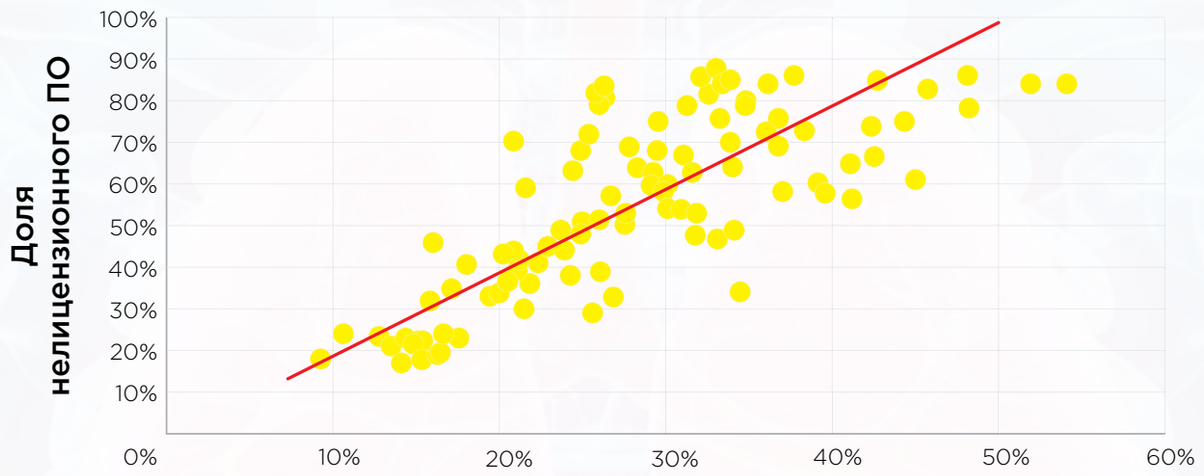
Угрозы безопасности, связанные с нелицензионным программным обеспечением в странах Европы: причины и ущерб — 2017 г.

Отчет IDC InfoBrief | Сентябрь 2017 г.

IDC
ANALYZE THE FUTURE

Сильная корреляция между вредоносными программами и нелицензионным ПО

Соотношение случаев заражения вредоносным кодом и доли нелицензионного ПО в 102 странах



- **Сильная корреляция (0,77)** — сильнее, чем между курением и раком легких (0,72).
- Высокий коэффициент корреляции еще не доказывает причинно-следственную связь, но ее подтверждает исследование, **подкрепляющее** данный отчет.
- Коэффициент детерминации (R-квадрат) равен 0,6. Это означает, что **60 % случаев заражения можно предсказать, исходя из доли нелицензионного ПО**.

За основу взяты данные по доле нелицензионного ПО за 2015 г. (BSA) и среднеквартальной частоте случаев заражения вредоносными программами (за II кв. 2015 г. и I кв. 2016 г.). Каждая точка соответствует стране.

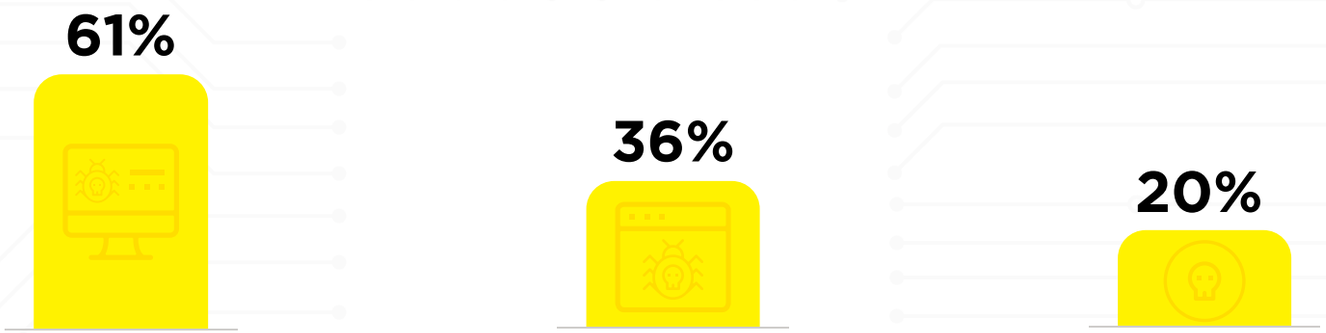
Ссылки:

Отчет Unlicensed Software and Cybersecurity Threats («Нелицензионное ПО и угрозы кибербезопасности»), BSA, январь 2015 г.
(http://globalstudy.bsa.org/2013/malware/study_malware_en.pdf)

China, Addicted to Bootleg Software, Reels from Ransomware Attack («Наводненный нелицензионным ПО Китай вздрогнул от атак программ-вымогателей»), *New York Times*, 15 мая 2017 г.
(https://www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html?_r=0

Причина сильной корреляции: доля заражения нелицензионных программ вредоносным кодом

Доля заражения по источникам нелицензионного ПО



ПО из ненадежных источников, предустановленное на компьютерах

Трояны и опасное рекламное ПО, загруженные с веб- и P2P-сайтов

Трояны в ПО на компакт- и DVD-дисках

» Вредоносный код может передаваться через сайты, распространяющие нелицензионное ПО, а также содержаться в скачанных программах либо в нелегальных программах-активаторах.

» К вредоносным программам относятся: опасное рекламное ПО, клавиатурные шпионы, программы для кражи паролей и учетных данных, а также бэкдоры для хакеров и программные средства для удаленного управления.

Основные данные: IDC, исследование заражений через веб- и P2P-сайты, предлагающие нелицензионные программы и ключи активации. Дополнительные данные: Национальный университет Сингапура, анализ ноутбуков с предустановленным нелицензионным ПО.

Ссылки:

Отчет The Link between Pirated Software and Cybersecurity Breaches («Связь между нелицензионным ПО и нарушениями кибербезопасности»), IDC, март 2014 г.
(http://download.softwareculicenta.ro/raport-idc-2014-03.pdf)

Отчет Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services («Черный рынок: процветающая торговля украденными данными, вредоносным ПО и сервисами для атак»), Symantec, ноябрь 2015 г.
(https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services)

Вероятность заражения через нелицензионное ПО в целом (независимо от его источника)

Вероятность заражения через нелицензионное ПО в Европе — 2017 г.

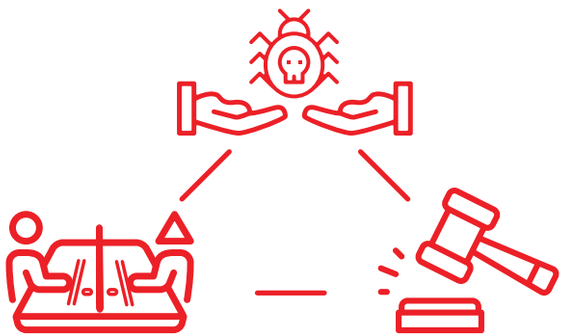
Нелицензионное ПО из всех источников: предустановленное, загруженное из Интернета (с веб- и P2P-сайтов) и установленное с носителей

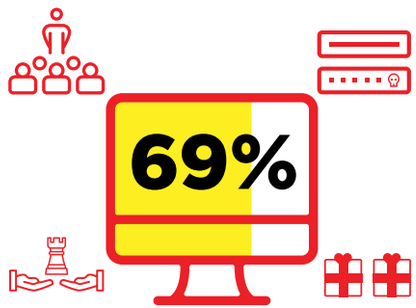
» Вероятность заражения примерно одинакова во всех исследуемых регионах и сегментах.

» Показатели вероятности заражения приведены в совокупности на основании исследования распространения ПО, проведенного компанией IDC.

Каждая третья нелицензионная копия компьютерного ПО становится причиной заражения вредоносным кодом!

Причина заражения № 1: ПО из ненадежных источников





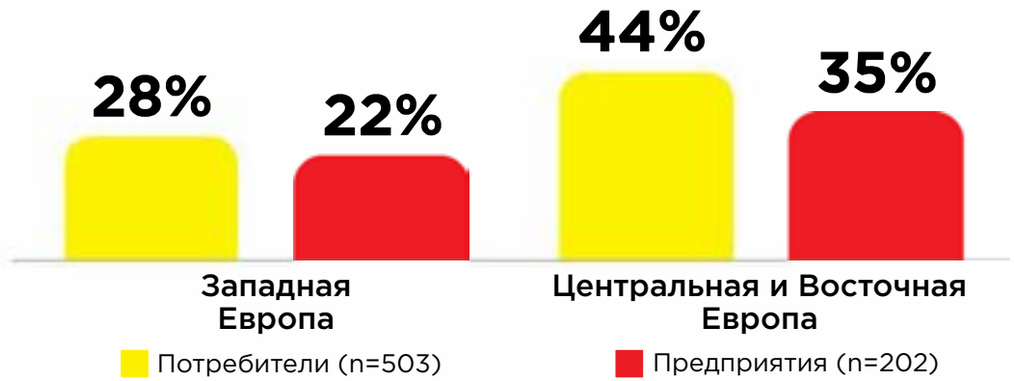
» У 66 % европейских потребителей возникали проблемы с ПО, которое они получили из ненадежных источников: например, загрузили с сайта онлайн-аукциона или интернет-поставщика, позаимствовали у друга, купили на уличном рынке и т. п.

» 69% домашних ПК в Европе за последние 2 года были получены из сомнительных источников: например, у консультантов, на сайтах онлайн-торговли, у небольших сборщиков или в качестве подарка.

» 33 % корпоративных компьютеров были получены из сомнительных источников.

Причина заражения № 2: небрежное отношение к обновлениям безопасности

Вероятность заражения вредоносным кодом из нелицензионного ПО в Европе — 2017 г.



» Небрежное отношение к обновлениям безопасности объясняется самыми разными причинами: от **опасений, что на компьютере будут обнаружены** нелицензионные программы, до отсутствия соответствующих процедур и инструментов контроля.

» Более 2/3 всех нарушений безопасности случаются, когда обновления, защищающие от них, уже доступны, но при этом еще не установлены.

Ссылки:

Статья The New Global Ransomware Attack Shows How Many People Still Don't Install Software Updates («Новая глобальная атака программ-вымогателей показала, что многие пользователи по-прежнему не устанавливают обновления ПО»), Business Insider, 28 июня 2017 г.

(http://www.businessinsider.com/people-still-dont-install-software-updates-2017-6).

Статья Seven Myths about Zero Day Exploits Debunked («Развенчание семи мифов об эксплойтах нулевого дня»), ZDNet, 3 августа 2010 г.

(http://www.zdnet.com/article/seven-myths-about-zero-day-vulnerabilities-debunked/)

Последствия небрежного отношения к обновлениям безопасности: атаки программ-вымогателей

Атаки программ-вымогателей и игнорирование обновлений безопасности (% респондентов, n=202)

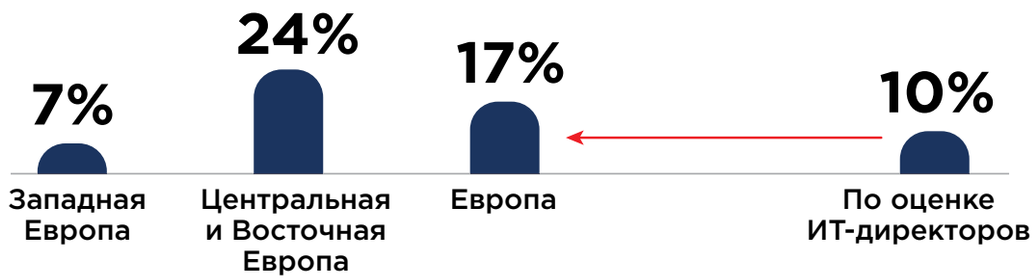
- Сильная корреляция (0,79) между атаками программ-вымогателей и игнорированием обновлений безопасности.
- Пользователи не устанавливают обновления по разным причинам, от нежелания тратить на это время и усилия до страха быть уличенными в использовании нелицензионного ПО.
- Коэффициент корреляции между проблемами с ПО и небрежным отношением к обновлениям безопасности еще выше (0,91).

Проблемы с ПО* и игнорирование обновлений безопасности (% респондентов, n=202)

* Приложения Office, предустановленные на ПК.

Троянский конь с вредоносными программами: когда сотрудники используют на рабочих компьютерах собственные программы

% сотрудников, установивших ПО на рабочих компьютерах без информирования своей компании за последние два года (n=369)



» ИТ-директора недооценивают число сотрудников, устанавливающих собственное ПО.

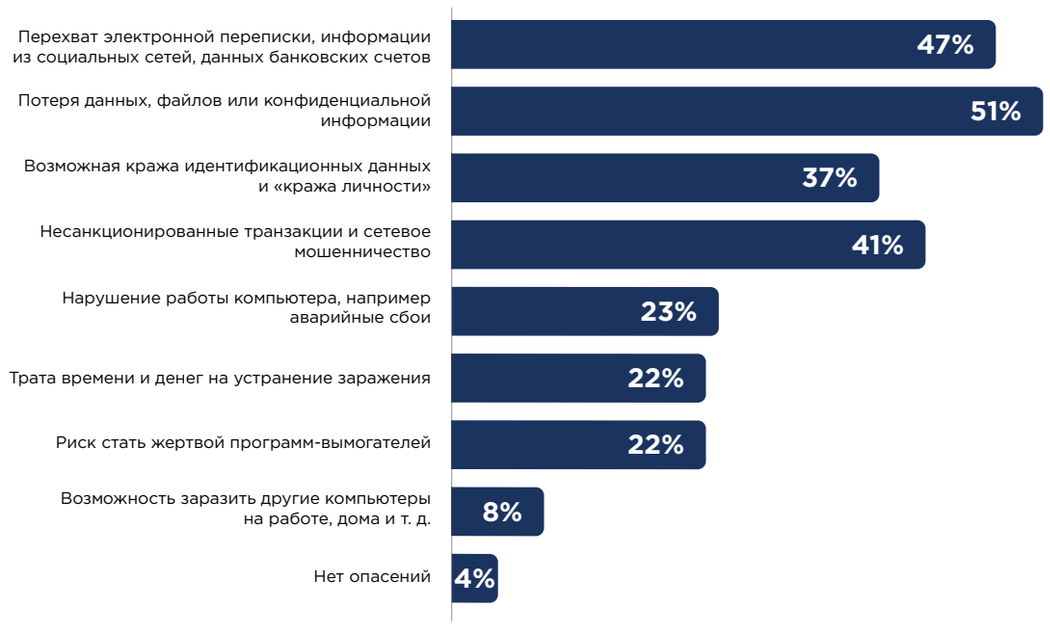
» В Европе около 50 % организаций проверяют ПО, установленное на компьютерах конечных пользователей, не чаще двух раз в год. Политики установки ПО конечными пользователями на рабочих компьютерах есть менее чем у половины компаний.

» Установка пользователями собственного ПО обходится дорого: 17 % сотрудников европейских компаний самостоятельно устанавливают на корпоративные компьютеры до 4 % ПО, которое в значительной степени является нелицензионным и не проверяется на наличие вредоносного кода. **Таким образом, использование сотрудниками собственных программ на 19 % увеличивает количество зараженного ПО на корпоративных компьютерах**.

Существование официальной процедуры для управления собственным ПО сотрудников на корпоративных компьютерах — важная часть защиты от вредоносного кода

Основные опасения европейских потребителей в отношении зараженного нелицензионного ПО

Самые серьезные опасения потребителей, связанные с зараженным нелицензионным ПО, % респондентов (n=503)

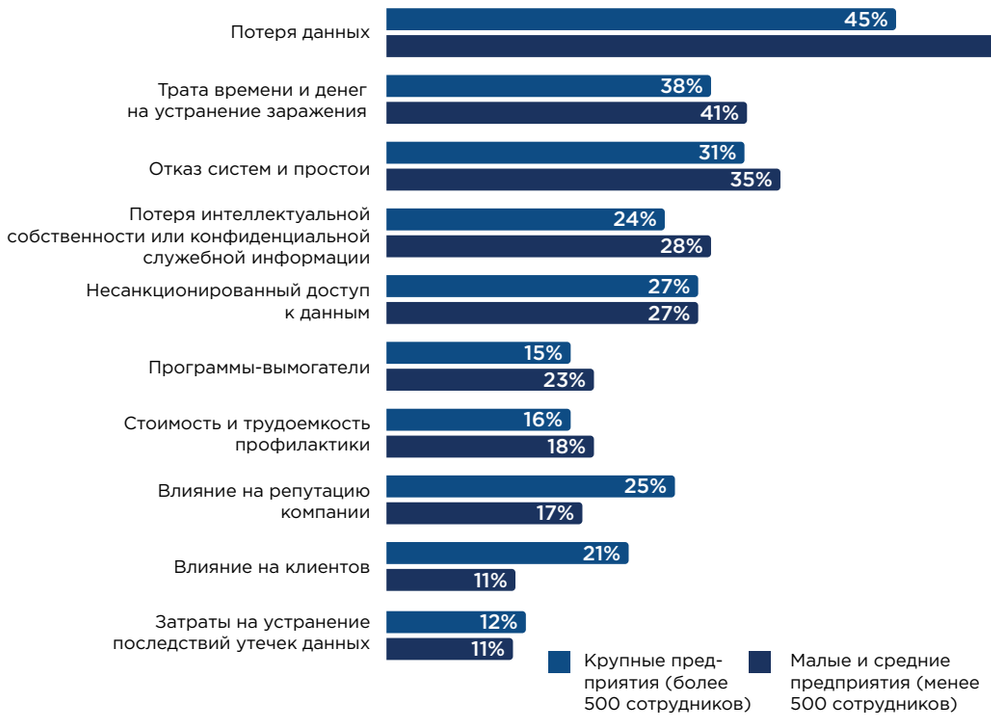


96 % потребителей обеспокоены заражением через недолицензированное или нелицензионное ПО

(Недолицензированное ПО — это легальное ПО, установленное на большем количестве компьютеров, чем это разрешено условиями лицензии)

Основные опасения европейских организаций в отношении зараженного нелицензионного ПО

Самые серьезные опасения европейских компаний, связанные с зараженным нелицензионным ПО, % респондентов (n=202)



- 16 % организаций сталкивались с утечкой данных (в среднем 3,7 случая утечки; средний объем утечки — 2900 записей).
- В Центральной и Восточной Европе утечки случались в 2,5 раза чаще, чем в Западной Европе, однако число записей, потерянных в результате каждой утечки, было в 5 раз больше в Западной Европе.
- 11 % организаций подвергались атакам программ-вымогателей. В среднем выкуп требовали 4,1 раза в год, средний размер запроса составил 1395 долларов США. Однако лишь в 18 % случаев компании платили мошенникам.
- Во многих случаях можно избежать уплаты выкупа, восстановив данные из резервной копии или расшифровав файлы с помощью специальных инструментов. Например, Майкрософт предлагает бесплатные средства, такие как Защитник Windows в Интернете, которые помогают в этом. Аналогичные программы есть и у других поставщиков.

Больше всего организации опасаются утечки данных и потери информации

Ущерб, нанесенный европейским потребителям вредоносным ПО: **7,2 млрд евро, 319 млн часов!**

Ущерб для европейских потребителей от вредоносного кода, содержащегося в нелицензионном компьютерном ПО (млрд евро), 2017 г.

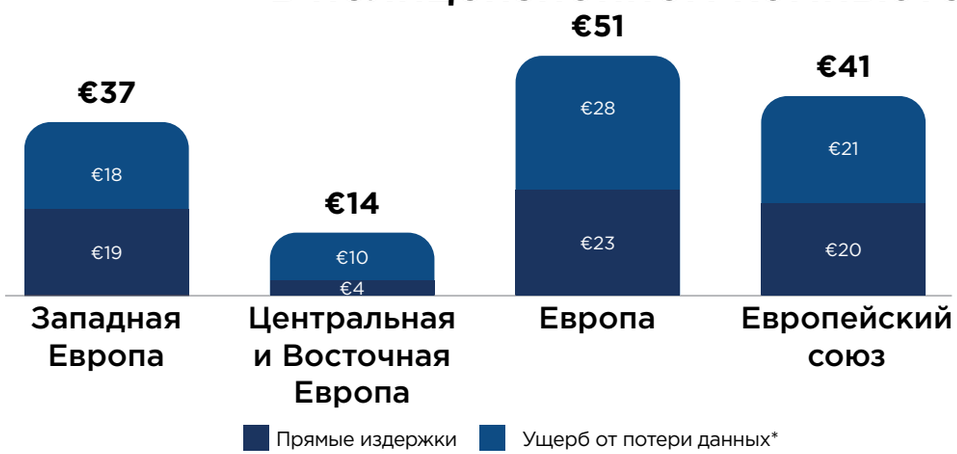
* Трудозатраты рассчитаны на основе средней заработной платы за 2017 г. для пользователя ПК.

- Затраты времени и денег связаны с идентификацией угрозы, восстановлением систем и данных, устранением последствий кражи идентификационных данных и атак программ-вымогателей.
- При оценке трудозатрат за основу взята средняя почасовая заработная плата в каждой стране (по обменному курсу 2016 г.).
- Общие расчетные затраты времени составляют 319 млн часов; потери соответствуют 10 часам (что эквивалентно 231 евро) на каждую зараженную единицу ПО.
- Данный анализ построен на средних значениях, но в каждом конкретном случае затраты могут существенно отличаться от средних. Например, согласно статистике по США, половина пострадавших от кражи личных данных справляется с сопутствующими проблемами меньше чем за день. Однако для 10 % из них эта работа занимает больше месяца.

Ущерб на каждую зараженную единицу ПО может во много раз превышать коммерческую стоимость легитимного ПО

Ущерб, нанесенный европейским организациям зараженным ПО: **51 млрд евро**

Ущерб для европейских потребителей от вредоносного кода, содержащегося в нелицензионном компьютерном ПО (млрд евро), 2017 г.



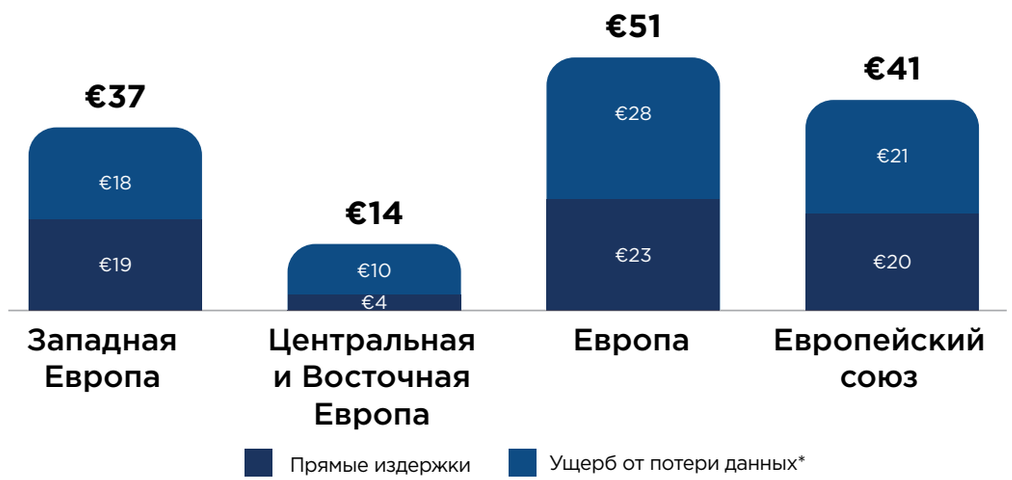
* Предполагается, что одна из тысячи зараженных программ и приложений становится причиной утечки данных.

- Организации тратят время и деньги (включая внешние и внутренние издержки) на идентификацию угрозы, восстановление систем и данных, а также устранение последствий атак программ-вымогателей.
- При оценке трудозатрат за основу взята средняя почасовая заработная плата ИТ-специалистов в каждой стране (по обменному курсу 2016 г.).
- Совокупный расчетный ущерб на каждую зараженную единицу ПО составляет 6220 евро. Сюда входят затраты на оплату труда ИТ-специалистов, внешние издержки, доля ИТ-бюджета, выделяемая на ИТ-безопасность, и последствия потери данных.
- При оценке ущерба от потери данных предполагалось, что причиной утечки данных становится одна из тысячи зараженных программ и приложений.
- Ущерб от утечки данных включает затраты на поиск и решение проблем, разъяснительную работу с клиентами, штрафы, расходы на юридические услуги и коммерческие потери. Сюда не относится ущерб, нанесенный программами-вымогателями, а также критические случаи утечки особо ценной информации (коммерческая тайна, интеллектуальная собственность и т. п.).

Ущерб на каждую зараженную программу или приложение может во много раз превышать коммерческую стоимость легитимного ПО

Малым и средним организациям зараженное ПО наносит наибольший ущерб

Ущерб для европейских организаций от вредоносного кода, содержащегося в нелицензионном компьютерном ПО (млрд евро) — 2017 г.



* Предполагается, что одна из тысячи зараженных программ и приложений становится причиной утечки данных.

- На небольшие и средние компании приходится менее 50 % всего ПО, развернутого во всех европейских организациях, но более 50 % всего нелицензионного ПО (за счет более высокой доли использования нелицензионного ПО).
- Из-за менее внимательного отношения к обновлениям безопасности на небольшие и средние компании приходится около 60 % всего зараженного нелицензионного ПО в европейских организациях.
- 60 % совокупного ущерба, нанесенного небольшим и средним компаниям, приходится на малый бизнес.

Чем меньше организация, тем выше риск экономического ущерба от заражения через нелицензионное ПО

Рекомендации от компании IDC

- Приобретайте компьютеры и ПО у надежных поставщиков.
- Остерегайтесь нелицензионного ПО — убедитесь, что установленные вами программы были получены легально.
- Устанавливайте надежные решения для обеспечения безопасности.
- Внимательно относитесь к обновлениям безопасности — не откладывайте их установку.
- Регулярно проверяйте ПО, установленное сотрудниками.
- Создавайте резервные копии файлов данных, по возможности в реальном времени.
- Не платите выкуп в случае атаки программ-вымогателей — преступникам доверять нельзя.