенных конечных точек, каждая из которых является потенциальным источником угрозы. Если учесть, что в будущем фактически во всех домах появятся бытовые устройства,

подключенные к Интернету, то каждый из нас должен позаботиться о безопасности подключения этих систем. Поскольку уровень знаний в области ИБ обычных пользователей (не работающих в области ИТ) довольно низкий, для производителей решений ИБ это тоже вызов: как создать простые в использовании решения по защите, но одновременно обеспечивающие высокий уровень защиты?

PC Week/UE: Какие позиции сегодня занимает компания Fortinet на рынке? Какие типы решений пользуются наибольшим спросом?

М.М.: Глобально компания Fortinet растет в среднем на 25-30% в год.

Например, рост компании за 2014 год составил по сравнению с 2013-м более 25%, а во втором квартале 2015 года по сравнению со вторым кварталом 2014 — более 30%. Как компания, акции которой котируются на бирже, мы не имеем права оглашать локальные результаты. Могу только сказать, что у нас был рост продаж в Украине как в 2014 году, так и в первых трех кварталах 2015-го.

Основным спросом в СМБ пользуются решения UTM, для корпоративного сегмента есть спрос на NGFW-решения. Мы наблюдаем повышенный интерес к решениям для защиты от DDoS-атак и защищенным беспроводным сетям.

IPAD PRO ПОИСТИНЕ НОВЫЙ ПЛАНШЕТ APPLE

«Самые большие новшества с момента появления iPad»

Нарушив традицию запуска своих новых планшетов в октябре, Apple в среду представила потрясающий новый iPad Pro с громадным экраном. Партнеры в канале восторгаются 12,9-дюймовым планшетом, который отвечает заветным чаяниям пользователей — иметь больше возможностей для офисной работы и графического дизайна.

iPad Pro позволит использовать новые аксессуары — клавиатуру и стилус; он получил еще более мощный процессор и функцию сенсорной аутентификации Touch ID. Увеличилось также время работы от батареи. А теперь — подробнее о главных новшествах в новом планшете Apple.

Большой экран

Во-первых, Apple увеличила экран нового планшета: если у iPad Air 2 он был 9,7-дюймовым, то у iPad Pro — 12,9-дюймовая панель Retina. Новый iPad Pro довольно легкий при своем размере: при толщине 6,9 мм он весит 712 г. Экран имеет разрешение 5,6 млн. пикселей и использует усовершенствованную технологию Multi-Touch.

«iPad яснее всего выражает наше видение будущего персональных вычислений, — подчеркнул главный управляющий Apple Тим Кук, представляя новинку в среду. — Это простая [в обращении] мультитач-панель из стекла, которая мгновенно превращается во всё, что вы хотите».

Камера

О камере в новом iPad Pro было лишь сказано, что у нее будет 8-мегапиксельная матрица.

Кроме того, в планшете используется переменная частота регенерации экра-

на, как называет ее Apple, что позволит экономить заряд батареи, автоматически понижая частоту регенерации, когда пользователь читает с экрана, а не смотрит видео. Также, в планшете реализована новая акустическая схема из четырех динамиков.

Более мощный процессор

Apple заявляет, что iPad Pro будет иметь быстроедействие выше, чем 80% портативных ПК, поставленных производителями за последние 12 месяцев, а обработку графики — быстрее, чем у 90% портативных ПК, поставленных за минувший год.

iPad Pro использует 64-разрядный чип третьего поколения A9X, который в 1,8 раз быстрее, чем A8, заявляет компания. Планшет может работать до 10 часов на одном заряде аккумулятора и оснащен технологией сенсорной аутентификации Touch ID.

«Чип A9X [в iPad Pro] побеждает большинство портативных ПК в обработке команд ЦП и в графических задачах, но [планшет] достаточно тонкий и легкий, чтобы носить его с собой весь день», — отмечает Филип Шиллер (Philip Schiller), старший вице-президент по всемирному маркетингу Apple.

Стилус Apple Pencil

Возможности нового планшета можно расширить, купив дополнительный стилус Apple Pencil за 99 долл. *; он позволяет писать заметки и рисовать на экране, сказал Кук. Стилус можно подзарядить через соединитель Lightning, который втыкается прямо в планшет.

Эти новшества, расширяющие возможности работы на iPad, рассматриваются как ключевые в конкуренции с фирмен-

ным планшетом Surface Pro от Microsoft, реализованном как устройство «2-в-1».

Раскладная клавиатура

iPad Pro имеет полноразмерную виртуальную клавиатуру, так что можно комфортно набирать текст прямо с экрана. Для тех, кто привык к традиционной клавиатуре, предлагается раскладная Smart Keyboard за 169 долл. с расширенными возможностями, позволяющая использовать функции QuickType в iOS 9.

Новый Smart Connector с тремя коаксиальными контактами на боковой стороне корпуса позволяет подключить iPad Pro к клавиатуре и устраняет потребность в отдельной батарее, переключателе «Вкл./Выкл.» и соединении по Bluetooth.

Клавиатура — еще одно новшество, которое ставит iPad на равных с Surface Pro в корпоративном сегменте.

Ресурс батареи и связь

Компания заявляет, что заряда батареи iPad Pro хватает на 10 часов с возможностью редактирования трёх потоков 4К-видео одновременно.

Возможности связи включают Wi-Fi 802.11 ac с технологией MIMO и поддержку спектра диапазонов LTE.

Программы для офисной работы

Во время презентации Apple продемонстрировала, как офисные приложения ее конкурента, Microsoft, будут работать в iOS. Microsoft Office — один из нескольких прикладных пакетов на iPad Pro, который будет привлекателен для корпоративных пользователей.

Apple продемонстрировала также одновременную работу трёх приложений Adobe на своем новом планшете, что, наверно, заинтересует дизайнеров графики. Эти приложения — Photoshop Fix для

редактирования фотографий, Photoshop Sketch для рисования и программа Comp, чтобы быстро набросать новые идеи.

iPad mini 4

В ходе презентации компания представила также новый iPad mini 4 как обновление своей линейки уменьшенных планшетов. Новый iPad mini имеет те же возможности, что и iPad Air 2, заявляет Apple; он оснащен 64-разрядным чипом A8 второго поколения, имеет датчик Touch ID, весит 295 г и на 18% тоньше своего предшественника — 6,1 мм.

Новая iOS 9

iPad Pro использует новейшую мобильную операционную систему Apple, iOS 9, которая официально стартует 16 сентября. Она дополнена функциями специально для планшета, в том числе такими функциями многозадачности, как использование «вложенного» и разделенного экрана. iOS 9 включает также новые предустановленные приложения — обновленную Notes, программу транспортной информации Maps и улучшенный голосовой ассистент Siri.

Начало продаж и цены

Планшет iPad Pro поступит в продажу в ноябре и будет стоить от 799 долл. за 32-Гбайт версию до 1079 долл. за 128-Гбайт модель. Предусмотрены три вида «металлической» отделки — серебристого, золотого и «космического серого» цвета. Планшет будет продаваться в фирменных розничных салонах Apple и через авторизованных реселлеров компании. Аксессуары к новому планшету — Apple Pencil, Smart Keyboard и защитные чехлы Silicone Case — также поступят в продажу в ноябре. Новый iPad mini 4 уже в продаже и стоит 399 долл.

IPHONE 6S ВМЕСТО IPHONE 6 – СТОИТ ЛИ ПЕРЕХОДИТЬ?

Apple поднимает свой культовый смартфон на новый уровень. Компания представила две новые модели с литерой «s» — iPhone 6s и 6s Plus — со множеством дополнительных плюсов от интерфейса 3D Touch до 4K-видео, с расширенными функциями фотосъемки и еще более мощным процессором. Но достаточно ли этого, чтобы заставить покупателя отправить в отставку свой имеющийся iPhone 6 Plus? Кому как.

Габариты и вес

Наиболее заметным новшеством в моделях 6s является сенсорный интерфейс 3D Touch, который учитывает силу нажатия на экран при обычных операциях скольжения и касания. Новый интерфейс позволяет «заглянуть внутрь» сообщений электронной почты, не открывая сами письма, а лишь легко удерживая палец вверху сообщения. Если нажать чуть сильнее и дольше, то

сообщение почты будет загружено для обработки. В каком-то смысле это похоже на использование правой кнопки мыши на обычном компьютере, когда выводится контекстное меню со списком опций для файла или приложения.



Корпус и дисплей стали прочнее

Если сравнивать экраны iPhone 6 Plus и нового 6s Plus, то у них один и тот же размер — 5,5 дюйма по диагонали. В новой модели дисплей сделан из более стойкого, ионно-упрочненного стекла — самого прочного среди всех смартфонов,

заявляет Apple. Заранее снимая вопросы о поперечной жесткости смартфона, обе новые модели имеют корпус из более прочного алюминиевого сплава серии 7000, который используется в аэрокосмической промышленности.

Процессор

Обе новые модели 6s используют фирменный 64-разрядный чип Apple третьего поколения A9. Компания заявляет, что его производительность на 70% выше прежнего A8 (используемого в iPhone 6 Plus) в обработке команд общего назначения и на 90% выше в графической обработке. Apple заявляет, что рост производительности процессора — огромный выигрыш для разработчиков игрового софта, так как позволяет строить более сложную среду с улучшенной графикой. Обновлен также сопроцессор обработки данных движения — M9 вместо прежнего M8. Он берет на себя обработку биологи-

ческой обратной связи, а именно данных состояния здоровья. В новой версии эти функции встроены непосредственно в ЦП, обеспечивая более надежное отслеживание.

Камера

Обе модели iPhone 6s оснащены 12-мегапиксельной камерой сзади. Это значительный апгрейд по сравнению с прежним iPhone 6, где использовалась 8-мегапиксельная матрица. Еще одно отличие в том, что модели 6s позволяют делать панорамные снимки размером до 63 мегапикселей, тогда как у iPhone 6 максимальный размер составлял 43 Мпикс. Новая камера позволяет также снимать 4К-видео, чего прежний iPhone 6 Plus не умел. Еще один приятный нюанс для будущих владельцев 6s в том, что дисплей служит также в качестве вспышки True Tone при съемке «селфи», обеспечивая требуемую цветовую температуру.

подтверждается подписью пользователя. Аудитор проверяет, с каким видом информации ограниченного доступа работает сотрудник банка и в каком виде она находится, совпадает ли это с его служебными обязанностями. Пользователь также должен знать, что является признаком отнесения информации к категории «с ограниченным доступом».

Если пользователь работает с информацией в электронном виде, аудитор должен удостовериться, что пользователь понимает к каким автоматизированным системам и хранилищам информации он имеет доступ, как он его получает и может изменить, а также правила выбора пароля доступа и периодичность его изменения.

Если пользователь работает с информацией в бумажном виде, аудитор должен убедиться, что пользователь знает: где хранятся документы и правила их хране-

ния; правила доступа к местам хранения информации; как организована (в общем виде) защита мест хранения.

Аудитор должен удостовериться, что пользователь знает: признаки инцидента ИБ; что делать в случае возникновения инцидента; возникали ли инциденты ИБ с участием конкретного пользователя, если да — что предпринималось по результатам (связь с обучением). Во время аудита выясняется, когда проводилось обучение конкретного пользователя вопросам ИБ (соответствует ли факт заявленной периодичности) и ознакомиться с его результатами (результат тестирования).

По результатам внутреннего аудита должен быть подготовлен отчет, показывающий недостатки, а также запущены корректирующие и предупреждающие действия, которые приведут к исправлению руководящих документов и как

следствие — управляющих процессов и технических решений.

Несмотря на достаточную прозрачность и понятность СУИБ, а также существующую практику в этой области, актуальным и требующим особого внимания и дополнительных ресурсов, остается: приведение систем в соответствие требованиям стандартов НБУ по управлению ИБ; проведение оценки рисков ИБ и стресс-тестирования СУИБ; организация и проведение внутренних аудитов СУИБ; и как дополнительный элемент — обучение ИБ.

Автор статьи — доцент кафедры Систем защиты информации Государственного университета телекоммуникаций, начальник отдела консалтинга и аудита ООО «ЕС АЙ ЦЕНТР»

>>> НАЧАЛО НА С. 20

ющие подразделения: ИБ; обеспечения внутреннего-объектового режима; ИТ; разработки и сопровождения программного обеспечения (при наличии); подразделения риск-менеджмента; внутреннего аудита; управления персоналом; документооборота; бизнес-подразделение фронт-офиса; бизнес-подразделение бэк-офиса; административно-хозяйственное подразделение.

Объектами проверки в основном являются: обращение с информацией; инциденты ИБ и управление ими; обучение вопросам ИБ.

Аудитор должен удостовериться, знает ли пользователь что отнесение информации к категории «с ограниченным доступом» производится в соответствии с внутренним положением и есть четкие перечни, факт ознакомления с которыми

PCWEEK UKRAINIAN EDITION

Уважаемые читатели!
Только полностью заполненная анкета, рассчитана на руководителей, отвечающих за автоматизацию предприятий, специалистов по аппаратному и программному обеспечению, телекоммуникациям, сетевым и информационным технологиям из организаций, имеющих более 10 компьютеров, даёт право бесплатной подписки на газету «PC Week Ukrainian Edition» в течении шести месяцев с момента получения анкеты. Пожалуйста, будьте внимательны при заполнении анкеты!

Примечание: на домашний адрес газета по бесплатной корпоративной подписке не высылается. Данная форма подписки распространяется только на территорию Украины.

Вы можете получить анкету в электронном виде, пишите на адрес: subscribe@pcweek.ua

Правила заполнения анкеты:

1. Записать полные данные по Вашему предприятию.
2. Поставить «✓» напротив выбранной Вами информации.

Название организации _____
 Почтовый адрес организации: Индекс _____ Область _____
 Город _____ Улица _____ Дом _____
 Фамилия _____ Имя _____ Отчество _____
 Подразделение/отдел _____ Должность _____
 Телефон _____ Факс _____ E-mail _____
 WWW _____

1. К какой отрасли относится Ваше предприятие?

1. Энергетика
2. Связь и телекоммуникации
3. Производство, не связанное с вычислительной техникой (добывающие и перерабатывающие отрасли, машиностроение и т.п.)
4. Финансовый сектор (кроме банков)
5. Банковский сектор
6. Архитектура и строительство
7. Торговля товарами, не связанными с информационными технологиями
8. Транспорт
9. Информационные технологии (см. также следующий вопрос)
10. Реклама и маркетинг
11. Научно-исследовательская деятельность (НИИ и ВУЗы)
12. Государственно-административные структуры
13. Военные организации
14. Образование
15. Медицина
16. Издательская деятельность и полиграфия
17. Иное (что именно): _____

2. Если основной профиль Вашего предприятия – информационные технологии – уточните, пожалуйста, сегмент, в котором предприятие работает:

1. Системная интеграция
2. Дистрибуция
3. Консалтинг
4. ИТ-аутсорсинг
5. Розничная продажа компьютерного оборудования
6. Ремонт компьютерного оборудования
7. Разработка и продажа ПО
8. Обучение
9. Иное (что именно): _____

3. К какой категории относится подразделение, в котором Вы работаете?

1. Информационно-аналитический отдел
2. Техническая поддержка
3. Служба АСУ/ИТ
4. Дирекция
5. Инженерно-конструкторский отдел (САПР)
6. Отдел рекламы и маркетинга
7. Бухгалтерия/финансы
8. Производственное подразделение
9. Научно-исследовательское подразделение
10. Учебное подразделение
11. Отдел продаж
12. Отдел закупок/логистики
13. Иное (что именно): _____

4. Ваш должностной статус

1. Директор/президент/владелец
2. Руководитель подразделения
3. Сотрудник/менеджер
4. Консультант
5. Иное (что именно): _____

5. Ваш возраст

1. До 20 лет
2. 21-30 лет
3. 31-40 лет
4. 41-50 лет
5. 51-60 лет
6. Более 60 лет

6. Численность сотрудников в Вашей организации

1. Менее 10 человек
2. 10-100 человек
3. 100-500 человек
4. 500-1000 человек
5. 1000-5000 человек
6. Более 5000 человек

7. Численность компьютерного парка Вашего предприятия

1. 10-20 компьютеров
2. 21-50 компьютеров
3. 51-100 компьютеров
4. 101-500 компьютеров
5. 501-1000 компьютеров
6. 1001-5000 компьютеров
7. Более 5000 компьютеров

8. Имеет ли сеть Вашей организации территориально-распределённую структуру (охватывает более одного здания)?

1. Да
2. Нет

9. Сколько серверов в Вашей организации? _____

10. Какое прикладное ПО используется в Вашей организации?

1. Офисные приложения
2. Средства разработки ПО
3. Графические системы
4. Издательские системы
5. Интернет-браузер
6. ПО для управления производственными процессами
7. САПР
8. Иное (что именно): _____

11. Если в Вашей организации установлено ПО для управления предприятием, то каких фирм-разработчиков?

1. 1С
2. Информационные технологии
3. Галактика
4. Парус
5. Microsoft
6. Oracle
7. SAP
8. Epicor Scala
9. Не установлено никакое
10. Иное (что именно): _____

12. Существует ли на Вашем предприятии единая корпоративная информационная система?

1. Да
2. Нет

13. Используете ли Вы облачные сервисы в компании? Если да, то укажите какие?

1. Да _____
2. Нет

14. Как Вы оцениваете своё влияние на решение о покупке средств информационных технологий для своей организации?

1. Принимаю решение о покупке (подписываю документ)
2. Составляю рекомендацию о приобретении
3. Не участвую в этом процессе
4. Иное (что именно): _____

15. На приобретение каких из перечисленных групп продуктов или услуг Вы оказываете влияние (покупаете, рекомендуете, составляете спецификацию)?

1. Системы
2. Серверы
3. Рабочие станции/Тонкие клиенты
4. Мобильные устройства
5. Системы хранения данных
6. Сетевое оборудование
7. Периферийное оборудование
8. Программное обеспечение
9. Облачные сервисы
10. Ничего из вышеперечисленного

16. Каков наивысший уровень, для которого Вы оказываете влияние на покупку компьютерных изделий или услуг (служб)?

1. Для всего предприятия
2. Для подразделения
3. Для рабочей группы
4. Только для себя
5. Не влияю
6. Иное (что именно): _____

17. Согласен получать рассылки сайта PC Week/UE

Дата заполнения _____

Заполненную анкету пришлите по адресу:
04205, г. Киев, пр-т Оболонский, 35, 2-ой этаж



SI Center - ЛИДЕР ПО ПОСТРОЕНИЮ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ДЛЯ УКРАИНСКИХ БАНКОВ



- ПОСТРОЕНИЕ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И ИТ
- РАЗРАБОТКА И РЕАЛИЗАЦИЯ ПРОЕКТОВ ПО ПОСТРОЕНИЮ ИТ-ИНФРАСТРУКТУР
- МОНИТОРИНГ И УПРАВЛЕНИЕ ИТ-СРЕДОЙ
- ВНЕДРЕНИЕ И РАЗВЕРТЫВАНИЕ ПРИКЛАДНЫХ СИСТЕМ

ООО «ЭС АЙ ЦЕНТР»
тел.: +380 44 364-99-99
e-mail: info@sicenter.ua
<http://sicenter.ua>