Тенденции использования нелицензионного программного обеспечения в России

По заказу BSA

Комментарий от IDC

На протяжении многих лет установка нелицензионного ПО оставалась серьезной проблемой для России. Однако в последние годы уровень использования контрафактного ПО значительно снизился, хотя он по-прежнему остается довольно высоким по сравнению с остальными развитыми странами.

Чтобы лучше понимать разницу между рынком России и рынками других стран, основное внимание в данном отчете уделяется ключевым тенденциям, которые влияют на изменение уровня нелицензионного использования ПО в стране. Специалисты IDC полагают, что в стране также существует различия в уровне использования нелицензионного ПО в зависимости от федерального округа. Тремя основными факторами, обуславливающими такие различия, являются социально-демографические характеристики региона, способы и методы приобретения ПО, и отношение населения региона к нелицензионному использованию ПО.

Настоящий отчет призван помочь предприятиям ИТ-отрасли, индивидуальным пользователям, а также лицам, определяющим политический курс, более эффективно планировать и реализовывать стратегии, направленные на сокращение доли нелицензионного ПО. Кроме того, отчет поможет лучше понять отношение к использованию нелицензионного ПО со стороны индивидуальных лиц и организаций во всех федеральных округах России.

Методология

При подготовке настоящего исследования использовались три основных источника данных. Первым источником данных послужило глобальное исследование BSA об уровне компьютерного пиратства в мире, которое было проведено исследовательской фирмой IDC ранее в этом году. Кроме того, было проведено два количественных исследования рынка, а также проанализировано две группы специальных интервью с индивидуальными пользователям и организациями в России.

Методология данного исследования ставит своей целью изучение программного обеспечения, установленного на персональных компьютерах – как на домашних, так и на офисных ПК. Эксперты IDC учитывали случаи как умышленного, так и непреднамеренного использования нелицензионного ПО, оценивая при этом объёмы ПО, установленного на ПК без выплаты надлежащего вознаграждения владельцам авторских прав. В рамках данного исследования мы не принимали в расчет программное обеспечение, запущенное на других устройствах, отличных от ПК (например, на серверах).

Общий уровень использования нелицензионного ПО в России, как и в других странах, вошедших в Глобальное исследование компьютерного пиратства, вычислялся согласно единой методологии, разработанной IDC, которая подразумевает сравнение совокупной стоимости программного обеспечения, реализованного на рынке, с общим количеством установленного на рынке ПО. В свою очередь, оценка общего количества установленного ПО осуществлялась исходя из общего количества используемых ПК и количества установленного ПО в расчете на каждый ПК.

Для оценки региональных тенденций компьютерного пиратства в России использовалась модель IDC, позволившая получить количество установленных ПК по региону, при этом в основном исследовании оценивается спрос и отражаются основные показатели компьютерного пиратства. Таким образом, мы провели два исследования пользователей ПК в семи федеральных округах России.

В рамках каждого исследования было опрошено 525 респондентов по всей России, представляющих все регионы страны. В первом исследовании индивидуальные пользователи персональных компьютеров отвечали на вопросы относительно того, каким образом они используют программное обеспечение в личных целях и по работе, а также об их отношении к пиратству. Второй опрос осуществлялся среди ИТ-директоров компаний самых различных размеров и работающих в различных секторах, во всех

регионах страны. Основные вопросы касались политик этих организаций, направленных на противодействие пиратству, и затрагивали отношение тех, кто отвечает за закупку программного обеспечения в этих организациях, к задачам сокращения компьютерного пиратства.

В целях обеспечения согласованности и качества данных, результаты этих двух отдельных опросов прошли перекрёстную проверку. Региональные уровни нелицензионного использования ПО вычислялись с использованием модели, в которой использовались статистические данные о населении, фирмография, статистика количества используемых ПК по каждому федеральному округу, а также данные о нелицензионном использовании ПО, полученные в ходе опроса.

В ЭТОМ ДОКУМЕНТЕ

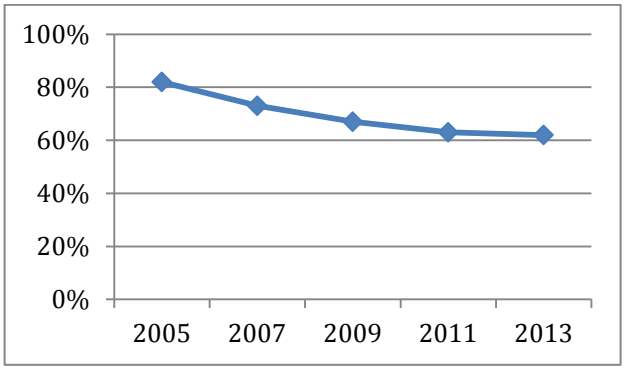
IDC изучает данные об уровне использования нелицензионного ПО в регионах России, анализирует отношение населения к использованию нелицензионного ПО и приводит рекомендации, помогающие снизить уровень использования нелицензионного ПО в России.

ОБЗОР СИТУАЦИИ

Уровень использования нелицензионного программного обеспечения в России значительно выше, чем на развитых рынках. Для сравнения во Франции, которая резко выделяется на фоне остальных развитых рынков, уровень использования нелицензионного ПО находится в диапазоне 40%-45%, тогда как в странах Северной Америки уровень использования нелицензионного ПО находится ниже 19%. Однако за последние восемь лет, благодаря изменению отношения пользователей к проблеме нелицензионного ПО, сравнительно стабильной покупательской способности и предпринимаемых правительством мер по борьбе с компьютерным пиратством, уровень использования нелицензионного ПО в России значительно снизился - с 83% до 63% в 2011 году. С тех пор установившийся уровень менялся очень незначительно. Таким образом, из страны с высоким уровнем компьютерного пиратства, Россия превратилась в рынок, где уровень использования нелицензионного ПО соответствует среднему уровню на рынках Центральной и Восточной Европы, который там составляет 61%. По состоянию на 2013 год, уровень использования нелицензионного ПО в России составляет 62%.

РИСУНОК 1

Уровень использования нелицензионного ПО в России



Источник: IDC, 2014

По данным IDC Russia, собранным ранее в 2014 году, потери российских организаций в связи с использованием вредоносного или нелицензионного ПО составят 20 млрд. долларов США. Из них 4,9 млрд. долларов США будет потрачено на выявление и решение проблем, связанных с использованием нелицензионного программного обеспечения, а потери на общую сумму 15 млрд. долларов США будут связаны с утечками данных.

Таким образом, угроза от использования нелицензионного ПО, а также связанные с этим риски, по-прежнему остаются весьма высокими как для корпоративных, так и для индивидуальных пользователей. Далее в данном исследовании будут рассмотрены экономические последствия использования нелицензионного ПО, а также иные сопутствующие факторы, влияющие на корпоративную репутацию и связанные с юридическими вопросами.

В следующем разделе данного документа мы проанализируем характер использования нелицензионного программного обеспечения, а также отношение населения к этому феномену, и сопоставим их с общим уровнем использования нелицензионного ПО за год. Анализ данных по федеральным округам представлен в следующем разделе настоящего документа.

РЕГИОНАЛЬНЫЙ АНАЛИЗ

Для более точной оценки уровня использования нелицензионного программного обеспечения по регионам специалисты IDC обратились к данным по семи федеральным округам России:

1. Центральный федеральный округ

2. Южный федеральный округ

3. Северо-западный федеральный округ

4. Дальневосточный федеральный округ

5. Сибирский федеральный округ

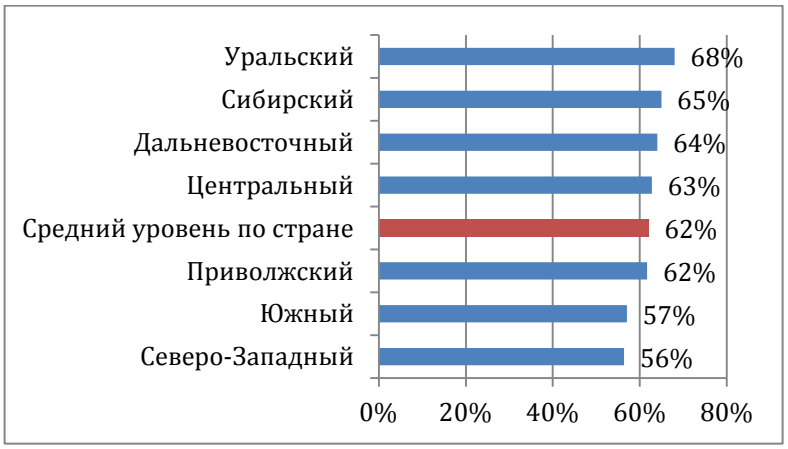
6. Уральский федеральный округ

7. Приволжский федеральный округ

Данные об уровне использования нелицензионного программного обеспечения в разбивке по федеральным округам представлены на рисунке 2.

РИСУНОК 2

Уровень использования нелицензионного программного обеспечения по федеральным округам



Источник: IDC, 2014

Результаты, представленные на диаграмме выше, свидетельствуют о том, что по меньшей мере в двух из семи регионов наблюдается лишь небольшое отклонение от общего уровня использования нелицензионного ПО в России. В Центральном федеральном округе и в Приволжском федеральном округе уровень использования нелицензионного ПО имеет лишь незначительное отклонение от среднего по России уровня. Двумя регионами, продемонстрировавшими наименее низкий уровень использования нелицензионного ПО, являются Северо-западный и Южный федеральные округа. В то же время, в Дальневосточном, Сибирском и Уральском федеральных округах, уровень использования нелицензионного ПО оказался выше, чем в среднем по стране.

Ответы респондентов свидетельствуют о том, что причины столь различных результатов объясняются главным образом разным характером процесса закупок программного обеспечения, а также различиями в предрасположенности к пиратству и в общем отношении населения к использованию нелицензионного ПО. Анализируя ответы на вопросы, связанные с характером приобретения ПО, можно увидеть, что среди респондентов из Дальневосточного, Сибирского и Уральского федеральных было больше тех, кто утверждал, что приобретал все компьютеры без предустановленного ПО: в этих регионах данная метрика находилась в пределах 29%-32%, тогда как среднее значение по всем респондентам было чуть ниже 27%. Еще одно любопытное наблюдение заключается в том, что среди респондентов из Уральского федерального

округа было большее количество тех, кто утверждал, что за последние два года самостоятельно собирал компьютеры из комплектующих. Характер процесса закупки программного обеспечения и отношение респондентов к проблемам управления лицензиями являются двумя основным аспектами, на которых необходимо заострить внимание, чтобы поддержать усилия по снижению уровня использования нелицензионного ПО в России.

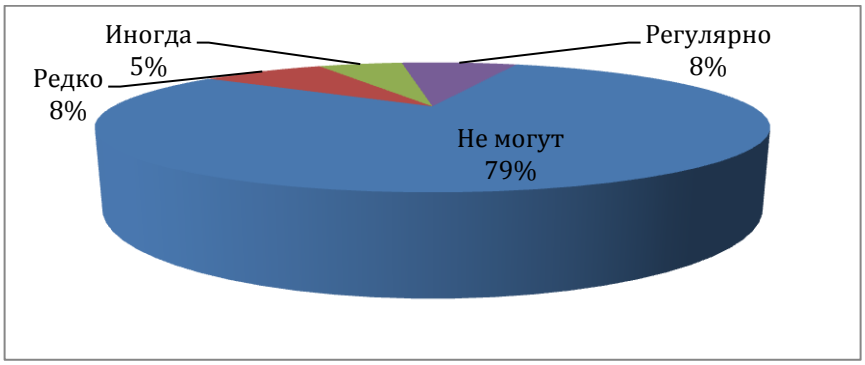
ПОКАЗАТЕЛИ ПРЕДРАСПОЛОЖЕННОСТИ К ИСПОЛЬЗОВАНИЮ НЕЛИЦЕНЗИОННОГО ПО

В результатах исследования приведён ряд показателей, указывающих на предрасположенность индивидуальных пользователей и лиц, отвечающих за принятие решений, к проблемам и сложностям, связанным с применением нелицензионного ПО. Многие из этих показателей являются общими для всех регионов и относятся к поведенческой модели российских пользователей ПК и их отношению к исследуемой проблеме в целом. Поэтому несмотря на отсутствие достаточной статистической базы для измерения отклонений в каждом из этих показателей по регионам, существующие данные позволяют судить об основных задачах и выстраивать общие направления политик и инициатив, нацеленных на снижение уровня использования нелицензионного ПО в России.

Один из показателей, принимаемых во внимание, заключается в проверке того, предусмотрены ли в организации правила и политики, которые бы ограничивали сотрудников в деятельности, связанной с установкой программного обеспечения, то есть предусмотрена ли в организации централизованная процедура, которая бы контролировалась сотрудниками ИТ-подразделения. Результаты опроса относительно реализуемых в организациях подходов по централизации процессов установки программного обеспечения представлены на Рисунке 3.

РИСУНОК 3

Могут ли сотрудники самостоятельно устанавливать программное обеспечение на своих компьютерах?



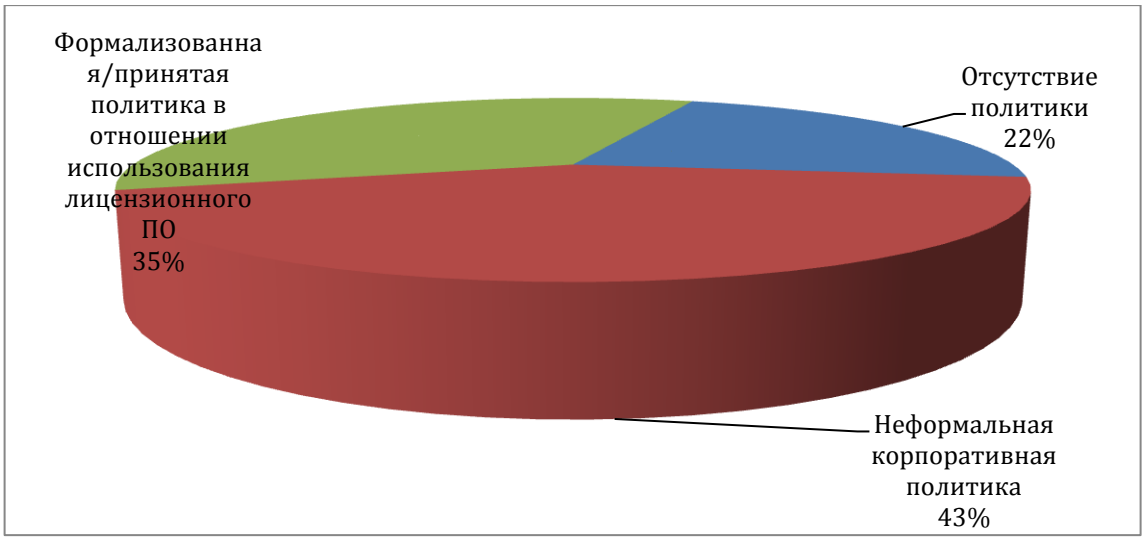
Источник: IDC, 2014

Эти данные свидетельствуют о том, что в четырех случаях из пяти сотрудники не могут самостоятельно устанавливать программное обеспечение, а сам процесс установки ПО контролируется специалистами ИТ-подразделений. Всё это способствует снижению рисков, связанных с использованием нелицензионного ПО. Более того, 58% опрошенных ИТ-директоров считают, что самостоятельная установка программного обеспечения сотрудниками компаний сопряжена с дополнительными рисками безопасности для организаций.

Одним из основных индикаторов, свидетельствующих о систематическом подходе, призванном минимизировать использование нелицензионного программного обеспечения, является наличие принятой корпоративной политики в отношении использования лицензионного ПО. Результаты опроса о наличии в организации подобной корпоративной политики по лицензированию программного обеспечения представлены на Рисунке 4.

РИСУНОК 4

Корпоративная политика в отношении использования лицензионного ПО



Источник: IDC, 2014

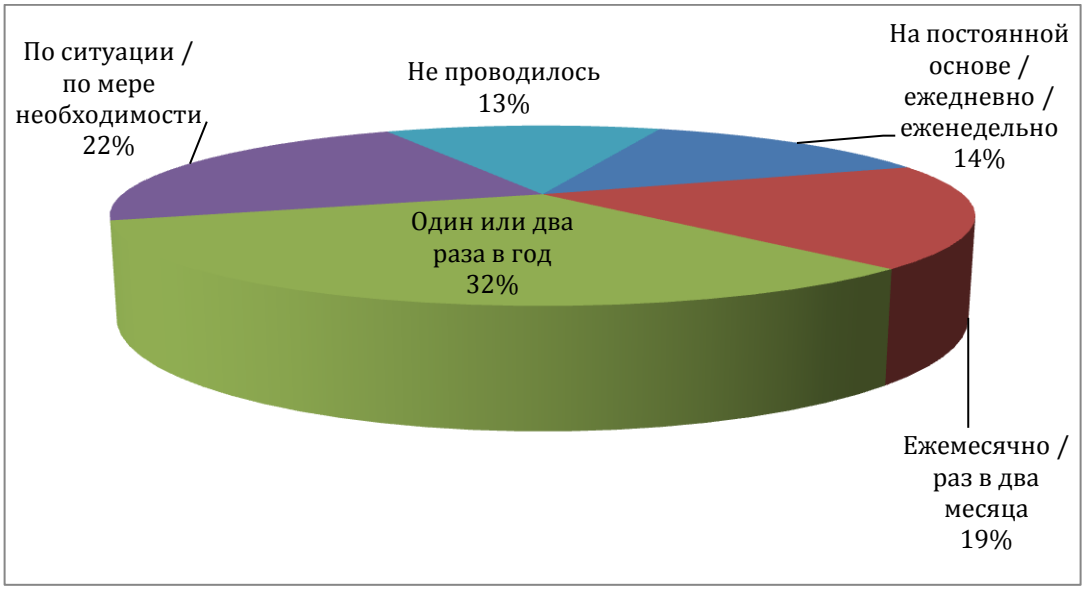
В настоящее время лишь чуть больше чем в трети опрошенных компаний (35%) предусмотрена и действует формальная, документально оформленная политика, направленная на сокращение использования нелицензионного ПО, при этом в 22% организаций такой политики не предусмотрено. Наиболее популярной практикой в российских компаниях

является использование неформальной корпоративной политики лицензирования ПО, а это означает, что в 78% опрошенных компаний хотя бы в минимальной форме действуют корпоративные политики в отношении лицензирования ПО.

Еще одним важным индикатором, указывающим на то, что организация способствует внедрению процессов управления лицензированием ПО, является проведение аудитов на лицензионную чистоту установленного программного обеспечения. Результаты опроса о том, насколько регулярно в компаниях проводятся подобные аудиты, представлены на Рисунке 5.

РИСУНОК 5

Регулярность лицензионных проверок в российских компаниях и организациях



Источник: IDC, 2014

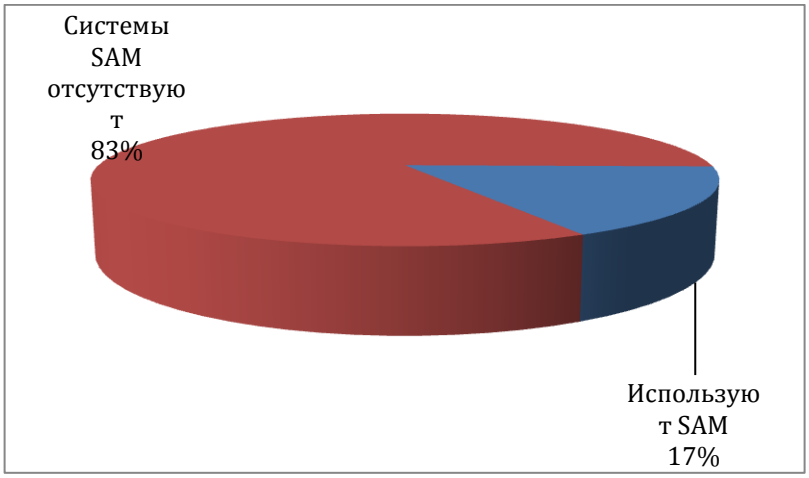
Осуществление регулярных повседневных аудитов лицензионной чистоты ПО является явным признаком того, что организация ведёт систематическую, целенаправленную работу по сокращению рисков использования нелицензионного программного обеспечения. По результатам данного исследования можно говорить о том, что все российские компании разделились на три примерно равные группы. Примерно в одной трети компаний аудиты проводятся на постоянной / непрерывной / ежедневной основе, или по меньшей мере еженедельные или ежемесячные аудиты наличия лицензий на все установленное ПО для персональных компьютеров. Во второй группе компаний подобные аудиты проводятся реже - один или два раза в год, в оставшейся трети не

проводится каких-либо периодических аудитов, проверки осуществляются либо эпизодически, либо не осуществляются вообще. Эти данные соответствуют текущему уровню использования нелицензионного ПО в России, составляющему 62%.

Одна из важных инициатив, позволяющих сократить уровень использования нелицензионного ПО, заключается в развёртывании на предприятии системы управления программными активами. В настоящее время, как показано на Рисунке 6, подобная система внедрена в среднем лишь в одной из каждых шести организаций.

РИСУНОК 6

Уровень проникновения методологий SAM в российских компаниях и организациях



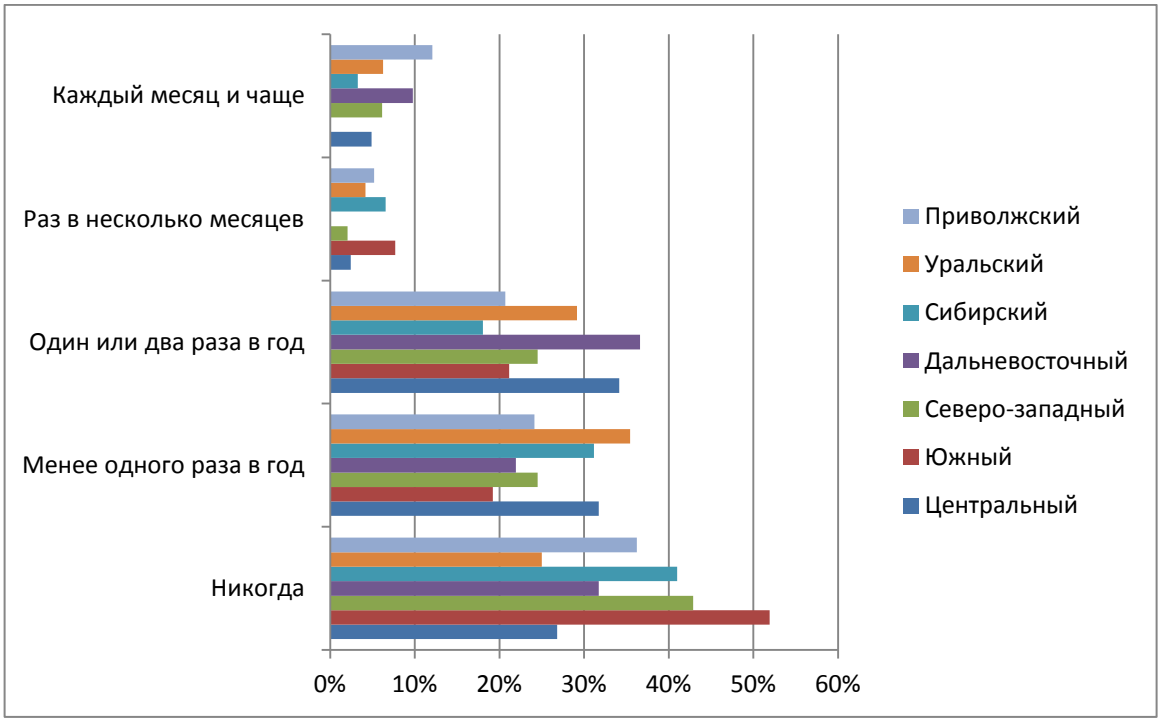
Источник: IDC, 2014

Из всех семи федеральных округов, данные по которым представлены в настоящем исследовании, наиболее высокий уровень проникновения систем управления программными активами зафиксирован в Южном федеральном округе и в Приволжском федеральном округе, где, подобная система в настоящее время используется, соответственно, у 21% и 23% опрошенных компаний.

Какие бы меры ни предпринимались для противодействия нелицензионному использованию ПО, основная задача для организации заключается в том, чтобы избежать или предотвратить сбои в работе своих систем - ситуации, когда сетевая инфраструктура, веб-сайты или ПК перестают функционировать из-за брешей в информационной безопасности. Статистика подобных случаев приведена на Рисунке 7.

РИСУНОК 7

Регулярность сбоев и неполадок в работе ИТ-систем организаций



Источник: IDC, 2014

На рисунке выше можно увидеть, что примерно две трети всех российских компаний либо вовсе не испытывают сбоев в работе своей ИТ-инфраструктуры из-за уязвимостей в системах информационной безопасности, либо подобные сбои происходят реже одного раза в год. Столь высокий уровень информационной безопасности является косвенным индикатором успешной реализации корпоративных политик по соблюдению лицензионной чистоты. Наиболее высокие показатели по этой метрике - чуть больше 70% - продемонстрировали компании из Южного и Сибирского федеральных округов. Остальным предприятиям следует незамедлительно рассмотреть возможность реализации кампаний по сокращению уровня использования нелицензионного ПО, которые осуществляются при активной поддержке со стороны государственных органов и отраслевых экспертов.

Чтобы можно было максимально эффективно спланировать содержание кампаний, направленных на снижение доли нелицензионного ПО, важно полностью понимать воспринимаемую значимость различных рисков,

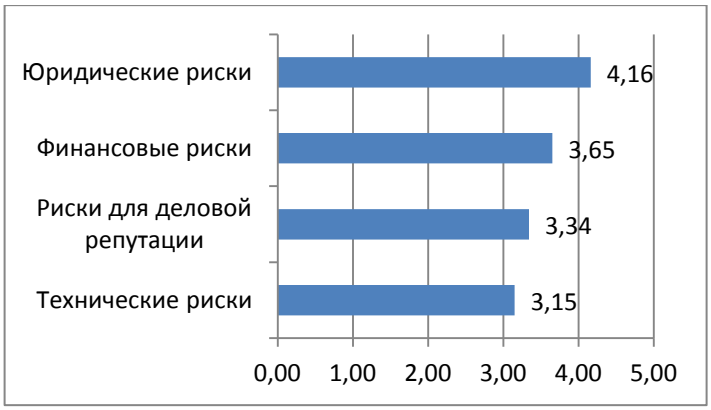
связанных с использованием нелицензионного ПО.

Во-первых, специалисты IDC проанализировали восприятие четырех крупных групп риск, связанных с использованием нелицензионного ПО. Наряду с традиционно признанными техническими рисками, обусловленными использованием нелицензионного ПО, результаты опроса свидетельствуют о растущей информированности о нематериальных рисках, в том числе юридических рисках и рисках для деловой репутации. Соответствующие результаты представлены на Рисунке 8.

РИСУНОК 8

Воспринимаемая значимость различных рисков использования нелицензионного ПО.

Оценки даны по пятибалльной шкале, где 1 балл – не имеет значения, 5 баллов – чрезвычайно важно.



Источник: IDC, 2014

На рисунке 8 показано, что в отличие от ситуации, наблюдавшейся всего лишь несколько лет назад, сегодня наиболее значимыми для большинства пользователей являются финансовые риски, а не казалось бы более очевидные технические риски, связанные с применением нелицензионного ПО. Более того, по степени воспринимаемой значимости технические риски находятся лишь на третьем месте, после юридических рисков. В целом, эти результаты свидетельствуют о произошедшем сдвиге в общественном восприятии в сторону опасений относительно нематериальных последствий использования нелицензионного или ненадлежащим образом лицензированного ПО. Теперь эти потенциальные нематериальные последствия воспринимаются столь же значимыми, что и материальные, что в свою очередь диктует потребность в реализации формальной политики по использовании лицензионного ПО, а также свидетельствует об очевидной необходимости внедрения инструментов SAM.

Специалисты IDC собрали информацию о наиболее значимых причинах не использовать нелицензионное ПО. Соответствующие результаты представлены на Рисунке 9.

РИСУНОК 9

Основные причины воздержаться от использования нелицензионного ПО: мнение ИТ-директоров

Источник: IDC, 2014

Результаты свидетельствуют о том, основной причиной, побуждающей предприятия использовать лицензионное программное обеспечение, по-прежнему остаются технологические риски, связанные с пробелами в информационной безопасности. Другие аспекты, в том числе наличие юридических и финансовых рисков, не столь очевидны для пользователей. Поэтому перед ИТ-отраслью по-прежнему стоит задача повышать информированность пользователей ПК о нематериальных негативных последствиях, обусловленных использованием нелицензионного или ненадлежащим образом лицензированного ПО. При сравнении данных по регионам, можно увидеть, что хотя во всех регионах основной причиной воздержаться от использования нелицензионного ПО являются возможные проблемы с безопасностью, только для компаний Центрального федерального округа почти таким же по значимости фактором в пользу работы с лицензионным ПО является отсутствие технической поддержки со стороны разработчика (50% упоминаний). И наоборот, в Южном, Северо-западном, Сибирском и Уральском федеральных округах отсутствие поддержки со стороны разработчика оказалось позади рисков для деловой

репутации, которые оказались более весомым доводом воздержаться от применения нелицензионного ПО.

ПРОБЛЕМЫ И ВОЗМОЖНОСТИ

Результаты исследования подтверждают, что использование нелицензионного ПО несёт в себе целый ряд негативных последствий, которые не ограничиваются одним лишь финансовым воздействием на софтверную индустрию. Эти потенциальные эффекты всё более внимательно воспринимаются, оцениваются и анализируются индивидуальными пользователями ПК, компаниями и правительственными структурами, при этом последние вынуждены принимать согласованные меры, направленные на сокращение доли нелицензионного ПО.

Данное исследование показывает, что отсутствие централизованного управления процессами установки ПО, отсутствие формальных, документально зафиксированных правил и политик, регламентирующих процессы лицензирования ПО, а также злоупотребление лицензиями являются основными источниками риска для компаний в России. Проблемам информационной безопасности следует уделять особое внимание при формировании любых бизнес-процессов в компаниях и организациях.

IDC рекомендует:

✓ Применять в организациях формальные, документально зафиксированные правила и политики в отношении использования лицензионного ПО.

✓ Внедрять на предприятиях и поддерживать в актуальном состоянии системы управления программными активами (SAM).

✓ Регулярно и разумной периодичностью проводить в масштабах всей организации аудиты на соблюдение лицензионной чистоты.

Индивидуальные пользователи могут подвергаться дополнительным рискам, которые могут быть обусловлены непреднамеренным использованием нелицензионного или ненадлежащим образом лицензированного ПО. Подобные ситуации возможны в связи с наличием различных каналов приобретения ПО с различной степенью прозрачности, что обуславливает возможные трудности с приобретением надлежащего числа лицензий. Кроме того, увеличению доли нелицензионного ПО в домашнем использовании способствует обмен программами с другими пользователями, и возможность загрузки нескольких копий одного и того же продукта членами одной семьи. Во всех этих случаях индивидуальные пользователи могут потерять время и деньги в случае заражения их ПК

вредоносным кодом или вирусами.

IDC рекомендует частным лицам:

✓ Использовать только надежные каналы приобретения программного обеспечения, уделяя должное внимание лицензионной чистоте и соблюдению надлежащих выплат правообладателям.

✓ избегать самостоятельной сборки ПК или услуг недобросовестных интеграторов, устанавливающих ПО в отсутствие надлежащих лицензий.

✓ не пользоваться пиринговыми сетями для обмена данными и файлами, поскольку это может привести к существенным финансовым потерям.

Что касается правительств и государственных структур, то с их точки зрения использование нелицензионного ПО представляет собой значительную проблему в силу негативного влияния на размеры налоговых поступлений, а также общего негативного эффекта от того, что граждане и организации подвергаются различным рискам. На протяжении нескольких лет лидеры софтверной отрасли и Правительство Российской Федерации совместными усилиями информировали общественность и отдельные целевые аудитории о рисках и негативных последствиях использования нелицензионного ПО.

IDC рекомендует:

✓ Продолжать реализацию мер по формированию эффективного правового окружения, регламентирующего использование лицензионного ПО частными лицами и предприятиями.

✓ Проводить обширные образовательные кампании с целью объяснения общественности негативных экономических последствий от применения нелицензионного или ненадлежащим образом лицензированного ПО рядовыми пользователями.

✓ Обеспечивать более широкую государственную поддержку мероприятиям, направленным на противодействие пиратству, в том числе поощрять компании и организации использовать передовые мировые практики в отношении управления программными активами.

✓ Продолжать систематическую поддержку правоприменительной деятельности по защите авторских прав.

ВЫВОДЫ

В данном исследовании, составленном IDC, подробно анализируется ситуация с относительно высоким уровнем использования нелицензионного ПО в России в сравнении с развитыми странами. Исследование подробно останавливается на ключевых факторах, влияющих на долю нелицензионного ПО, в том числе приводится анализ региональных различий в характере процедур закупки ПО, а также разница в восприятии нелицензионного ПО индивидуальными и корпоративными пользователями. Приводятся рекомендации, помогающие сократить долю нелицензионного ПО и избежать некоторых сопутствующих рисков. Эти рекомендации представлены для трёх целевых аудиторий: индивидуальных пользователей ПК, компаний и организаций, и для правительственных структур и отраслевых экспертов.

Специалисты IDC рекомендуют использовать настоящее исследование в качестве ориентира при реализации дальнейших инициатив по сокращению уровня использования нелицензионного ПО в России, и в частности в регионах, где нелицензионное программное обеспечение по-прежнему представляет собой значительную проблему. Кроме того, в исследовании анализируются отдельные показатели, характеризующие поведение пользователей ПК, установившаяся у них практика работы с ПО и общее отношение пользователей к проблеме. Предложенный анализ может служить в качестве подспорья при планировании мероприятий, направленных на сокращение доли нелицензионного ПО.