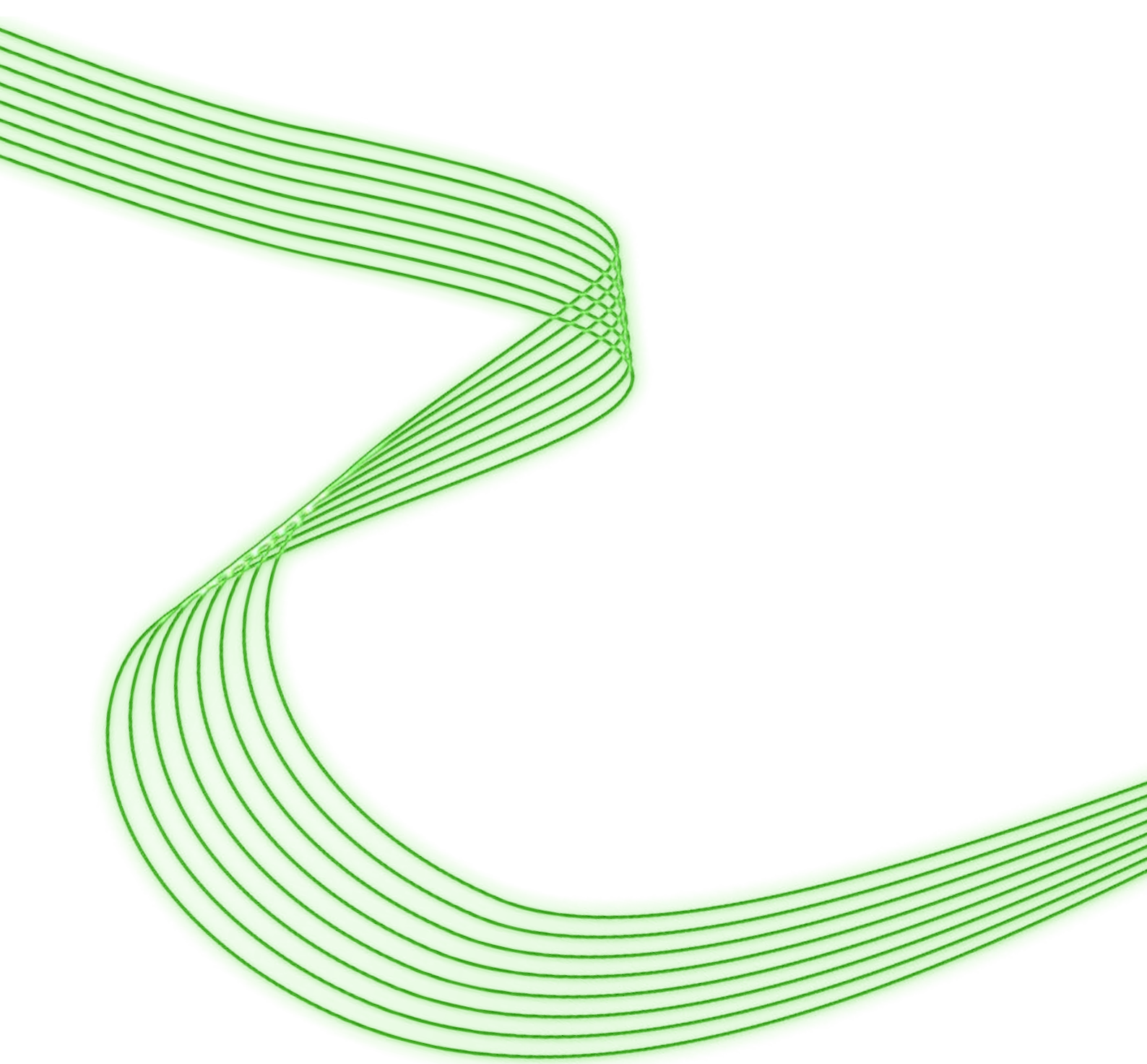


ПОЧЕМУ СЛОЖНОСТЬ – ЗЛЕЙШИЙ ВРАГ БЕЗОПАСНОСТИ

В этом документе анализируется то, как сложность IT-инфраструктуры может значительно повысить риски для безопасности, и как этого избежать.

Kaspersky Security для бизнеса.
Время серьезных решений

kaspersky.ru/business

KASPERSKY lab

Современные бизнес-риски

1.0

Во всем мире организации стремятся приумножить свои достижения за счет внедрения инновационных технологий. Но первичными целями были и остаются повышение производительности и конкурентоспособности бизнеса, а также сокращение издержек. Ключевая роль в обеспечении выполнения всех этих требований ложится на плечи IT-департамента.

Новые требования приводят к росту сложности IT-инфраструктуры и появлению дополнительных задач для IT-департамента. Из-за усложнения IT-среды легко пропустить уязвимость в системе, которая может привести к серьезным проблемам обеспечения безопасности. Это может быть, например, новое устройство в сети или приложение, для которого не установлено исправление. Организации осознают эту угрозу. Когда «Лаборатория Касперского» проанализировала мнения и опыт более 3300 старших IT-специалистов, собранные в 22 странах в рамках глобального опроса об IT-рисках за 2012 год, для нее не стал сюрпризом тот факт, что киберугрозы рассматриваются как второй по значимости бизнес-риск после экономической нестабильности (см. рис. 1).

Рис. 1. Самые серьезные на сегодняшний день бизнес-риски[1]

Основные области, в которых требуются дополнительные ресурсы и средства администрирования, – это управление мобильными устройствами, шифрование, контроль рабочих мест (например, контроль использования программ, устройств и веб-ресурсов), а также системное администрирование. При этом проблема установки исправлений, часто выполняемой вручную, заняла первое место в глобальном опросе об IT-рисках, проведенном в 2012 году «Лабораторией Касперского» (см. рис. 2).

[1] Источник: глобальный опрос об IT-рисках, проведенный в 2012 году «Лабораторией Касперского»

«Эффективное обеспечение безопасности IT-инфраструктуры – это всегда баланс между рисками, издержками и удобством. Но при этом вы можете правильно оценивать два последних фактора только тогда, когда имеете полное представление опервом. Я обеспокоен тем, что в настоящее время риски растут быстрее, чем организации осознают их, и это подтверждается результатами опроса.»
Вице-президент по продуктам и услугам для обеспечения безопасности компании IDC Крис Кристиансен (Chris Christiansen)[3]

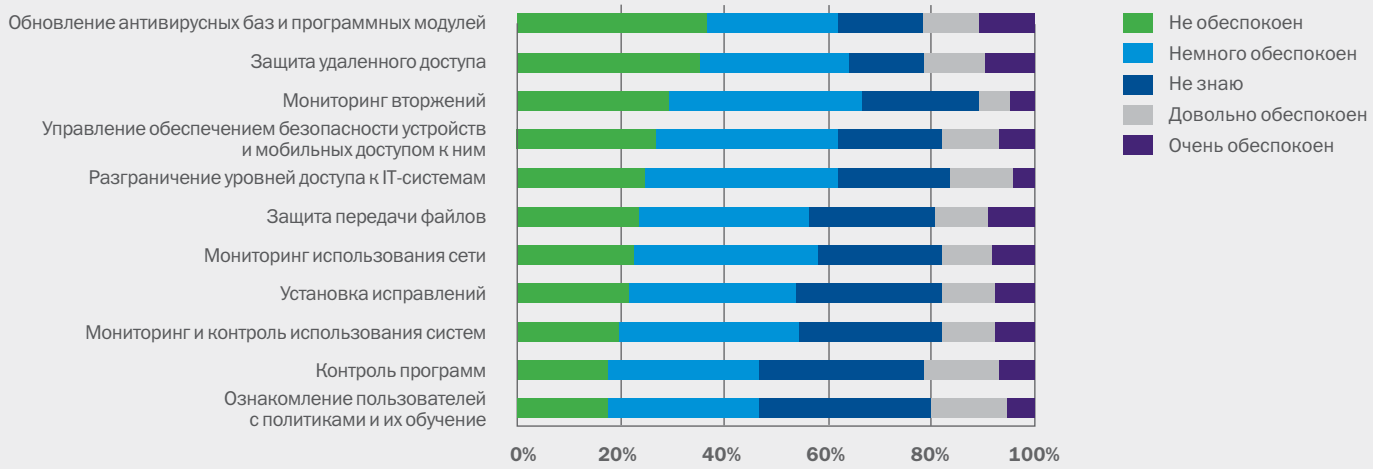
Имеющиеся решения для обеспечения безопасности IT-инфраструктуры могут усугублять проблемы, связанные со сложностью систем. Это происходит потому, что они обычно представляют собой узкоспециализированные решения для конкретных задач, таких как управление мобильными устройствами или шифрование. В лучшем случае такие решения «связаны», в худшем – никак не взаимодействуют между собой. Это означает, что IT-администраторам приходится переключаться между панелями управления, чтобы применить политики, проверить состояние безопасности рабочих мест и установить исправления для ОС и программ. В результате в системе безопасности легко возникают бреши.

Чтобы обеспечить надежность защиты, большая транснациональная организация может себе позволить инвестировать в мощные инструменты «корпоративного масштаба», для обслуживания которых будут выделены специализированные ресурсы. Но это совершенно не по силам большинству предприятий малого и среднего бизнеса, которые вынуждены решать подобные проблемы при значительно меньшей численности IT-отделов.

Организации находятся меж двух огней: с одной стороны, необходимо управлять большими объемами критически важных бизнес-данных и более сложными системами, а с другой стороны, нужно бороться с постоянно растущими внешними рисками.

Этот факт четко проявился в ходе глобального опроса об IT-рисках, проведенного в 2012 году «Лабораторией Касперского»[2]. Анализируя результаты исследования, Крис Кристиансен (Chris Christiansen), вице-президент по продуктам и услугам для обеспечения безопасности компании IDC, сказал: «Эффективное обеспечение безопасности IT-инфраструктуры – это всегда баланс между рисками, издержками и удобством. Но при этом вы можете оценивать два последних фактора только тогда, когда имеете полное представление о первом. Я обеспокоен тем, что в настоящее время риски растут быстрее, чем организации осознают их, и это подтверждается результатами опроса».

Рис. 2. Насколько вы обеспокоены следующими повседневными проблемами обеспечения безопасности IT-инфраструктуры в вашей организации?[2]



Организациям, которые знают, какие задачи нужно решать (и зачастую знают, как это делать), требуется новый подход, который бы выходил за существующие рамки и нормы и позволил ограниченным в ресурсах IT-отделам строить намного более обширные системы безопасности IT-инфраструктуры и управлять ими.

В этом документе рассматриваются реальные проблемы, с которыми сталкиваются организации, и возникающие из-за них угрозы IT-безопасности. В наше время уже недостаточно одного только антивирусного программного обеспечения, поэтому в документе делается попытка выяснить, какой новый подход к обеспечению безопасности IT-инфраструктуры требуется для эффективного реагирования на изменяющиеся угрозы и новые способы работы.

[2] Источник: глобальный опрос об IT-рисках, проведенный в 2012 году «Лабораторией Касперского»
[3] Источник: отчет «Лаборатории Касперского» Global IT Risk Report, 2012 год

Движущие силы бизнеса: что вызывает проблемы?

2.0

Необходимость нового подхода к обеспечению безопасности IT-инфраструктуры является следствием изменений, диктуемых организациями своим IT-департаментам. Причиной некоторых изменений являются технологические требования. Однако абсолютно все изменения вызваны фундаментальными мотивами снижения издержек и повышения гибкости и продуктивности.

2.1. Технологии
Сегодня технологии влияют на развитие бизнеса как никогда раньше. Это приводит к появлению все большего числа систем и платформ, от которых зависит эффективность работы. Предприятия всех размеров быстрыми темпами внедряют технологии во множестве различных областей. Чтобы ускорить принятие решений и сократить затраты времени и денег на командировки, повсеместно внедряются средства совместной работы. С этой же целью организации снабжают своих сотрудников различными мобильными устройствами.

Все это увеличивает объем используемых данных и порождает новое поколение рабочих мест и потенциальных лазеек для киберпреступников.

2.2. Недостаточно подготовки и ресурсов?
Груз управления всем этим ложится на IT-подразделения, у которых есть и другая, намного более важная и сложная работа. Причем их ресурсы нередко остаются такими же ограниченными.

Руководители IT-департаментов и администраторы должны делать все и сразу. Им необходимо выполнять несколько задач одновременно, а также быстро осваивать новые технологии. Утром они могут перезагружать серверы, в обед – настраивать правила сетевого экрана и списки контроля доступа. После обеда им может понадобиться разобраться с параметрами мобильного устройства, чтобы директор мог пользоваться почтой и иметь доступ в сеть со своего смартфона или планшетного ПК. А в конце рабочего дня они будут пытаться разрешить конфликты преобразования сетевых адресов на маршрутизаторах.

Это все может показаться обычной работой, но проблемы возникают, когда мы имеем дело с новыми технологиями и требованиями, которых просто не существовало несколько лет назад.

2.3. Изменение алгоритмов работы
В наши дни сотрудники привыкли иметь в своем распоряжении удобные и функциональные инструменты и технологии. Новое поколение пользователей с легкостью переходит на использование новых средств совместной работы, программ и устройств в бизнес-среде. Пользователи хотят получать доступ к веб-службам в любом месте и иметь под рукой нужные программы, сведения и ресурсы, зачастую без поддержки со стороны IT-отдела или, что более важно, без контроля за тем, как и с чем они работают. Побочным эффектом такого подхода, так называемой консьюмеризации, стала необычайная потребность в гибкости бизнеса, которую невозможно удовлетворить с помощью традиционных способов работы с корпоративной IT-инфраструктурой.

Вместо того чтобы ограничивать использование личных устройств в работе, следует направить усилия на поиск способа управлять ими.

2.4. Мобильность

В III квартале 2012 года компания IDC сообщила, что по всему миру было продано 444,5 миллиона смартфонов, что на 2,4% больше по сравнению с аналогичным периодом прошлого года[4]. Многие из этих устройств будут использоваться для работы конечными пользователями, которым нужна мобильность как средство совмещения профессиональной и личной деятельности.

В марте 2012 года «Лаборатория Касперского» в сотрудничестве с аналитической компанией Bathwick Group провела глобальное исследование на тему «Готовность систем для обеспечения безопасности в изменяющейся среде технологий» (см. рис. 3). Исследование показало, что в настоящее время мобильность имеет первостепенное значение для IT-специалистов по всему миру. Рост количества сотрудников (зачастую это руководители), использующих личные устройства для работы, которые обеспечивают доступ в сеть компании и работу с корпоративной информацией, означает, что IT-специалисты проигрывают битву за контроль.

Рис. 3. Какие проблемы вызывают у вас наибольшую озабоченность с точки зрения безопасности вашей организации?[5]

Вместо того чтобы ограничивать использование личных устройств в работе, следует направить усилия на поиск способа управления ими. Это непростая задача, учитывая, что используется огромное количество различных устройств, операционных систем и мобильных приложений. При этом невозможно контролировать пользователей, когда они просто подключают свои устройства к сети (с помощью проводного или беспроводного соединения) и получают доступ к нужным сведениям. Еще выше сложность, еще сложнее управлять инфраструктурой.

Сочетание изменений IT-инфраструктуры, новых алгоритмов работы и потребностей бизнеса серьезно затрудняет достижение баланса ресурсов, издержек и безопасности.

[4] В 2011 году ожидаемый рост мирового рынка смартфонов составил 55%, к 2015 году объем отгрузок приблизится к 1 млрд. По данным компании IDC от 9 июня 2011 г., http://www.idc.com/getdoc.jsp?containerId=prUS22871611

[5] Источник: компания Bathwick Group, «Готовность систем обеспечения для безопасности в изменяющейся среде технологий», март 2012 года

Современные угрозы: эра усложнения

3.0

- База знаний «Лаборатории Касперского» содержит более 67 миллионов уникальных угроз[6].
- Каждый день появляется 125 000 новых угроз[6].
- Каждый день появляется 140 новых вредоносных программ для мобильных устройств[6].
- 91% организаций подверглись по крайней мере одной атаке за последние 12 месяцев[7].

Эволюцию киберугроз за последние несколько лет можно описать двумя словами: количество и изощренность. Это подтверждается результатами глобального опроса об IT-рисках, проведенного «Лабораторией Касперского» в 2012 году, который показал, что 91% организаций хотя бы однажды подверглись атаке за последние 12 месяцев.

Уровень сложности и изощренности вредоносного программного обеспечения вырос настолько, что многие считают, что «традиционных» средств борьбы с вредоносными программами больше недостаточно. Среди нашумевших угроз такие вредоносные программы, как Stuxnet и Flame. Они попали в заголовки газет не только благодаря ущербу, который они нанесли, но и тому, что они очень долго оставались необнаруженными. Вирус Flame, например, существовал многие годы, но был формально идентифицирован только в мае 2012 года.

3.1. Новое поколение сложных угроз

Эти примеры указывают на то, что теперь уровень киберпреступников повысился: вирусы стали более изощренными и используют уязвимости с явной целью кражи ценных данных.

Банковские счета предприятий – это основная цель для преступников, поскольку на них сосредоточены большие денежные средства. При этом владельцы счетов часто не принимают адекватных мер для обеспечения безопасности. Это объясняет рост количества троянцев и таких вредоносных программ, как Zeus, которые крадут информацию и позволяют хакерам получать доступ к корпоративным финансам.

Эта тенденция подтверждается увеличением количества комплексных таргетированных угроз (Advanced Persistent Threats, APT). Правительства и транснациональные корпорации теперь не единственные мишени для атак вредоносных программ высокой сложности. Малый бизнес тоже подвергается риску. Более того, чем чаще такие угрозы используются киберпреступниками, тем выше риск сопутствующего ущерба. На линии огня могут оказаться организации, которые даже не являются целью атак.

3.2. Охват инфраструктуры

Уровень сложности и решительности угроз приводят требования к обеспечению IT-безопасности организации к совершенно новой парадигме. Многие современные атаки начинаются с использования уязвимостей в широко используемых программах. В прошлом сама операционная система Windows была главной целью злоумышленников, ищущих уязвимости, которые могут быть использованы для установки вредоносного кода на компьютер. Но в последние годы регулярный выпуск компанией Microsoft обновлений системы безопасности вынудил киберпреступников перевести свое внимание на приложения, не входящие в состав Windows. Теперь Windows даже не находится в списке 10 наиболее уязвимых программных пакетов (см. рис. 4 и 5). К сожалению, многие программы не получают исправлений в течение длительного времени.

[6] Источник: «Лаборатория Касперского»
[7] Источник: глобальный опрос об IT-рисках, проведенный в 2012 году «Лабораторией Касперского»

Согласно сведениям, приведенным на сайте securelist.ru, более 80% всех атак, использующих уязвимости, нацелены на Java и Adobe Acrobat Reader[8]. Помимо того, что пакет Java установлен на огромном числе компьютеров (согласно данным компании Oracle, это 1,1 млрд. компьютеров), обновления выполняются не автоматически, а по требованию пользователя. Что касается Adobe Acrobat Reader, то функция автоматического обновления есть только в последних версиях. Пользователи привыкли самостоятельно устанавливать программы на свои компьютеры и мобильные устройства, и со временем на них накапливаются десятки управляемых и неуправляемых программ, при этом любая из них может иметь некоторое количество потенциальных уязвимостей.

Растущее разнообразие устройств и операционных систем, с помощью которых предприятия обрабатывают данные, только усугубляет угрозу безопасности: чем больше количество устройств и программ, которыми надо управлять, тем больше брешей необходимо закрывать.

На этих платформах также появилось множество уязвимостей, а регистрация и исправление их всех почти невозможны при растущем количестве операционных систем и десятках тысяч программ, написанных для них. Эту тенденцию отражает разнообразие программ и операционных систем, имеющих уязвимости (см. рис. 4 и 5).

Рис. 4. Приложения, наиболее часто используемые для атак[8]

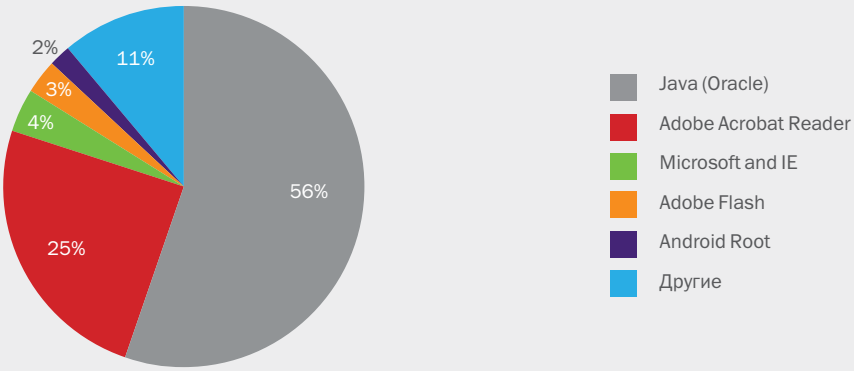


Рис. 5. Список 10 самых используемых уязвимостей программного обеспечения за I квартал 2012 года[9]

№	Приложение, содержащее уязвимости	Процент пользователей, подвергающихся риску (%)	Оценка
1	Oracle Java (многочисленные уязвимости)	35	Очень опасно
2	Oracle Java (три уязвимости)	21,7	Чрезвычайно опасно
3	Adobe Flash Player (многочисленные уязвимости)	19	Очень опасно
4	Adobe Flash Player (многочисленные уязвимости)	18,8	Очень опасно
5	Adobe Reader и Acrobat (многочисленные уязвимости)	14,7	Чрезвычайно опасно
6	Apple Quick Time (многочисленные уязвимости)	13,8	Очень опасно
7	Apple iTunes (многочисленные уязвимости)	11,7	Очень опасно
8	Winamp, обработка файлов AVI и IT	10,9	Очень опасно
9	Adobe Shockwave Player (многочисленные уязвимости)	10,8	Очень опасно
10	Adobe Flash Player (многочисленные уязвимости)	9,7	Чрезвычайно опасно

[8] Источник: https://www.securelist.com/ru/analysis/208050773/Razvitie_informatsionnykh_ugroz_v_tretem_kvartale_2012_goda#4
[9] Источник: https://www.securelist.com/ru/analysis/208050773/Razvitie_informatsionnykh_ugroz_v_tretem_kvartale_2012_goda#14

Современные угрозы: эра усложнения

Предотвращение утечек: все более широкое использование инструментов шифрования

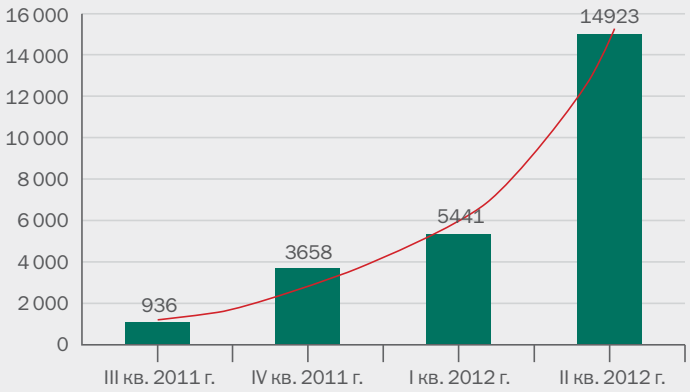
- У 15% организаций происходили утечки данных в результате кражи мобильных устройств.[11]
- Вредоносное программное обеспечение и спам остаются самыми главными причинами утечек данных.[11]
- Шифрование данных стоит на втором месте в списке областей, нуждающихся, по мнению большинства организаций, в улучшении.[11]

3.3. Мобильные устройства

Мобильные устройства добавляют рискам еще одно измерение. Сегодня операционные системы iOS и OS X компании Apple и различные варианты операционной системы Android компании Google распространены так же широко, как и Windows. Киберпреступники ушли далеко вперед в использовании для своих целей рисков, создаваемых мобильными устройствами. Во II квартале 2012 года количество троянских программ, нацеленных на платформу Android, выросло почти в три раза по сравнению с I кварталом 2012 года (см. рис. 6).

Рис. 6. Количество модификаций вредоносных программ, предназначенных для ОС Android[10]

«Лаборатория Касперского»



Эта угроза будет расти, поскольку легкость, с которой можно получить или перехватить данные, используемые деловыми людьми на мобильных устройствах, делает мобильные устройства новой мишенью для киберпреступников.

Глобальный опрос об IT-рисках, проведенный в 2012 году «Лабораторией Касперского», выявил тенденцию использования личных устройств для работы и показал, что все больше организаций разрешают владельцам устройств получать доступ к корпоративным данным и сетям без каких-либо дополнительных мер по обеспечению безопасности. Этот удивительно либеральный подход объясняется рядом факторов, в основном ростом количества таких устройств, а также тем, что используется просто слишком много различных типов устройств и версий операционных систем, которыми IT-подразделения проблематично управлять в условиях дефицита ресурсов.

Беспроводные технологии, облачные сервисы и программы синхронизации файлов сильно повышают соблазн кражи таких устройств.Воры и хакеры, получив доступ к украденным мобильным устройствам, будут использовать их для хищения ценных данных или проникновения в корпоративные сети. Ежегодный прямой денежный ущерб от утери или кражи мобильных устройств оценивается в 7 миллионов долларов США[12]. Косвенный ущерб от связанных с этим хакерских атак неизвестен.

3.4. Социальные сети: ограничений все меньше, а рисков все больше

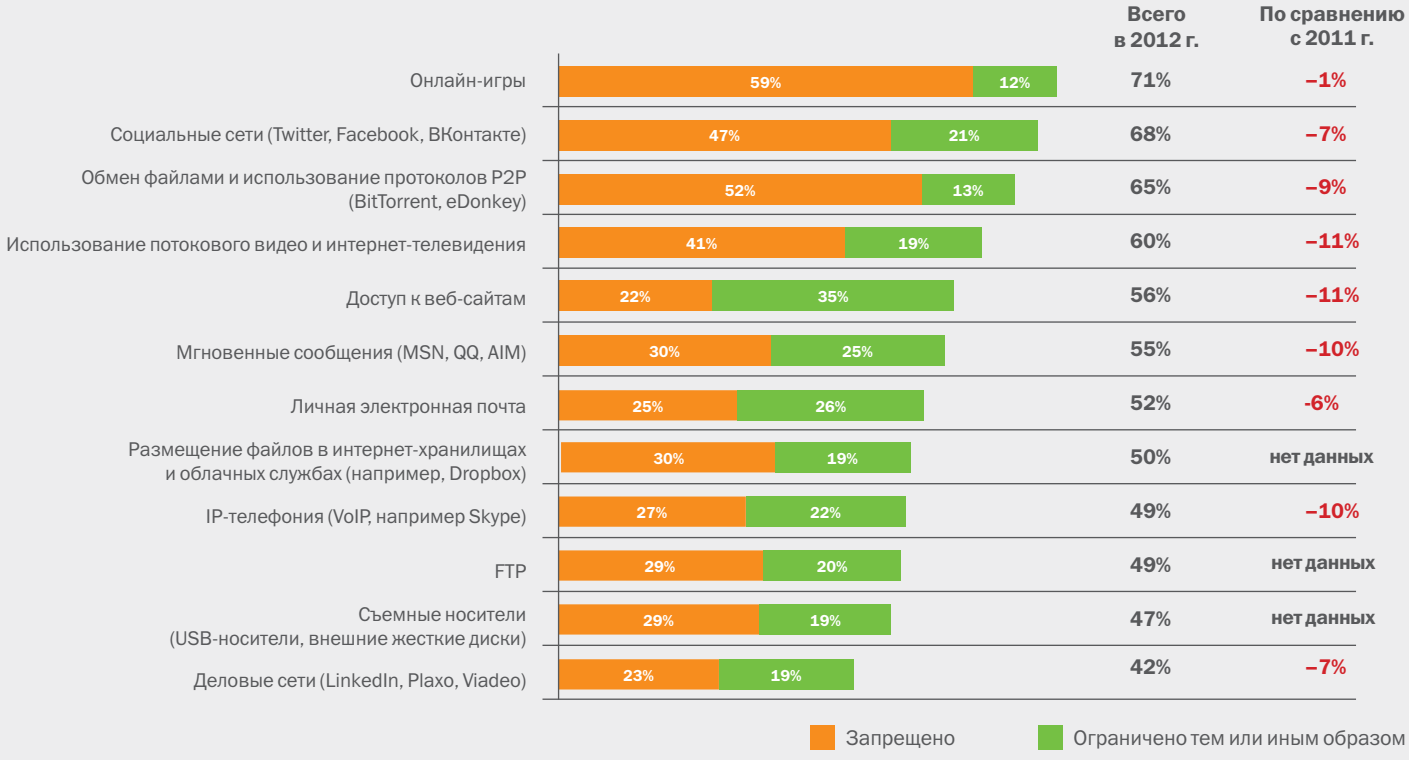
IT-администраторы справедливо отмечают, что наибольшие риски для безопасности исходят не от используемых инструментов и технологий, а от людей. Повсеместное использование социальных сетей и интернета, а также желание сотрудников быть всегда «на связи» все больше и больше затрудняют IT-подразделениям управление рисками нарушения безопасности.

[10] Источник: отчет securelist.ru за II квартал 2012 года: https://www.securelist.com/ru/analysis/208050763/Razvitie_informatsionnykh_ugroz_vo_vtorom_kvartale_2012_goda
[11] Источник: отчет «Лаборатории Касперского Global IT Risk Report, 2012 год
[12] Источник: https://www.lookout.com/resources/reports/mobile-lost-and-found/billion-dollar-phone-bill

Самая актуальная тема – это социальные сети. Они рассматриваются как одна из самых больших угроз IT-безопасности и остаются на втором месте в списке областей, подвергаемых наиболее тщательному контролю. Пользование социальными сетями полностью запрещено в половине организаций (см. рис. 7). Но ограничений по использованию социальных сетей и интернета становится все меньше. Причем трудно определить, с чем это связано: с тем, что IT-подразделения «проигрывают войну», или с тем, что бизнес-преимущества от использования социальных сетей и интернета слишком велики.

Дэвид Эмм (David Emm), старший региональный исследователь «Лаборатории Касперского», отметил: «Попытки тотального запрета на использование социальных сетей похожи на борьбу с приливом; гораздо лучше научиться управлять им».[14]

Рис. 7. Виды деятельности, запрещенные или ограниченные на рабочем месте[13]



Тревожный вывод состоит в том, что в организациях этот вопрос не проработан. В будущем управление использованием социальных сетей и предотвращение бесконтрольного доступа в интернет могут стать основными признаками хорошо защищенной организации. При этом социальные сети опасны не столько сами по себе, сколько тем, что пользователи переходят по рекламным ссылкам и участвуют в опросах, предлагаемых в социальных сетях. Еще более опасен общий настрой «делиться информацией», который, судя по всему, значительно вырос. FTP-сайты и файлообменные сервисы несут в себе множество серьезных рисков для IT-безопасности, однако воспринимаются многими как безопасные.

IT-подразделениям необходимо осознать серьезность новых опасностей и то, что они представляют наивысшую степень угрозы для конечных пользователей. Только тогда организации любых размеров смогут сделать объективную переоценку своего состояния безопасности и подхода к ней.

[13] Источник: глобальный опрос об IT-рисках, проведенный в 2012 году «Лабораторией Касперского»
[14] Источник: отчет «Лаборатории Касперского» Global IT Risk Report, 2012 год

Упрощаем задачу: единая платформа

4.0

Много аспектов безопасности, много решений: защита бизнеса – это комплексная задача

- 44% организаций в настоящее время защищают данные с помощью шифрования
- 33% организаций разрешают «бесконтрольный» доступ к своим сетям со смартфонов[15]

4.1. Почему производители средств для обеспечения IT-безопасности только затрудняют решение проблемы

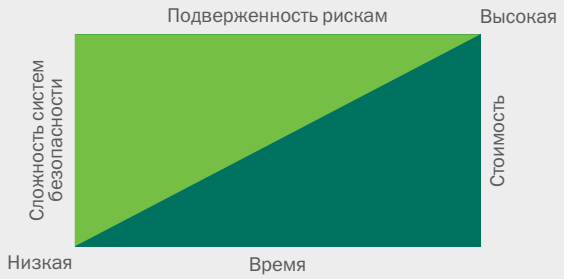
Производители средств для обеспечения IT-безопасности пока не облегчают жизнь организациям. Распространение различных технологий до недавнего времени вело к созданию узкоспециализированных решений. Само по себе это обычное явление и является признаком роста рынка и развития технологий. В организациях, где нет выделенных служб IT-безопасности, многопрофильные IT-департаменты могут с трудом ориентироваться в предложениях, доступных на рынке. Поиск, оценка и приобретение действительно нужных продуктов – действительно сложная задача.

Зачастую организации используют широко распространенные средства борьбы с вредоносным программным обеспечением для базовой защиты рабочих мест. Некоторые организации добавляют к этим решениям функции шифрования электронной почты и систем совместного доступа к файлам. Если сотрудники организации используют мобильные устройства, то она может приобрести решение для управления мобильными устройствами, чтобы контролировать корпоративные и личные устройства. Наконец, организации иногда применяют какой-либо подход к управлению установкой исправлений, чтобы отслеживать и устанавливать исправления в своей операционной среде и, таким образом, не допускать появления брешей в системе безопасности из-за программных уязвимостей.

Несмотря на произведенные вложения, перед предприятиями возникает еще более серьезная проблема. Различные системы обеспечения безопасности попросту не взаимодействуют друг с другом. Каждый раз, когда системный администратор формирует отчет, производит настройку параметров, реагирует на оповещения или выполняет обновление программного обеспечения, ему приходится работать с различными консолями управления для отдельных решений. Это требует больших затрат времени (см. рис. 8) и снижает эффективность обеспечения безопасности.

Например, вы используете пять различных средств защиты, при этом у вас уходит по пять минут на каждое из них для настройки одной задачи, чтобы скоординировать действия в нескольких программах, таким образом на внедрение этой задачи вам потребуется 25 минут. Прибавьте к этому усилия, необходимые для того, чтобы убедиться, что все изменения внесены правильно, поскольку у каждой программы свои механизмы формирования отчетов. В результате системный администратор тратит часы, открывая все программы, просматривая многочисленные отчеты, чтобы выполнить задачу, которая должна быть относительно автоматизированной.

Рис. 8. Сложность – это враг эффективности при обеспечении безопасности. Чем выше сложность средств для обеспечения безопасности и чем больше времени требуется для их настройки, тем выше издержки на обеспечение безопасности и ниже окупаемость инвестиций в такие системы[16]



[15] Источник: глобальный опрос об IT-рисках, проведенный в 2012 году «Лабораторией Касперского»
[16] Источник: компания 2112 Group, «Сложность – враг безопасности», октябрь 2012 г.

«Наряду с недостаточностью знаний и подготовки персонала, во многих организациях также явно ощущаются недостатки на уровне управления, когда различные решения и политики по обеспечению безопасности применяются к различным группам пользователей и устройств. Каждый из этих недостатков – потенциальная уязвимость. Организациям требуется единый подход и комплексные решения для контроля.»

Крис Кристиансен (Chris Christiansen), вице-президент по продуктам и услугам для обеспечения безопасности компании IDC[17]

Хотя термин «интеграция» и употребляется в IT-отрасли довольно часто, она крайне важна для повышения уровня безопасности. Когда ресурсы ограничены, невозможно управлять множеством систем, отслеживать многочисленные события и вовремя предпринимать корректирующие действия.

Скорость обнаружения угрозы и реакции на нее чрезвычайно важна при обеспечении IT-безопасности. Чем дольше не производится установка исправлений, тем дольше IT-инфраструктура находится в состоянии уязвимости.

Это еще более справедливо для сложных современных IT-сред, в состав которых входят мобильные устройства, виртуальные машины и личные устройства сотрудников. Возможность быстро и просто настраивать задачи и политики – важный компонент эффективного подхода.

Причина, по которой интеграция представляет такую проблему в этом контексте, состоит в том, что многие «консолидированные» подходы созданы путем простого объединения узкоспециализированных решений.

Само по себе это не проблема, технологии определенно будут «работать» вместе, но это будет весьма неэффективная работа. И самое важное – на обслуживание такой системы безопасности будет уходить больше времени: требуется много усилий для того, чтобы разбираться в различных программах и обеспечивать правильность и согласованность применения политик в рамках всех используемых технологий.

Время – это ценность, и его не хватает IT-подразделениям, которые и без того испытывают недостаток ресурсов. Необходим единый подход к выполнению множества задач в различных средах.

[17] Источник: отчет «Лаборатории Касперского» Global IT Risk Report, 2012 год

Как вы можете защитить то, чего вы не видите? Простое управление обеспечивает прозрачность системы безопасности

5.0

5.1. Проблемы издержек и ресурсов
По мере того как предприятия внедряют все больше разнородных технологий, мобильных устройств и средств совместной работы и все больше зависят от управления данными в деле повышения производительности и обеспечения непрерывности бизнес-процессов, главной задачей становится повышение уровня безопасности и снижение рисков, исходящих от действий хакеров и вредоносного программного обеспечения. К сожалению, это неизбежно приводит к тому, что потребности в обеспечении безопасности вступают в противоречие с имеющимися ресурсами. Растущие издержки на IT-подразделения не обязательно влекут за собой увеличение штата и повышение квалификации специалистов.

Поставщики средств обеспечения IT-безопасности стремятся создавать и продвигать на рынке программы и инструменты, которые характеризуются большей функциональной совместимостью и поддерживают интеграцию. В настоящее время крупные предприятия добиваются этого с помощью систем, создаваемых на заказ, которые объединяют и стандартизируют процессы формирования отчетов. Но такой подход требует значительных издержек и наличия специалистов, которые будут заниматься обслуживанием таких систем, что очень редко по силам большинству предприятий малого бизнеса.

5.2. Ломая стереотип: отслеживайте, контролируйте и защищайте все ваши рабочие места с помощью единого средства
Новый подход должен начинаться с единой платформы, с единой консоли управления. Она дает общую картину, которая необходима IT-администраторам для принятия взвешенных решений по защите бизнеса и данных.

Прозрачность обеспечивает контроль, а контроль усиливает защиту.

Если речь не идет о крупном предприятии, используемые решения не должны требовать значительных административных ресурсов и интеграции систем. Такие решения должны управляться сотрудниками, не являющимися специалистами по обеспечению IT-безопасности. Но они должны предоставлять удобный способ отслеживания, контроля и защиты всех рабочих мест, на которых используются корпоративные данные, будь то настольные компьютеры, виртуальные машины, планшетные ПК, смартфоны, а также личные устройства сотрудников.

Сердцем такой системы должна быть единая консоль управления. В этом случае можно получать доступ к средствам обеспечения безопасности и управлять ими из единой панели мониторинга, обеспечивающей единообразие конфигурирования, применения и контроля политик и параметров безопасности в рамках всей организации.

Заключение

6.0

Kaspersky Security для бизнеса предоставляет следующие возможности:

- защита от вредоносного программного обеспечения
- шифрование данных
- управление мобильными устройствами и их защита
- контроль использования программ, устройств и веб-ресурсов
- системное администрирование, включая управление установкой исправлений

«Лаборатория Касперского» понимает, что для большинства организаций обеспечение безопасности компьютеров и устройств, а также управление ими стало трудной, непосильной задачей. Совершенно ясно, что справиться со сложностью можно только с помощью единого, комплексного подхода к обеспечению IT-безопасности. Проблемы, рассмотренные в этом документе, побудили «Лабораторию Касперского» к разработке нового подхода, воплощенного в продуктовой линейке Kaspersky Security для бизнеса.

Kaspersky Security для бизнеса принципиально отличается от остальных продуктов, доступных сегодня на рынке, поскольку он был создан «с нуля» на единой технологической базе. Другими словами, это единая платформа для обеспечения IT-безопасности, а не множество соединенных вместе программ.

В результате этот продукт значительно упрощает поддержку общего уровня безопасности, поскольку политика создается один раз, а затем одним нажатием кнопки распространяется на множество конечных узлов сети различных типов.

Kaspersky Security для бизнеса – это всеобъемлющая, полностью интегрированная платформа, которая обеспечивает надежную защиту от вредоносного программного обеспечения, надежный контроль программ, системное администрирование, шифрование данных и управление мобильными устройствами. Все это доступно из единой консоли. Kaspersky Security для бизнеса защищает ваши данные, управляет вашими программами и дает вам возможность отслеживать, контролировать и защищать все устройства – физические, виртуальные или мобильные, корпоративные или личные.

Это означает, что организации наконец могут достичь высокого уровня безопасности сложной и постоянно меняющейся IT-среды с меньшими требованиями к IT-специалистами и минимальными затратами на их обучение. Технологии, которые раньше считались сложными, дорогими и трудноуправляемыми, сейчас стали реальностью для всех организаций независимо от их размера и ресурсов.

Контроль и защита в любых обстоятельствах.
Kaspersky Security для бизнеса. Время серьезных решений.

О «Лаборатории Касперского»
«Лаборатория Касперского» – крупнейшая в мире частная компания, специализирующаяся в области разработки программных решений для обеспечения IT-безопасности. Компания входит в четверку ведущих мировых производителей защитных систем класса Endpoint Security. Вот уже более пятнадцати лет «Лаборатория Касперского» предлагает эффективные защитные решения для домашних пользователей, предприятий малого и среднего бизнеса и крупных корпораций. Ключевым фактором успеха компании является инновационный подход к обеспечению информационной безопасности. Технологии и решения «Лаборатории Касперского» защищают более 300 миллионов пользователей почти в 200 странах и территориях мира.

Узнать больше о Kaspersky Security для бизнеса: www.kaspersky.ru/business