

Windows IT Pro/RE

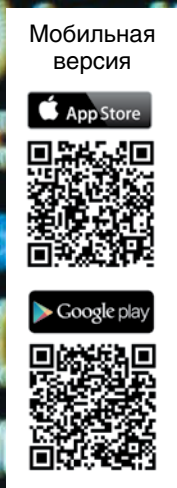
№5 МАЙ 2016

WWW.WINDOWSITPRO.RU

ИНФО ДЛЯ ИТ-ПРО

PowerShell

В ВОПРОСАХ И ОТВЕТАХ



Работа с адресами IPv4
в среде PowerShell

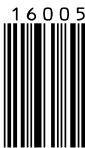
Проверка подлинности запросов
веб-служб с помощью PowerShell

Вопросы о PowerShell

Учим PowerShell
нажимать на кнопки

ISSN 1563-101X

16005



9 771563 101008

Издание для специалистов, интересующихся технологиями компании Microsoft.

Главный редактор: Д. Торопов (toropovd@osp.ru)
 Ответственный редактор: Е. Петровичева
 Корректор: Л. Теремко
 Верстка и дизайн: О. Шуранова
 Номер также готовили: Е. Овсянников
 Т. Евдокимова, А. Китаев, А. Федотов,
 Н. Басалова, Ю. Власов, Д. Щепкин, А. Адзиев

Адрес для писем: 127254, Москва, а/я 42
 Телефон: (495) 725-4780/83, (499) 703-1854
 Факс: (495) 725-4783
 E-mail: windowsitpro@osp.ru

Реклама: ООО «Рекламное агентство
 'Чемпионс', тел.: (495) 725-4780,
 Е. Амелехина (kam@osp.ru)

© 1999-2016 Издательство «Открытые системы»
 © 1999-2016 Penton Media, Inc.

Свидетельство о регистрации средства массовой информации ПИ №ФС77-63737 от 16 ноября 2015г.

Выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзором).

Цена свободная. Выходит 12 раз в год.



Учредитель и издатель:
 ООО «Издательство «Открытые системы»
 127254, Москва, пр-д Добролюбова, д. 3,
 строен. 3, каб. 13.

Президент М. Е. Борисов

Генеральный директор Г. А. Герасина

Директор ИТ-направления П. В. Христов

Коммерческий директор Т. Н. Филина

Подписные индексы:

Объединенный каталог «Пресса России» — 38185,
 «Каталог российской прессы» — 99483.

Отпечатано в ООО «Богородский полиграфический комбинат».

142400, Московская область,

г. Ногинск, ул. Индустриальная, д. 406

Тел.: (495) 783-9366, (49651) 73179

Тираж 10 000 экз.

Редакция не несет ответственности за содержание рекламных материалов. Все права защищены. Полное или частичное воспроизведение или размножение каким бы то ни было способом материалов, опубликованных в настоящем издании, допускается только с письменного разрешения ООО «Издательство «Открытые системы».

Windows®, Windows Vista® и Windows Server® — зарегистрированные торговые марки корпорации Microsoft. Название Windows IT Pro используется Penton Media, Inc. в соответствии с соглашением с владельцем торговой марки. Название Windows IT Pro/RE используется ООО «Издательство «Открытые системы» по лицензионному соглашению с Penton Media, Inc. Windows IT Pro/RE — независимое от корпорации Microsoft издание. Корпорация Microsoft не несет ответственности за редакционную политику и содержание журнала. Редакция оставляет за собой право не вступать в переписку.

Отобранные для публикации письма редактируются в соответствии с терминологическими нормами, принятыми в издательстве.

Названия продуктов и компаний, упомянутых в журнале, могут быть товарными знаками их владельцев.



Penton Media, Inc.

ИТ И БИЗНЕС

2 Новая напасть

ВЛАДИМИР БЕЗМАЛЫЙ

4 Запуск WorkMail не напугал ни Microsoft, ни Google

ТОНИ РЕДМОНД

6 Успешная карьера в сфере ИТ в эпоху «облака»

ПОЛЬ РОБИШО

ТЕМА НОМЕРА

8 Работа с адресами IPv4 в среде PowerShell

БИЛЛ СТУАРТ

12 Проверка подлинности запросов веб-служб с помощью PowerShell

МАРК МИНАСИ

14 Вопросы о PowerShell

ДЖОН СЭВИЛЛ

22 Учим PowerShell нажимать на кнопки

МАРК МИНАСИ

SQL SERVER

24 Логическая обработка запросов: предложения FROM и объединения

ИЦИК БЕН-ГАН

31 Логическая обработка запросов: предложение FROM и оператор APPLY

ИЦИК БЕН-ГАН

OFFICE SYSTEM

38 Синхронизация фотографий в Office 365

ТОНИ РЕДМОНД

40 Незначительные сбои как причина больших проблем

ТОНИ РЕДМОНД

42 Приступаем к проектированию локальных надстроек

ЛИАМ КЛИРИ

45 SharePoint 2016: конструируем надстройку с помощью Visual Studio

ЛИАМ КЛИРИ

ВВОДНЫЙ КУРС

49 Как создать установочный USB-диск на Mac

ВЛАДИМИР БЕЗМАЛЫЙ

50 USB Recovery Drive для операционной системы Windows 10

ВЛАДИМИР БЕЗМАЛЫЙ

51 Windows Defender Offline в Windows 10

ВЛАДИМИР БЕЗМАЛЫЙ

ОБНОВЛЕНИЯ

52 Предварительная версия SharePoint 2016: состояние дел

ЛИАМ КЛИРИ

ЛАБОРАТОРИЯ

54 Инструменты управления сервером Server Management Tools в Windows Server 2016

ДЖОН СЭВИЛЛ

EXCHANGE & OUTLOOK

56 Оглядываясь на мир Exchange в 2015 году

ТОНИ РЕДМОНД

58 Как развиваться администраторам Exchange в отсутствие углубленных учебных курсов

ТОНИ РЕДМОНД

60 Защита в сети — единственный возможный путь

ТОНИ РЕДМОНД

61 Трудности аудита почтовых ящиков Exchange

ТОНИ РЕДМОНД

62 Требования к общедоступным папкам

ТОНИ РЕДМОНД

63 Прогноз для Exchange на 2016 год

ТОНИ РЕДМОНД

ИЛЛЮСТРАЦИЯ НА ОБЛОЖКЕ KAVZOV® (FOTOLIA.COM)

Новая напасть

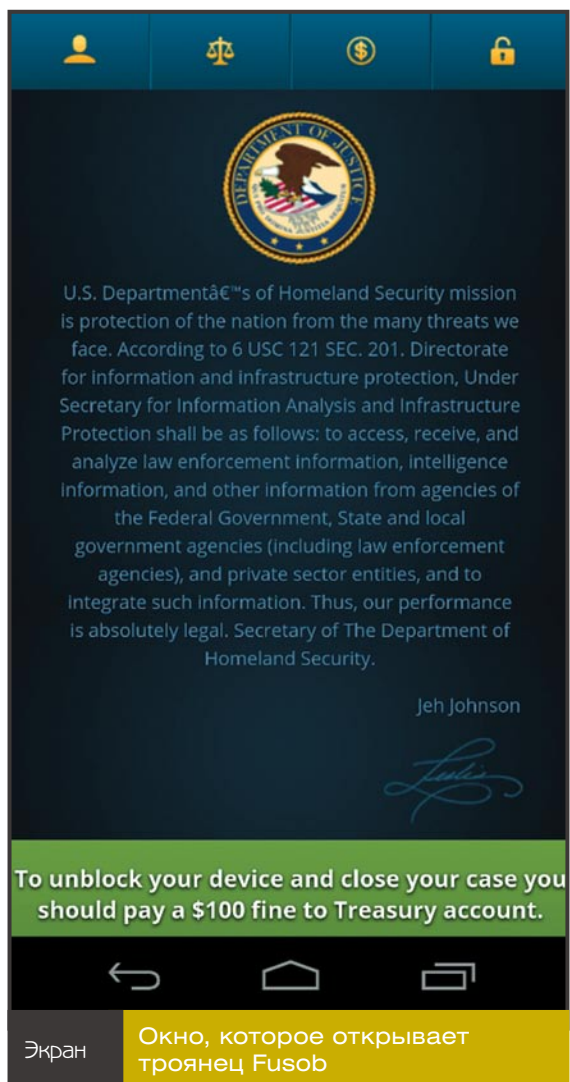
Владимир Безмалый

Одним из направлений развития вредоносных программ сегодня является программное обеспечение, блокирующее работу персонального компьютера, смартфона или планшета, обозначаемое термином ransomware. Если рассматривать его историю, то первыми видами таких программ были блокировщики браузеров. В дальнейшем развитие направления блокировки работы привело к появлению различного рода вредоносных шифровальщиков данных. Вначале это были программы для компьютеров под управлением Windows, затем для операционных систем Linux и Android, а теперь уже и для Mac. Фактически цикл развития данной «особи» завершен. В дальнейшем будут, вероятнее всего, совершенствоваться методы заражения и увеличиваться длина ключа шифрования.

Однако самыми опасными, на мой взгляд, являются программы типа Ransomware, реализованные в виде службы. Это происходит, когда разработчики соответствующего вредоносного программного обеспечения просто сдают его в аренду и сами практически не «светятся», а сосредоточиваются на разработке новых версий и новых методов заражения. Мало того, отследить такие группы разработчиков практически невозможно, ведь они мало контактируют с внешним миром. С другой стороны, резко увеличивается возможность заражения, ведь атаку на пользователей ведет множество групп подписавшихся на эту службу дилетантов, причем она продолжается ограниченное время. Следовательно, обнаружить подобную атаку бывает достаточно сложно, ведь при следующей попытке вредоносное программное обеспечение, скорее всего, будет уже модифицировано.

Что можно предпринять?

1. Универсальным советом по преодолению последствий атаки Ransomware, как и других, является создание резервных копий ваших данных на внешних носителях, подключаемых только на период создания копии. Говорят о таком способе противодействия достаточно давно, но, увы, особенно в среде пользователей персональных компьютеров резервное копирование так и не получило широкого распространения. Проблемой резервного копирования в «облачное» хранилище является в данном случае то, что «облачное» хранилище, как правило, подключено постоянно, следовательно, данные в нем могут быть также заражены и зашифрованы.
2. Обновление операционной системы и приложений, безусловно, поможет уменьшить вероятность заражения. Для этого необходимо вовремя обновлять операционную систему компьютера и приложения. В то же время, ввиду ухудшения качества обновлений, необходимо перед обновлением выполнять создание контрольной точки или опять-



Экран

Окно, которое открывает троянец Fusob

таки делать полную резервную копию компьютера. Не забудьте, что обновлять нужно не только операционную систему и приложения от Microsoft, но и приложения независимых разработчиков, в которых также могут быть уязвимые места.

3. Никогда не запускайте приложения, полученные из неизвестных источников. Как можно внимательнее отнеситесь к получаемым сообщениям электронной почты. Никогда не запускайте приложение и не щелкайте по ссылке в письме, особенно если не уверены в источнике. Не постесняйтесь переспросить отправителя, если письмо пришло из известного источника, на что именно он хотел обратить ваше внимание, что это за ссылка у него в письме.
4. Регулярно обновляйте антивирус. Хотя этот совет вы слышите очень часто, все же не забудьте обновить свой антивирус. И никогда не пользуйтесь взломанным антивирусом, поскольку неизвестно, в какой момент он откажет. Уж лучше используйте бесплатную версию.

Ransomware для Android

По данным Kaspersky Lab, в 2015 году, по сравнению с 2014 годом, количество обнаруженных семейств класса Trojan-Ransom удвоилось. Количество обнаруженных модификаций за этот же период выросло в 3,5 раза. Что это означает? Злоумышленники переключаются на выманивание денег у пользователей с помощью троянцев-вымогателей, продолжая активно создавать новые модификации вредоносных программ. Актуальность угроз подтверждается количеством атакованных пользователей. За 2015 год этот показатель вырос более чем в пять раз.

За разблокировку устройства пользователям предлагается заплатить от 12 до 100 и более долларов (см. экран). Зabloкированным устройством пользоваться невозможно. Некоторые программы умеют перекрывать даже системные диалоги (например, выключение телефона).


Однако самым важным событием 2015 года стало появление программ семейства Trojan-Downloader, которые в основном загружали в систему троянца-вымогателя Trojan-Ransom.AndroidOS.Pletor. Особенностью этих троянцев-загрузчиков стало то, что они используют уязвимые места в системе, чтобы получить права суперпользователя на устройстве и установить Trojan-Ransom в системную папку. После этого установленный троянец практически невозможно удалить.

Ransomware для Mac

В 2016 году программы типа Ransomware добрались до компьютеров Apple. Вымогатель шифрует файлы, а затем требует выкуп в 400 долл. для восстановления доступа к данным. О том, что компьютеры Mac были атакованы 28 февраля 2016 года, сообщало, например, агентство Reuters со ссылкой на представителей компании Palo Alto Networks. По словам директора компании Palo Alto Threat Intelligence Райана Олсона,

вирус под названием KeRanger стал первым в своем роде вирусом, заразившим компьютеры Mac от Apple. Злоумышленники смогли заразить компьютеры Mac через вредоносную копию популярной программы Transmission. Пользователи загружали версию 2.90 этой программы, и таким образом заражали свои компьютеры.

Представитель Apple заявил агентству, что компания незамедлительно приняла меры для предотвращения дальнейшего распространения вируса, аннулировав цифровой сертификат, который позволял мошенникам устанавливать программы на Mac. Другие подробности он сообщить отказался.

Как мы видим, атаки Ransomware принесли такую выгоду создателям этой программы, что в дальнейшем стоит ожидать лишь увеличения числа подобных атак. Тем более что занимающиеся борьбой с этим явлением представители спецслужб рекомендовали платить, мотивируя это тем, что таким образом пользователи смогут получить доступ к своим данным за минимальное время. С другой стороны, мне кажется, что, выплачивая деньги злоумышленникам, мы лишь поддерживаем их деятельность. Решение, одновременно простое и сложное, как я уже неоднократно говорил, состоит лишь в создании резервных копий на внешних отчуждаемых носителях. 

Владимир Безмальный (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor



DeviceLock® DLP

20 лет

70 000 клиентов

7 000 000 инсталляций

www.smartline.ru

Реклама

Запуск WorkMail не напугал ни Microsoft, ни Google



Тони Редмонд

Как мы недавно узнали, компания Amazon присвоила статус общей доступности своему решению WorkMail, предназначенному для управления календарями и электронной почтой. Цены начинаются от 4 долл. в месяц за почтовый ящик объемом в 50 Гбайт, но, учитывая, какую долю рынка «облачной» корпоративной почты занимают сейчас компании Microsoft и Google, можно себе представить, какой огромный путь предстоит проделать Amazon, чтобы занять здесь хоть сколько-нибудь значимое положение. Посмотрим, конечно, как будут развиваться события в течение года, однако не думаю, что большое число нынешних «локальных» клиентов Exchange за это время «бросятся в объятия» Amazon в стремле-

нии скорее опробовать на себе их новое решение.

Итак, компания Amazon объявила о том, что ее решение WorkMail, предназначенное для управления календарями и электронной почтой, наконец стало общедоступным, что, безусловно, не может не радовать всех, кто напряженно трудился над этим проектом в течение года.

Представители Amazon сообщили, что WorkMail работает с клиентами для рабочих станций и мобильных устройств, и предоставление данного сервиса обеспечивается центрами обработки данных Amazon Web Services (AWS), расположенными в США и Ирландии. Однако тот факт, что предоставление данного сервиса со стороны прочих региональных центров обработки дан-

amazon WorkMail




ных пока не реализовано, существенным образом ограничивает потенциал WorkMail в тех странах, где безопасному хранению данных уделяется особенное внимание.

И хотя представители Amazon заявляют, что WorkMail несложен в установке и поддержке, я полагаю, будет весьма непросто убедить потенциальных пользователей в том, что WorkMail — это реальный соперник для прочих систем на рынке корпоративной электронной почты. Надо сказать, что не многое изменилось с тех пор, как я впервые смог оценить предмет нашего обсуждения в апреле 2015 года, когда компания Amazon объявила о выпуске предварительной версии WorkMail. В частности, фактическое отсутствие какой-либо программной экосистемы вокруг этого продукта, скорее всего, будет иметь место и далее, поскольку компания Amazon не относится к числу тех крупных поставщиков программного обеспечения, которые широко известны своим успешным партнерским сотрудничеством с разработчиками.

Кроме того, у компании Amazon отсутствует какой-либо послужной список в деле выполнения миграций. Не буду спорить, они, конечно же, выполняли какие-то тестовые миграции на финишном этапе разработки своего продукта, но до меня не доходила какая-либо достоверная информация ни по сарафанному радио, ни посредством других, более современ-

ных видов связи о том, что мир электронной почты просто содрогнется до основания, когда в него придет WorkMail.

У меня есть вполне реальные основания сомневаться в том, что они способны выполнить миграцию на свою платформу чего-либо, кроме небольшого локального сервера Exchange, и не в последнюю очередь потому, что у них есть зависимость от 32-разрядных версий Outlook 2010 или 2013. Все-таки технологии миграции несколько изменились с тех пор, как обязательным требованием стала установка почтовых клиентов на серверах.

Я сильно сомневаюсь в том, что компании Microsoft или Google видят в ближайшей перспективе какую-либо угрозу в лице WorkMail для своих Exchange или Gmail. Несомненно, некоторые обязательно опробуют и эту технологию, но без гибридной связи и возможностей Microsoft Onboarding Center вряд ли многие из тех, кто подумывает о переходе с локального сервера Exchange, отдадут предпочтение WorkMail перед Office 365, даже учитывая более низкую цену в 4 долл. за почтовый ящик на 50 Гбайт. 

Тони Редмонд (12knocksinna@gmail.com) — редактор журнала Windows IT Pro, старший технический редактор Exchange & Outlook Administrator, вице-президент и главный технолог HP Services

ОАО «Корпорация «Иркут» защищает данные с помощью DeviceLock

Открытое акционерное общество «Научно-производственная корпорация «Иркут» (ОАО «Корпорация «Иркут») — вертикально-интегрированное предприятие, обеспечивающее полный цикл работ по проектированию, испытаниям, производству, маркетингу, реализации и послепродажному обслуживанию авиационной техники военного и гражданского назначения.

ИТ-инфраструктура корпорации предоставляет собой распределенную мультисервисную среду, охватывает центральный офис и удаленные структурные подразделения, включает в себя более 1500 рабочих мест. Аудит и оценка состояния информационной безопасности в компании проводятся непрерывно с помощью специализированного сертифицированного программного обеспечения, предназначенного для контроля уровня защищенности и степени соответствия стандартам и требованиям. В штате работают специалисты, прошедшие подготовку в области аудита на соответствие ISO27001.

Высокий уровень зрелости ИТ-составляющей корпорации, растущий объем и интенсивность обработки и обмена информацией как во внутренней распределенной сети, так и с внешними партнерами стали факторами, требующими наличия специализированного инструмента для контроля и мониторинга информационных потоков.

С внедрением ПО DeviceLock появилась возможность ограничить и контролировать использование сотрудниками внешних накопителей информации, принтеров и беспроводных устройств. С помощью ПО DeviceLock ведется контентный мониторинг файлов и данных, передаваемых на внешние носители информации. Кроме того, в результате внедрения DeviceLock были соблюдены требования государственных органов контроля по защите различных видов конфиденциальной информации.

Выбор ПО DeviceLock был обусловлен опытом работы с другим ПО, производители которого декларировали возможности совместимости своих программных продуктов по контролю использования внешних портов ПК. Кроме того, на выбор повлияли результаты анализа рынка программного обеспечения с аналогичной функциональностью. После успешного пилотного тестирования ПО DeviceLock в 2012 году было принято решение о его закупке, после чего собственными силами подразделения ИБ корпорации при участии интегратора были выполнены полномасштабное развертывание и настройка ПО DeviceLock с переводом системы в промышленную эксплуатацию. Стоит отметить, что случаи обращения в техническую поддержку разработчика отмечались только на этапе внедрения и в течение первого года эксплуатации ПО DeviceLock. При этом специалистами службы технической поддержки были оперативно предложены варианты решений возникших вопросов, а в течение последующего периода эксплуатации продукта причин для обращения в техподдержку уже не возникало.

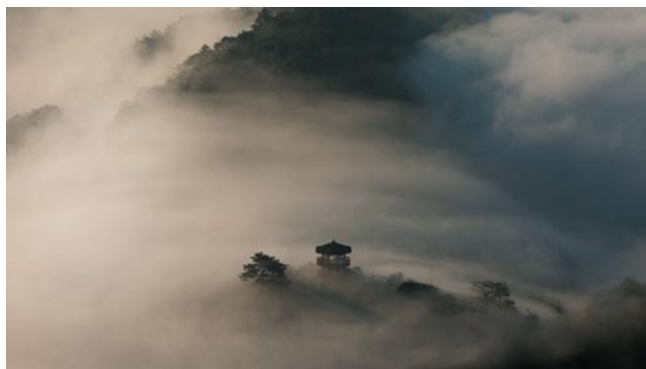
Успешная карьера в сфере ИТ В эпоху «облака»

Отрасль информационных технологий всегда была не самым удобным полем приложения сил для тех, кто хочет делать карьеру. Многие полагают, что такие явления, как стремительные изменения в «начинке» ИТ-систем, в технологиях, в динамике занятости, начались с появлением в нашей жизни «облачных» служб, но это не так. Те же тенденции, что беспокоят сегодняшних ИТ-администраторов, отмечались 40 и более лет назад — во времена, когда обработка деловой информации для предприятий обычно выполнялась на мэйнфреймах, расположенных в отдельных помещениях со стеклянными стенами в центрах обработки данных. С изменением доминирующих на рынке технологий менялся и набор компетенций, необходимых для специалистов, желающих оставаться на плаву. Один из самых распространенных вопросов, которые мне приходится слышать, когда речь идет о платформах Office 365, Azure и других «облачных» службах, звучит следующим образом: «Как мне повысить свою квалификацию так, чтобы держать руку на пульсе в ситуации, когда процессы, которыми я управляю, перемещаются в «облако»?»

Свой ответ на этот вопрос предлагают двое моих бывших коллег по Summit 7 Systems — обладатель статуса MVP по продукту Office 365 Бен Карри и ведущий эксперт по SharePoint Брайан Лоз. Оба они утверждают, что традиционно применявшийся и хорошо знакомый нам набор компетенций уже не актуален, и надо признать, что место испытанных временем «специалистов по ИТ» занимает теперь новая категория — «облачные профессионалы». Это интересная модель. Ее стоит рассмотреть подробнее и проанализировать, как она вписывается в тенденции современного рынка труда и как сочетается с другими силами, формирующими возможности трудоустройства в сфере ИТ.

Немного истории

В старые добрые времена специализация в сфере обработки информации была исключительно узкой. Существовали четкие различия между программистами, создававшими прикладные программы, системными программистами, разрабатывающими инструментальные средства и операционные системы, системными архитекторами или аналитиками, инженерами по оборудованию, обеспечивающими безотказную работу мощных систем, обслуживающим персоналом (чьи задачи часто сводились к выполне-



нию таких рутинных операций, как смена лент или чистка машин для перфорирования карт, но включали и такие задачи, как планирование работ и управление пользователями) и т. д. Бывало, что сотрудники переходили с одного участка на другой, но это случалось не так часто, как можно подумать: навыки, необходимые для выполнения различных видов работ, нередко являлись узкоспециализированными, и само обилие эксплуатируемых аппаратных и программных средств приводило к тому, что во многих случаях сотрудники имели дело с одной и той же платформой или технологией на протяжении почти всей своей карьеры. Такой была первая стадия формирования современной роли ИТ-профессионала. Это были высокоспециализированные, ориентированные на выполнение особых задач сотрудники, чья квалификация повышалась главным образом на рабочем месте.

Появление и развитие портативных компьютеров повлекло за собой явную демократизацию работы в сфере ИТ. Все началось с выпуска специализированных текстовых процессоров, поставляемых такими компаниями, как Wang, Lanier и Ecxon. Работа с этими системами не требовала (и чаще всего не допускала) программирования. Они могли функционировать без вмешательства со стороны системных архитекторов. Обычно их могли обслуживать сотрудники с ограниченными навыками в сфере ИТ (а то и вовсе без таковых). Производителям универсальных вычислительных средств не понадобилось много времени для того, чтобы тоже вступить на этот путь. Сначала появились мини-компьютеры, ориентированные на обслуживание филиалов и региональных офисов или центральных офисов не очень крупных компаний; за ними последовали системы для департаментов и рабочих групп. А это, в свою очередь, привело благодаря интенсивной эксплуатации закона Мура к появлению все