ЭКСПЕРТНЫЙ ДОКЛАД

Нелицензионное программное обеспечение и риски для кибербезопасности

По заказу BSA | The Software Alliance

Джон Ф. Гантц
Томас Вавра
Виктор Лим
Январь 2015 г.

Павел Сопер
Профессор Ларс Смит (Луисвиллский университет)
Стивен Минтон

ВВЕДЕНИЕ

В настоящем экспертном докладе проанализирована зависимость между уровнем использования нелицензионного программного обеспечения и количеством заражений вредоносными программами, что позволяет сделать следующие выводы: во-первых, существует четкая корреляция между этими двумя показателями; во-вторых, использование нелицензированного программного обеспечения является сильным *прогностическим фактором* заражения вредоносными программами; в-третьих, существует эмпирическое доказательство причинно-следственной связи.

Аналитики уже давно выяснили, что существует связь между использованием нелицензионного программного обеспечения и угрозой кибербезопасности. Например, когда в 2008 и 2009 годах вирус-червь Conficker распространился через компьютеры по всему миру, аналитики в области кибербезопасности предупреждали, что загрузка нелицензионного программного обеспечения является одним из наиболее вероятных путей заражения компьютера[1]. Через несколько лет в процессе обезвреживания бот-сети Citadel, которая создала 5 миллионов компьютеров-зомби в 90 странах мира, было установлено, что запустившие ее преступники заразили персональные компьютеры частично путем продажи нелицензионных версий Microsoft Windows, предварительно зараженных вредоносной программой Citadel[2]. Таким образом, опубликованное ФБР в 2013 году предупреждение для потребителей о том, что нелицензионное программное обеспечение может содержать вредоносные программы, не стало неожиданностью[3].

Однако до недавнего времени не был проведен тщательный статистический анализ зависимости между использованием нелицензированного программного обеспечения и угрозой в отношении

[1]См. блог-пост Кребса от 20 июня 2011 года о безопасности под названием «Взломанное программное обеспечение: отличный способ заразить ваш компьютер», а также соответствующие комментарии по адресу http://krebsonsecurity.com/2011/06/software-cracks-a-great-way-to-infect-your-pc/.

[2]Краткое описание обезвреживания вируса Citadel можно найти на веб-сайте BBC News, в статье от 6 июня 2013 г., озаглавленной «ФБР и Microsoft обезвредили $500-миллионную воровскую бот-сеть Citadel» («FBI and Microsoft take down $500m-theft botnet Citadel»). См. http://www.bbc.com/news/technology-22795074.

[3]Опубликовано в августе 2013 года и размещено на веб-сайте http://www.fbi.gov/news/stories/2013/august/pirated-software-may-contain-malware.

кибербезопасности со стороны вредоносных программ. Учитывая этот факт, ассоциация BSA | Software Alliance попросила компанию IDC изучить имеющиеся доказательства такой зависимости. Результаты этого анализа убедительно свидетельствуют о том, что государственные постановления и наработанные на уровне отдельных организаций методики, обеспечивающие легальное и должным образом лицензированное использование программного обеспечения, способствуют поддержанию более высокому уровню информационной безопасности вычислительных сред.

ОПРЕДЕЛЕНИЕ КОРРЕЛЯЦИИ

Для определения взаимосвязи между использованием нелицензионного программного обеспечения и угрозами кибербезопасности компания IDC проанализировала данные об использовании нелицензионного программного обеспечения и уровне рисков для кибербезопасности в 81 стране, где имелась достаточно надежная информация в отношении обоих факторов.

Данные об уровне использования нелицензионного программного обеспечения были взяты из *«Глобального исследования рынка программного обеспечения» (Global Software Survey),* которое IDC проводит для BSA раз в два года[4], а информация по угрозе кибербезопасности – из Отчета службы разведки по обеспечению безопасности (Security Intelligence Report) компании Microsoft[5], анализирующего работу 600 млн. пользовательских компьютеров в месяц. В качестве метрики в рамках настоящего экспертного доклада была выбрана *интенсивность заражения вирусами*, выражающаяся в процентных долях. Данные были получены с компьютеров, на которых было установлено антивирус Microsoft, отправляющее ежеквартальные отчеты об обнаружении вредоносного ПО. Для понимания масштабов явления: в течение каждого квартала 2013 года примерно на 20% персональных компьютеров по всему миру фиксировалось попытки заражения вредоносными программами[6].

На рисунке 1 показаны точки, отражающие зависимость количества случаев обнаружения вредоносных программ от уровня использования нелицензионного программного обеспечения в каждой из 81 страны, по которым эта информация была доступна за 2013 год.

---

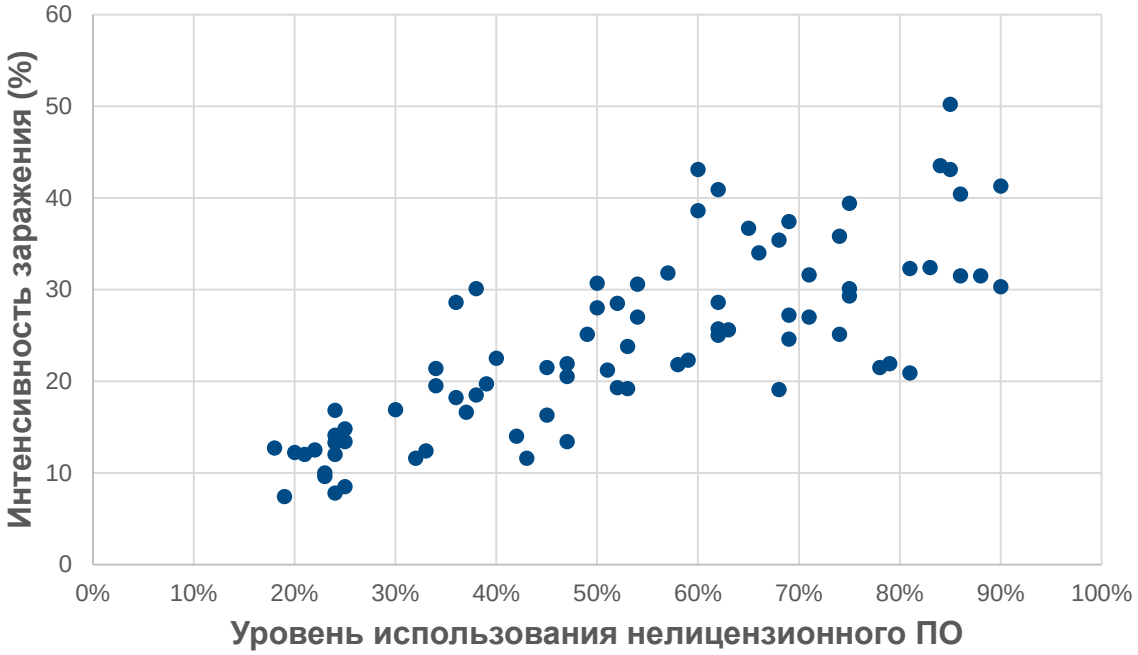
[4]*Глобальное исследование рынка программного обеспечения: пробелы в лицензировании (BSA Global Software Survey: The Compliance Gap)*, июнь 2014 года, размещено на веб-сайте http://www.bsa.org/studies.

[5]Описания данных и методики приведены в выпусках 15 и 16 на веб-сайте http://www.microsoft.com/security/sir/default.aspx.

[6]Является ли это наилучшим показателем в отношении угрозы кибербезопасности? Существуют и другие показатели, опубликованные такими компаниями, как Cisco, IBM, Kaspersky, Microsoft, Symantec, Trend Micro и Verizon, а также государственными и частными группами по действиям в условиях чрезвычайных компьютерных ситуаций. Однако большинство из этих групп, если и располагает информацией по данной стране, концентрируется на источнике угрозы, а не на ее цели. Использование показателей, разработанных для персональных компьютеров и отслеживаемых во многих странах, также удобно для сравнения с показателем уровня использования программного обеспечения для персональных компьютеров.

РИСУНОК 1

Наблюдается сильная корреляция между уровнем использования нелицензионного программного обеспечения и количеством случаев обнаружения вредоносных программ



Каждая точка представляет уровень использования нелицензионного ПО для конкретной страны и соответствующую ему интенсивность заражения вредоносными программами (полная информация приведена в Приложении). Структура демонстрирует статистически сильную корреляцию 0,79 между этими двумя переменными.

Источник: IDC, 2015

Значения явно находятся в прямой зависимости: чем выше уровень использования нелицензионного программного обеспечения для ПК по стране, тем больше в этой стране регистрируется случаев обнаружения на ПК вредоносных программ.

Например, в 2013 году уровень использования нелицензионного ПО в США составлял 18%, а интенсивность заражения была равна, в среднем, 13% за квартал. В Индонезии уровень использования нелицензионного ПО составлял 84%, в то время как интенсивность заражения вредоносными программами была равна, в среднем, 44% за квартал. В Бразилии с уровнем использования нелицензионного ПО 50%, интенсивность заражения за квартал составила 31%.

Статистический анализ подтверждает, что эти две переменные имеют сильную положительную корреляцию, то есть они увеличиваются и уменьшаются в прямой зависимости друг от друга.

Коэффициент корреляции в этом случае составляет 0,79 (1,0 представляет случай идеальной прямолинейной корреляции, 0 означает отсутствие корреляции). Для сравнения: коэффициент корреляции между курением и раком легких составляет 0,72[7], между образованием и доходом - 0,77[8], а строгость антикоррупционной политики и экономический рост показывают коэффициент корреляции 0,77[9].

В то время как эта установленная корреляция не доказывает и не опровергает причинно-следственную связь, она явно демонстрирует тот факт, что при низком уровне использования нелицензированного программного обеспечения наблюдается столь же низкая интенсивность обнаружения вредоносных программ.

ПОСТРОЕНИЕ ПРОГНОСТИЧЕСКОЙ МОДЕЛИ

Следующей фазой анализа была разработка модели, целью которой было определить, с какой точностью можно полагаться на уровень использования нелицензионного программного обеспечения для прогнозирования интенсивности заражения вредоносными кодами. Авторы исследования использовали для этих целей статистическую методику, называемую «регрессионным анализом». В рамках этой методики на основании массивов данных выводится формула, в соответствии с которой одна переменная (уровень использования нелицензированного программного обеспечения) может прогнозировать значение другой (интенсивность заражения вредоносными программами).

На рисунке 2 представлены результаты этого анализа. Если бы формула работала идеально, все значения находились бы на линии. Если бы формула не работала совсем, значения были бы рассеяны беспорядочно. В рассматриваемом случае большинство значений сгруппировано вблизи линии со статистически выраженным прогностическим значением (известным как коэффициент детерминации R-квадрат) 0,62. Это означает, что модель работает достаточно хорошо. Полученный результат можно интерпретировать следующим образом: 62% разницы в интенсивности заражения вредоносным ПО между двумя странами можно считать обусловленными разницей в уровнях использования нелицензионного программного обеспечения в этих странах.

---

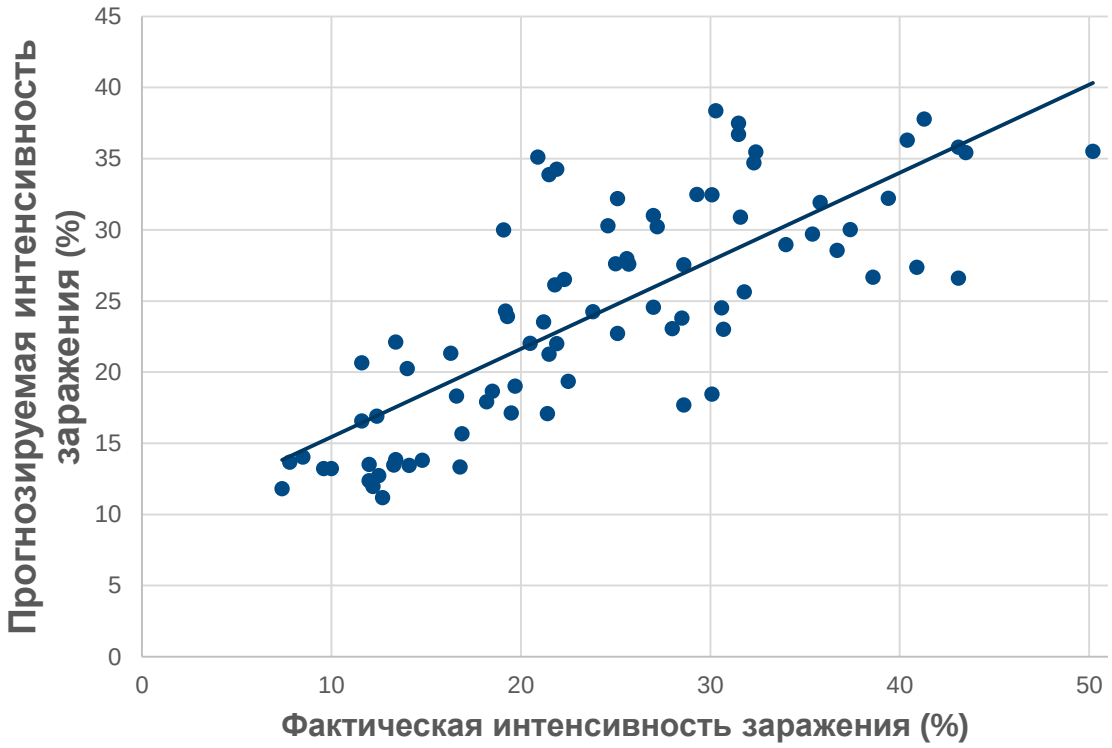
[7]Речь идет о проведенном правительством Англии исследовании, в котором зависимость заболеваемости раком легких от количества выкуриваемых в день сигарет была определена среди тысяч людей в 25 профессиональных группах. С выдержкой из исследования можно ознакомиться на веб-сайте http://www3.nd.edu/~busiforc/handouts/Data%20and%20Stories/correlation/smoking%20and%20cancer/smoking.html, а подробные расчеты, использованные для определения коэффициента корреляции, приведены на веб-сайте http://www.spcforexcel.com/correlation-analysis.

[8]Статистические данные по образованию в различных странах мира (International Education Statistics), автор: Фридрих Хюблер (Friedrich Huebler), август 2008 года, размещено на веб-сайте http://www.spcforexcel.com/correlation-analysis. Корреляция Пирсона определена IDC.

[9]См. Отчет ОЭСР (OECD) по вопросам коррупции и экономического роста, размещенный по адресу http://www.oecd.org/g20/topics/anti-corruption/issues-paper-on-corruption-and-economic-growth.htm.

РИСУНОК 2

Уровень использования нелицензионного программного обеспечения является сильным прогностическим фактором в отношении ожидаемой интенсивности заражения вредоносными программами



Каждая точка представляет уровень использования нелицензионного ПО в конкретной стране и прогнозируемую интенсивность заражения (полная информация приведена в Приложении). Расположение точек демонстрирует статистически сильное прогностическое значение (R-квадрат) 0,62 для зависимости между уровнем использования нелицензионного ПО и интенсивностью обнаружения вредоносных программ.

Источник: IDC, 2015

ДОКАЗАТЕЛЬСТВА ПРИЧИННО-СЛЕДСТВЕННОЙ СВЯЗИ

Факт сильной корреляции между уровнем использования нелицензионного программного обеспечения и интенсивностью заражения вредоносными программами, равно как и свидетельство результатов регрессионного анализа об их взаимной предсказуемости, возможно, не вызывает большого удивления. Однако сами по себе результаты исследования не доказывают, что снижение уровня использования нелицензионного программного обеспечения автоматически приведет к снижению интенсивности заражения вредоносным ПО.

Чтобы сделать такой вывод, результаты статистического анализа необходимо рассмотреть с учетом существования веского *эмпирического* доказательства причинно-следственной связи.

Другими словами, две переменные вполне могут иметь высокое значение корреляции при весьма низкой взаимной прогностической силе в рамках регрессионного анализа. Это происходит, когда корреляция случайна и является результатом простого совпадения. Например, давно замечено, что существует высокая корреляция между объемом продаж мороженого и смертностью в результате убийства в Соединенных Штатах, однако совершенно очевидно, что эти два явления никак не связаны между собой (хотя жаркая погода может быть причиной обоих событий)[10]. Однако в нашем случае доказательства причинно-следственной связи *существуют*.

Например, компанией IDC и Национальным университетом Сингапура (NUS) в 2014 году было проведено исследование, включавшее в себя более 800 проверок персональных компьютеров, купленных с уже установленным нелицензионным программным обеспечением, DVD дисков с нелицензионным ПО, а также нелицензионного ПО и ключей активации, загруженных из Интернета. Тестирование охватывало десятки стран Азии, Европы, Северной и Южной Америк. В ходе проверок было выявлено большое количество вредоносных программ. На основании результатов исследования был сделан следующий вывод: в среднем, пользователь нелицензионного программного пакета получит вредоносную программу с вероятностью один к трем[11].

Эта вероятность заражения, умноженная на количество нелицензионных программных пакетов в мире, дает основания предположить, что в настоящее время всего в обращении находится более 500 миллионов зараженных нелицензионных программных пакетов. (Исследование, кроме того, показало, что более 40% потребителей не осуществляли регулярное автоматическое обновление средств киберзащиты, что также может способствовать заражению персонального компьютера вредоносным кодом).

Исследование, проведенное IDC-NUS на основании соответствующего опроса около 1000 пользователей персональных компьютеров из 15 стран, дало следующие результаты: 1 из 5 респондентов указал, что нелицензионное программное обеспечение заразило его компьютер вирусом, 2 из 5 указали, что оно существенно замедлило работу компьютера, и они были вынуждены его удалить (возможный признак присутствия скрытой вредоносной программы), и 1 из 10 указал, что нелицензионное ПО повредило его файлы.

---

[10] Джастин Питерс (Justin Peters) из журнала *Slate* подготовил сводный отчет по этой корреляции. См. «Одновременно с ростом объема продаж мороженого растет число убийств. Совпадение или следующее эскимо будет Вашим последним?» («When Ice Cream Sales Rise, So Do Homicides. Coincidence, or Will Your Next Cone Murder You?»), 9 июля 2013 года, размещен по адресу: http://www.slate.com/blogs/crime/2013/07/09/warm_weather_homicide_rates_when_ice_cream_sales_rise_homicides_rise_coincidence.html.

[11] *Связующее звено между пиратским программным обеспечением и нарушениями кибербезопасности,* опубликовано в марте 2014 года, размещено по адресу: *http://news.microsoft.com/download/presskits/dcu/docs/idc_031814.pdf*. Это исследование явилось продолжением предыдущих исследований IDC, опубликованных в 2013 и 2007 годах, по теме вредоносных программ в нелицензионном программном обеспечении.

Учитывая все сказанное, неудивительно, что «Глобальное исследование рынка программного обеспечения», проведенное BSA в 2013 году, показало, что пользователи компьютеров во всем мире рассматривают угрозу кибербезопасности со стороны вредоносных программ в качестве главной причины, по которой не следует использовать нелицензионное программное обеспечение.

ВЫВОД

Настоящий статистический анализ и собранные фактические данные указывают на очевидную связь между использованием нелицензионного программного обеспечения и угрозой кибербезопасности. Не любая угроза кибербезопасности является следствием воздействия на систему вредоносных программ, и не все вредоносные программы попадают в систему вместе с нелицензионным ПО. Однако совершенно очевидно, что *некоторые* вредоносные программы *попадают в систему* вместе с нелицензионным программным обеспечением, и *большинство* вирусов представляют угрозу кибербезопасности[12].

Что касается организаций, правительств и потребителей, то очевидно, что одним из способов снижения рисков в отношении кибербезопасности является ограничение использования нелицензионного ПО. Для этого необходимо внедрение и соблюдение эффективных правил и процедур контроля программного обеспечения, а также выделение средств и ресурсов на повышение осведомленности о потенциальных опасностях, связанных с использованием нелицензионного программного обеспечения. Пользователя подстерегают опасности со стороны вредоносных кодов, которые могут быть встроены в программное обеспечение, загружены с веб-сайтов или получены из других источников. Опасность также проистекает от нежелания пользователей нелицензионного программного обеспечения производить регулярные обновления программных средств защиты от вредоносных программ. При этом полученные данные бесспорно свидетельствуют о том, что использование нелицензионного ПО связано с рисками для безопасности со стороны вредоносных программ, потери от которых в мировом масштабе достигают сотен миллиардов долларов в год[13].

[12]В своем отчете, озаглавленном «Отчет о расследованиях нарушений безопасности данных за 2013 год» (2013 Data Breach Investigations Report), компания Verizon определила, что 40% угроз программной защите были связаны с присутствием в системе вредоносных программ, а мишенью 71% вирусов были устройства конечного пользователя. См. ссылку http://www.secretservice.gov/Verizon_Data_Breach_2013.pdf.

[13]См. *Связующее звено между пиратским программным обеспечением и нарушениями кибербезопасности,* в цитируемой работе (*The Link between Pirated Software and Cybersecurity Breaches*, op. cit.)

ПРИЛОЖЕНИЕ. ДАННЫЕ ПО СТРАНАМ, ИСПОЛЬЗОВАННЫЕ В НАСТОЯЩЕМ ИССЛЕДОВАНИИ

Таблица 1 содержит данные для ряда стран, использованные в настоящем исследовании.

ТАБЛИЦА 1

Уровень использования нелицензионного программного обеспечения и интенсивность заражения вредоносными программами по странам в 2013г. (%)

Страна	Уровень использования нелицензионного ПО	Интенсивность заражения вредоносными программами
Молдова	90	30
Грузия	90	41
Венесуэла	88	32
Белоруссия	86	32
Ирак	86	40
Алжир	85	43
Пакистан	85	50
Индонезия	84	44
Украина	83	32
Нигерия	81	21
Вьетнам	81	32
Гватемала	79	22
Кения	78	22
Албания	75	29
Доминиканская Республика	75	30
Тунис	75	39
Китай	74	25
Казахстан	74	36
Ливан	71	27
Таиланд	71	32
Аргентина	69	25
Сербия	69	27
Филиппины	69	37

ТАБЛИЦА 1

Уровень использования нелицензионного программного обеспечения и интенсивность заражения вредоносными программами по странам в 2013г. (%)

Страна	Уровень использования нелицензионного ПО	Интенсивность заражения вредоносными программами
Уругвай	68	19
Эквадор	68	35
Марокко	66	34
Перу	65	37
Болгария	63	26
Греция	62	25
Румыния	62	26
Россия	62	29
Египет	62	41
Индия	60	39
Турция	60	43
Чили	59	22
Кувейт	58	22
Иордания	57	32
Малайзия	54	27
Мексика	54	31
Латвия	53	19
Литва	53	24
Хорватия	52	19
Колумбия	52	29
Польша	51	21
Саудовская Аравия	50	28
Бразилия	50	31
Катар	49	25
Эстония	47	13
Кипр	47	21
Италия	47	22

ТАБЛИЦА 1

Уровень использования нелицензионного программного обеспечения и интенсивность заражения вредоносными программами по странам в 2013г. (%)

Страна	Уровень использования нелицензионного ПО	Интенсивность заражения вредоносными программами
Словения	45	16
Испания	45	22
Гонконг	43	12
Пуэрто-Рико	42	14
Португалия	40	23
Венгрия	39	20
Тайвань	38	19
Корея	38	30
Словакия	37	17
Франция	36	18
ОАЭ	36	29
Чешская Республика	34	20
ЮАР	34	21
Ирландия	33	12
Сингапур	32	12
Израиль	30	17
Норвегия	25	9
Канада	25	13
Нидерланды	25	15
Финляндия	24	8
Швейцария	24	12
Германия	24	13
Англия	24	14
Бельгия	24	17
Швеция	23	10
Дания	23	10
Австрия	22	13

ТАБЛИЦА 1

Уровень использования нелицензионного программного обеспечения и интенсивность заражения вредоносными программами по странам в 2013г. (%)

Страна	Уровень использования нелицензионного ПО	Интенсивность заражения вредоносными программами
Австралия	21	12
Новая Зеландия	20	12
Япония	19	7
США	18	13

Источник: IDC, 2015

О компании IDC

Компания International Data Corporation (IDC) является ведущим мировым провайдером аналитической рыночной информации, консультативных услуг и организации мероприятий в сфере информационных технологий, телекоммуникаций и рынков потребительских технологий. IDC помогает специалистам в области ИТ, руководителям организаций и инвесторам принимать грамотные, обоснованные решения о приобретении технологий и при выработке стратегий ведения бизнеса. Более 1100 аналитиков компании IDC предоставляют на глобальном, региональном и местном уровне свои заключения в отношении направлений развития и возможностей технологии и отраслей индустрии в более чем 110 странах мира. В течение 50 лет компания IDC предоставляет своим клиентам стратегический анализ, который помогает им решать важные бизнес-задачи. IDC является дочерней структурой компании IDG - мирового лидера в области технологических СМИ, исследований и мероприятий.

Международный головной офис

5 Speen Street
Framingham, MA01701
USA
508.872.8200
Твитер: @IDC
idc-insights-community.com
www.idc.com