ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ РЕАЛИЗАЦИИ КОНЦЕПЦИИ BYOD

DOI: 10.25629/HC.2019.12.12

Останина Е.А.

Московский авиационный институт (национальный исследовательский университет)

Москва, Россия

Военная академия Ракетных войск стратегического назначения имени Петра Великого

Балашиха, Россия

Аннотация. Динамика современного мира диктует свои условия работы нынешних компаний. Внедрение новых концепций в работу организации наряду с положительными моментами связано со множеством возникающих рисков. В статье показан процесс интеграции Bring Your Own Device (BYOD) в организациях разных стран, соотношение ее сторонников и противников в ряде государств. Рассматриваются вопросы информационной безопасности деятельности организаций, принимающих концепцию BYOD в различных ее проявлениях. Показаны возможные последствия внедрения этой концепции без должного сопровождения процесса службой информационной безопасности, раскрыты нюансы защиты мобильных устройств различных производителей, которые могут использоваться сотрудниками в рабочих целях. Указаны основные направления работы служб информационной безопасности при реализации концепции BYOD при решении основных проблем и рассмотрены примеры решений. Описана общая стратегия безопасности. Предложена формула, описывающая общую стратегию безопасности BYOD, которую целесообразно дополнить распределенным личностным компонентом, учитывающим персональные характеристики подверженности социальной инженерии сотрудников организации. Сформулированы общие рекомендации по обеспечению безопасности при работе в концепции BYOD, которые включают установку MDM/MAM для управления безопасностью мобильных устройств, организацию подключения всех устройств только через VPN, предотвращение несанкционированного доступа с помощью использования надежных паролей с регулярным их обновлением, осуществление шифрования данных на устройствах, установку одобренного компанией антивирусного программного обеспечения, привлечение сторонних консультантов, фиксированный контроль любых обращений к ценным файлам, внедрение листов контроля доступа и брандмауэров, настройку оповещения о подозрительной деятельности, установку ограничений на скачивание и установку программ, внедрение комплексной ИТ-политики.

Ключевые слова. Информационная безопасность, концепция Bring Your Own Device (BYOD), личные технические устройства, мобильность, конфиденциальность, мотивация, уязвимости, целевые атаки, корпоративная сеть, облачные технологии.

Введение

Окружающий нас мир посредством внедрения новых технических и программных продуктов постоянно меняется, что сказывается на всех сферах деятельности человечества. Уже практически невозможно представить человека вдали от компьютеров и сотовых телефонов, незнакомого с Интернетом и виртуальной реальностью. Различные технические средства сопровождают нас повсюду: люди уже не расстаются со своими смартфонами практически не на миг, носят фитнес браслеты, чтобы быть в том числе постоянно на связи и контролировать свое состояние с помощью электронных устройств, связанных по Bluetooth и Wi-Fi. При этом происходит постоянный процесс подбора, адаптации, подстройки устройства «под себя» посредством реализации вкусовых предпочтений, настройки интерфейса и установки востребованного владельцем программного обеспечения и, таким образом, все большее к нему привыкание.

В тоже время все больше проявляется тенденция разрыва по техническим характеристикам и возможностям между личными и предоставляемыми организациями для работы техническими средствами, используемыми программными продуктами. Причем данная тенденция характерна не только для государственных организаций, но и для коммерческих. Так, все больше руководителей и собственников предпочитают экономить на обновлениях компьютеров, периферии и программах в том случае, если отсутствует явная (безусловная) потребность в этом. В результате у работников возникает внутренний диссонанс. Имея доступ к более совершенному оборудованию в личном пользовании сложно быстро и качественно выполнять работу на устаревшем. Подчеркнем, что данное явление наиболее свойственно тем государственным организация, для которых характерно отставание финансирования от современных темпов развития информатизации общества. В тоже время потребности в современных технических новинках человек вынужденно реализует с учетом своих интересов и за счет собственных средств. В результате можно предположить, что с большой долей вероятности, с учетом личной заинтересованности в результатах своего труда, работник может начать выполнять работу на более совершенной технике, используя личные устройства.

Следует также отметить существование у ряда организаций заинтересованность в использовании личных устройств и программных продуктов работниками в своей трудовой деятельности [12]. Это позволяет экономить на покупке и модернизации компьютерной и программной базы. Однако возникает и ряд существенных особенностей при такой организации процесса. В первую очередь это отражается на информационной безопасности и уровне технической поддержки работников.

Краткий анализ литературы

Анализ научной литературы, как в области информационной безопасности, так и в смежных с ней областях (компьютерные сети, информационные технологии, социальная инженерия) приводит к пониманию, что вопросы информационной безопасности организаций с учетом современных реалий и использования ими концепции Bring Your Own Device требуют дополнительной проработки, так как они оказывают существенное влияние на сохранение конфиденциальности информации, ее целостности и доступности.

Обсуждение

Тем не менее в настоящее время все больше компаний в той или иной степени внедряют у себя концепцию Bring Your Own Device (BYOD), что можно интерпретировать как «принеси свое собственное устройство». Так еще в 2004 году VoIP-провайдер BroadVoice предложил подключать к своей сети оборудование клиентов и обозначил такой способ как BYOD. В 2005 году появилась работа Рафаэля Баллагаса «BYOD: Bring Your Own Device», где подробнее рассматривалась возможность использования своих гаджетов в официальных организациях [6].

В 2009 Intel «обновила» понятие BYOD, несколько расширив его значение, и теперь данный термин стал означать использование сотрудниками компаний личных устройств для решения бизнес-задач.

По заключениям ряда экспертов, уже в 2014 г. на каждого работника умственного труда в среднем приходилось 3,3 подключенных устройства (в 2012 г. этот показатель составил 2,8 единицы) [3]. Постоянно растет применение мобильных технологий и устройств мобильного доступа. Проводимые исследования западных компаний свидетельствуют, что 95% организаций разрешают своим сотрудникам использовать на рабочем месте собственные устройства, 84% респондентов даже оказывают таким сотрудникам некоторую поддержку, а 36% опрошенных предприятий обеспечивают полную поддержку устройств сотрудников. Другими словами, они предоставляют поддержку любых устройств (смартфонов, планшетов, ноутбуков и т.п.), используемых сотрудниками на рабочих местах.

Приведем еще ряд данных, полученных при исследовании данного вопроса. Так по результатам исследований компании Fortinet, 74% респондентов регулярно используют личные гаджеты в производственных целях. В тоже время 55% из опрошенных считают такое использование личных устройств своим правом, а не привилегией. По данным исследования компании

Microsoft, наиболее лояльно к концепции BYOD относятся китайские компании (86%) и наименее лояльно – японские (30%) [4]. На рисунке приведено распределение уровня лояльности компаний разных стран к концепции BYOD.

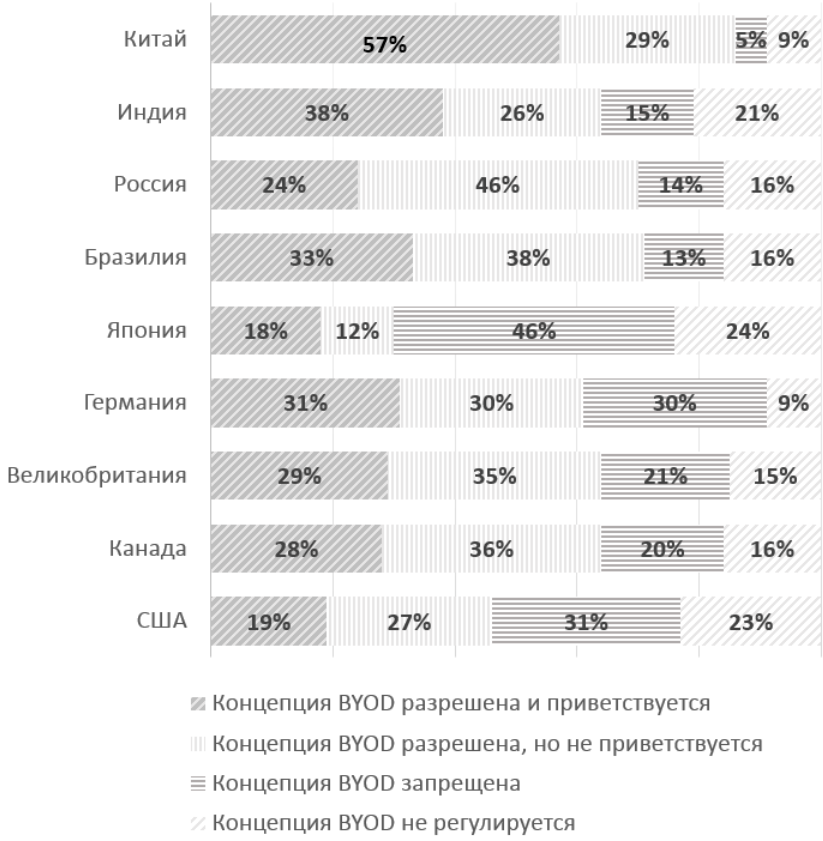

Рисунок 1 – Распределение уровня лояльности компаний в разных странах к концепции BYOD

Таким образом, в настоящее время можно сказать, что переход к данной концепции во многих организациях разных стран произошел «де факто».

По данным исследования Global Market Insights к 2022 году объем рынок BYOD превысит 366 млрд долларов, а Cisco сообщает, что 95% организаций в том или ином виде допускает использование личных устройств на рабочих местах [9].

Данная концепция помимо некоторой финансовой экономии может значительно повысить эффективность деятельности работников. Как правило, это приводит к изменению подхода, определяющего взаимоотношения компания-сотрудник и сотрудник с удовольствием использует то оборудование, которое выбрал сам, в тоже время компания получает работника, который всегда на связи и порой выполняет работу даже в нерабочее время. По данным Frost & Sullivan, BYOD добавляет к рабочему времени сотрудников до 58 минут в день и увеличивает продуктивность на 34%.

Следует отметить, что концепцию BYOD в разных организациях зачастую понимают по-разному. Например, некоторые компании разрешают сотрудникам использовать личные устройства для решения рабочих вопросов и компенсируют все расходы на связь и ремонт, либо подключают работников к корпоративному договору. В других компаниях все эти затраты сотрудник может нести сам [7].

В случае, когда компания не выбирает используемые сотрудниками устройства, может появиться проблема их совместимости. В этом случае решению вопросов финансово-правового характера и ее устранению будет способствовать подобная BYOD концепция CYOD. Ее аббревиатура CYOD расшифровывается как Choose Your Own Device – «выбери свое устройство». В рамках этой концепции сотрудник может выбрать из перечня типовых устройств то, которое наилучшим образом позволит ему решать рабочие задачи [5]. В этом случае в зависимости от корпоративной политики использование корпоративных устройств для личных целей может быть, как разрешено, так и запрещено.

Еще одной разновидностью данного подхода является COPE. Этот термин расшифровывается как Corporate-Owned, Personally Enabled и означает, что выбранные сотрудником устройства приобретаются компанией, но их настройкой и обслуживанием он занимается самостоятельно. Как правило, COPE предполагает и возможность использования устройства в личных целях [13].

В литературе можно встретить еще одно понятие Personally owned, company enabled (POCE) – «куплено сотрудником, разрешено в компании». Можно сказать, что по сути, это просто еще одно обозначение BYOD.

Таким образом, к преимуществам данной концепции для сотрудников можно отнести [9]:

возможность использования одного устройства для личных и рабочих задач (если это не противоречит установленной в организации корпоративной политике),

возможность использования самых новых моделей устройств,

мобильность,

гибкий график,

возможность удаленной работы.

В тоже время для компании неоспоримыми преимуществами становятся [9]:

снижение расходов (в зависимости от реализуемого варианта концепции компания может и вовсе не нести затрат на приобретение устройств, либо ограничиваться лишь их частичной компенсацией),

повышение уровня мотивации сотрудников,

доступность сотрудников в нерабочее время,

более высокую оперативность решения срочных вопросов,

снижение потребности в офисных помещениях.

Однако не стоит забывать, что концепция BYOD создает множество сложностей для ИТ-службы, службы защиты информации, а также разнообразных рисков для компании.

Применение личных технических устройств в качестве вспомогательных средств, а именно телефонов с выходом в Интернет для получения справочной информации в любом месте нахождения сотрудника, проведение каких-либо срочных работ на личных компьютерах\ноутбуках вне офисов (составление срочных писем, заявок, переговоров) является нормой, и даже необходимостью, во многих организациях [1]. Однако, использование личных ноутбуков в рабочих целях либо в качестве вспомогательного устройства, являясь довольно распространенной практикой, приносит и ряд сопутствующих проблем [2]. Службе защиты информации необходимо постоянно отслеживать на устройствах наличие критичных данных, реквизитов доступа к ресурсам корпоративной сети, к электронной почте и т.д. Этот процесс достаточно трудоемок, не всегда возможен с должным качеством и часто носит рекомендательный характер. В тоже время полный запрет использования личных устройств, к чему прибегает определенная категория организаций, осуществить в настоящее время весьма затруднительно. Зачастую это обусловлено и самими организациями, не обеспечивающими в должной мере обновление технических устройств и их программного обеспечения, а порой и просто отсутствие у предоставляемых устройств необходимых возможностей для быстрого и качественного выполнения поставленных задач.

Таким образом, можно утверждать о наличии такой уязвимости, как целевые атаки на личные устройства сотрудников, которые осуществляются для извлечения информации, срыва или создания помех для выполнения задач, программ или служб, а также для того, чтобы иметь возможность осуществления этих намерений при необходимости в будущем. Это усугубляется тем, что в большинстве случаев пользователи работают на своих устройствах с правами локального администратора, что значительно упрощает доставку вредоносного кода на эти устройства. Наиболее часто этот процесс осуществляется посредством атак методами социальной инженерии.

Отметим, что сейчас смартфоны и планшеты обладают, с точки зрения хранящихся на них данных, практически всеми возможностями ноутбуков. Они позволяют осуществлять доступ к корпоративным документам, специализированным сервисам, электронной почте, деловым контактам, планам и графикам рабочего процесса. Завладев таким устройством в результате кражи или банальной утери владельцем, злоумышленник может достаточно легко получить доступ к этим данным. В этом случае особым фактором риска может быть и невозможность мгновенного уведомления службы безопасности или оперативной блокировки устройства.

Отметим подверженность личных смартфонов и планшетов атакам, к которым относят и активное прослушивание. Это атаки класса Man in the middle (MITM), когда злоумышленник тайно ретранслирует и, при необходимости, может изменять связь между двумя сторонами, считающими, что они общаются друг с другом непосредственно. Службе безопасности довольно сложно осуществлять контроль за эфиром в зоне передвижения работника (владельца смартфона), в то время как заставить подключится мобильное устройство к «известной» точке доступа довольно легко. И в это время без ведома и желания обладателя смартфона злоумышленник легко может совершить перехват и подмену трафика или напрямую атаковать устройство (например, в случае с Android часто используют специальные модули Metasploit Framework) [14]. В тоже время Android-устройства с большой долей вероятности могут быть заражены какой-либо вредоносной программой, что обусловлено и большим ростом выявленных уязвимостей устройств, управляемых данной операционной системой. Риск при утере или краже может быть выше для устройств, прошедших процесс рутинга, когда были получены права суперпользователя, ведь основными целями рутинга является снятие ограничений производителя либо оператора связи, манипулирование системными приложениями и возможность запуска приложений, требующих прав администратора. Аналогичный процесс есть и для других устройств, например, для устройств на базе Apple iOS он называется джейлбрейк. Здесь очень важно заметить, что большинство пользователей, а по проведенным опросам этот показатель может достигать 80%, не читает предупреждений и подтверждает практически любые запросы от приложений [15].

Не лучше с точки зрения информационной безопасности обстоят дела и со столь популярными в наше время облачными технологиями. В этом случае при доступе к корпоративным данным значительно увеличивается риск утечки или кражи данных. Безусловно, облачные технологии открывают большие возможности комфортной работы из любой точки, с различными программами и большими объемами данных. Однако, проведенный опрос показал, что подавляющее большинство респондентов не читает пользовательское соглашение даже при размещении личной информации, что уж говорить о рабочей. Ведь подспудно работник считает, что об этом заботится соответствующая служба организации, в которой он работает. Однако нативные облачные хранилища (gmail, icloud, onedrive и т.д.) личных мобильных устройств находятся вне сферы контроля подразделений информационной безопасности и с высокой долей вероятности могут быть скомпрометированы злоумышленниками [8].

Также потенциальные угрозы могут быть обусловлены нерегулируемым доступом к сети, довольно слабой парольной политикой большинства пользователей, слабой подготовкой к угрозам целевых атак и применением социальной инженерии.

Таким образом, работа служб информационной безопасности при реализации концепции BYOD должна быть направлена на решение следующих основных задач:

снятие ограничений (например, заключение соответствующих договоров с владельцами) по контролю пользовательских устройств, задействованных в рабочем процессе;

разграничение личных и корпоративных конфиденциальных данных на устройствах;

учет и, если будет возможно, повышение защищенности мобильных ОС (iOS, Android), которые не предоставляют многих традиционных функций безопасности и соответствующих интерфейсов для их реализации.

Для предотвращения рисков безопасности в этом случае целесообразно установить политику BYOD с четким планом и адаптацией ко всем используемым платформам вне зависимости от размера и статуса организации. Только после установки всех правил и критериев использования как технических средств, так и программных продуктов, возможна выдача разрешений на подключение к корпоративной сети личных устройств сотрудников. Уже на начальных этапах необходимо принять решение, какими приложениями можно пользоваться исключительно с корпоративных компьютеров, а какие будут доступны с любого устройства [11]. Возможно также разрешение использования личных устройств при условии установки на них специального программного обеспечения для доступа к информационным ресурсам организации или напротив, определение выборки типов мобильных устройств, разрешенных к использованию. Невозможно дать рекомендации для всех организаций без исключения и здесь необходимо с учетом современного развития технических средств и программных продуктов найти приемлемое решение для любых сценариев, используя тот или иной подход.

В идеале это призвано обеспечить баланс между обеспечением безопасности корпоративных данных и соблюдением конфиденциальности сотрудников, которые должны иметь возможность продолжать использование своих устройств в личных целях. К сожалению, чаще всего работник начинает использовать персональное устройство, либо не задумываясь о возможных последствиях, либо подспудно ожидая тотального контроля над своим устройством со стороны службы безопасности [10]. Необходимо помнить, что, чрезмерно строгая или агрессивная политика со стороны администрации и службы информационной безопасности контрпродуктивна. Она должна быть полностью прозрачна в плане определения ответственности каждой из сторон и нацелена на их взаимные интересы.

В свете вышесказанного с учетом природы возникающих рисков, связанных с информационной безопасностью, компаниям целесообразно осуществлять непрерывный мониторинг корпоративной сети и всех ее точек доступа. Безусловно, при использовании концепции BYOD недостаточно организовать защиту только физического периметра, она должна простираться на все конечные устройства.

В качестве одного из примеров такого типа решений можно привести Adaptive Defense – сервис обнаружения атак на конечные устройства и реагирования на них, способный точно классифицировать любое приложение и блокировать многие современные угрозы, включая направленные атаки и угрозы нулевого дня [8].

В настоящее время одним из надежных решений по обеспечению безопасности при использовании в организации концепции BYOD считается удаленное подключение персональных устройств через терминальные сессии к виртуальным Windows-средам, которые в свою очередь защищены хостовой DLP-системой, обеспечивающей предотвращение утечек информации с виртуальных машин. Такой подход носит название Virtual Data Leak Prevention (vDLP).

При использовании инфраструктуры виртуальных рабочих мест VDI (Virtual Desktop Infrastructure), они представляют собой пользовательские приложения или целые операционные системы, работающие в виртуальной среде под управлением супервизора, функционирующего на централизованном сервере. В этом случае один физический сервер, на котором развернута виртуальная среда, может одновременно работать со множеством виртуальных пользовательских рабочих мест, развернутых в его виртуальных машинах. Их число зависит от количества памяти и вычислительных ресурсов этого сервера. Такой подход обеспечивает централизованное администрирование и хранение данных. Он позволяет по мере необходимости наращивать инфраструктуру, создавать, или удалять рабочие места, а также легко переносить

их с одного сервера на другой. К достоинствам применения таких рабочих мест относят достаточно высокую защиту корпоративных данных в виртуальной среде с одновременным предоставлением пользователю свободы действий и открытием доступа к корпоративным информационным ресурсам через защищенное окно, которое предотвращает утечку конфиденциальных данных на личное устройство.

Таким образом, данная технология предлагает контролируемое предоставление удаленного доступа к корпоративным данным в отличие от локального хранения данных на BYOD-устройствах в подходе MDM (Mobile Device Management).

Приложения MDM представляет собой программное обеспечение для работы с корпоративными системами при помощи мобильных устройств. Однако, к сожалению, многие мобильные пользовательские устройства и средства управления ими не решают проблем распространения и обновления программного обеспечения, применения корпоративных политик, полного управления инвентаризацией и сетевыми сервисами. В настоящее время многообразие пользовательских устройств в значительной степени затрудняет внедрение MDM подхода. Он применим и может эффективно применяться при использовании только некоторых типов устройств, в то время как остальные остаются уязвимыми для потенциальных атак.

Идею MDM-продуктов можно уложить в рамки многоуровневой модели безопасности (Layered Security Model), предложенной компанией MobileIron [17]. Суть данной стратегии состоит в нахождении компромисса при решении следующих задач:

сохранение привычной для пользователя рабочей среды;

минимизация влияния на процесс взаимодействия пользователя со своим устройством механизмов безопасности;

создание доверенной среды пользовательских приложений, разрабатываемых сторонними организациями и применяемыми пользователем в то время как они предоставляют необходимый набор сервисов.

В литературе [8] можно встретить следующую формулу, описывающую общую стратегию безопасности BYOD:

$$\text{Безопасность BYOD} = \text{MDM} + \text{vDLP (App} + \text{VPN} + \text{VM} + \text{DLP)},$$

где MDM – система контроля локальных приложений на устройствах удаленного уничтожения данных, обеспечения надежной парольной защиты устройства и шифрования данных и т.п.;

App – приложение для удаленного подключения мобильного устройства через интернет к виртуальному хостингу приложений организации (например, Citrix Receiver);

VPN – защищенное криптографическим протоколом SSL подключение к VPN-сети организации, используемое опубликованными приложениями, в том числе для дополнительной аутентификации пользователей;

VM – виртуальная реализация Windows-системы на базе средств виртуализации Citrix / WTS / MS RDx / др., предоставляющая пользователям рабочую среду, в которой могут быть опубликованы и доступны необходимые для работы приложения и данные;

DLP – система предотвращения утечек данных, интегрированная в виртуальную рабочую среду Windows, обеспечивающая контроль доступных в этой виртуальной среде каналов передачи данных (электронная почта, веб-сайты, мессенджеры, канал печати, перенаправленные в виртуальную среду локальные USB-устройства) для предотвращения утечек данных с BYOD-устройства.

Данная формула достаточно полно учитывает компоненты, необходимые в настоящее время для обеспечения информационной безопасности в организации, использующей концепцию BYOD. Однако целесообразно дополнить ее распределенным личностным компонентом,

учитывающим персональные характеристики подверженности социальной инженерии сотрудников организации. Отметим, что значения данной составляющей при использовании личного или корпоративного устройства могут значительно разниться, что может быть обусловлено психологической компонентой работника, его подсознательным отношением к личному и рабочему устройствам, настрою на деятельность и т.д.

Как правило, применяющийся в настоящее время в организациях набор политик, работающий на уровне сети, способен обеспечить контроль доступа пользователей в сеть и сформировать профили для различных сетевых элементов при определении того, какая информация может храниться или передаваться через то или иное устройство. В тоже время определяются точки контроля передаваемых данных до того, как они попадают в сеть или покидают ее. Однако не существует единого универсального средства, способного решить одновременно все проблемы [16]. Только системный подход, ориентированный на использование проверенных эффективных практик в области технологий защиты информации, решений по безопасности для сетевой инфраструктуры и клиентского программного обеспечения, поддерживающих современные мобильные технологии позволит пользователю быть уверенным в том, что его приложения будут надежно защищены, не зависимо от местоположения устройства.

Для примера приведем защиту сети компанией Fortinet, которая предлагает UTM-устройства, обеспечивающие функции межсетевого экрана, аппаратно-реализованные в специализированных ASIC-микросхемах, а также функции антивируса, системы противодействия прохождению различных типов вредоносного кода, системы предотвращения вторжений, способные обеспечивать защиту инфраструктуры в режиме реального времени. Для защиты передаваемых и хранимых данных компания предлагает встроенный в продукты Fortinet модуль безопасности Application Control, использующий постоянно обновляющуюся в режиме онлайн базу данных сигнатур FortiGuard, который позволяет контролировать уже более 2200 различных веб-приложений, программ, сетевых сервисов и протоколов на предмет наличия в них вредоносного трафика. Для распознаваемых сетевых приложений решение Fortinet способно контролировать все действия, предпринимаемые программным обеспечением, и создавать для этого гранулярные политики в зависимости от пользователя, группы, дня недели, времени, а также комбинации этих и ряда других параметров [16]. Отметим, что другой важной функцией, входящей в комплект решения Fortinet, является функция предотвращения утечек данных – DLP (Data Loss Prevention), которая имеет целый набор функций выявления в передаваемых данных утечек важной информации во внешние сети. Для контроля и защиты устройств мобильных пользователей при покидании ими периметра защищенной корпоративной сети, используется Web-фильтрация запросов пользователей, позволяющая задавать категории сайтов, разрешенных для посещения пользователям в определенное время и поддерживающая обновляемый в режиме реального времени сервис подписки на базу данных категорий веб узлов в зависимости от их содержимого. Также важным условием является возможность создания списка запрещенных URL для определенных групп или всех пользователей корпоративной сети. Следует отметить присутствие в этой системе существенного компонента защиты от перехвата пользовательской информации, а именно шифрования с применением технологий IPSEC и SSL. Таким образом, клиентское программное обеспечение – агент FortiClient, работающее на большинстве типов мобильных платформ, позволяет обеспечить максимальную защиту каждого конкретного клиентского устройства.

На основании вышеизложенного можно сформулировать общие рекомендации по обеспечению безопасности при работе в концепции BYOD:

установка MDM/MAM (mobile device management/mobile application management) для управления безопасностью мобильных устройств;

организация подключения всех устройств только через VPN;

блокирование устройств надежными паролями с регулярным их обновлением;

осуществление шифрования данных на устройствах, чтобы все данные, скачиваемые на пользовательское устройство, хранились на нем в зашифрованном виде;

установка одобренного компанией антивирусного программного обеспечения;

привлечение сторонних консультантов для аудита безопасности и поиска оптимальных решений;

контроль любых обращений к ценным файлам, включая автоматические обращения со стороны сервисных процессов, таких как SFTP;

внедрение листингов контроля доступа и брандмауэров;

настройка оповещения о подозрительной деятельности, неавторизованных попытках получения доступа, отсутствии лог-файлов;

установка ограничений на скачивание и установку программ, наличие собственного средства распространения программного обеспечения;

внедрение комплексной ИТ-политики, запрещающей пользователям делиться логинами и паролями. В случае необходимости делегирования рабочих задач использовать временный доступ к соответствующей учетной записи для «заместителя» или использовать цифровое хранилище данных для входа в сеть.

Выводы

Применение концепции BYOD нуждается в постоянном контроле со стороны служб информационной безопасности для предотвращения потенциальных угроз. Необходим тщательный учет возможных рисков и защита сетевого периметра и устройств пользователей. Разработка и внедрение в повседневную практику политики безопасности, на которую могут ориентироваться пользователи в процессе работы, позволит обеспечить дополнительный уровень защиты.

Заключение

Исследования могут быть продолжены в направлении создания гибкой системы информационной безопасности, адаптирующейся под различные модификации личных технических устройств и современных программных продуктов при использовании компанией концепции BYOD и ее вариантов. На основе данных регулярного мониторинга возможна разработка дополнительных рекомендаций по обеспечению информационной безопасности и преодолению возможных негативных последствий в следствии несвоевременного выявления угроз и новых атак.

Литература

1. Григорьев С.М., Карасев В.А., Останина Е.А. Моделирование механизма мотивации в процессе управления персоналом // Человеческий капитал. 2019. №5(125). С. 163-170.

2. Концепция BYOD: Гибкость и безопасность // URL: https://pirit.biz/informaciya/articles/koncepciya-byod-gibkost-i-bezopasnost (дата обращения: 25.09.2019).

3. Корпоративная мобильность Bring Your Own Device - BYOD // URL: http://www.tadviser.ru/... Bring_Your_Own_Device_-_BYOD) (дата обращения: 06.10.2019).

4. Крылов А. Подходы к обеспечению безопасности в концепции BYOD // URL: https://www.anti-malware.ru/analytics/Technology_Analysis/BYOD_Security (дата обращения: 05.10.2019).

5. Монтгомери С. От BYOD к CYOD: внедрить и не «подставить» IT-отдел // URL: http://www.avclub.pro/articles/byod-cyod/ot-byod-k-cyod-vnedrit-i-ne-podstavit-it-otdel/ (дата обращения: 25.09.2019).

6. Мухаметшин Р. Что такое BYOD и насколько она эффективна в организациях? // URL: https://ecm-journal.ru/post/Chto-takoe-BYOD-i-naskolko-ona-ehffektivna-v-organizacijakh.aspx (дата обращения: 06.10.2019).

7. Останин О.В., Останина Е.А. Актуальные подходы к мотивации персонала организаций различного профиля // Инновационная экономика и современный менеджмент. 2017. №5. С. 31-37.

8. Пискунов И. Концепция безопасности BYOD в корпоративной среде // URL: https://ipiskunov.blogspot.com/2016/07/byod.html (дата обращения: 10.10.2019).

9. Приносить нельзя запретить: как реализовать концепцию BYOD и не нанести ущерба информационной безопасности // URL: https://habr.com/ru/company/trendmicro/blog/467399/ (дата обращения: 05.10.2019).

10. Сафонов Л. BYOD – удобство против безопасности // URL: https://habr.com/ru/company/pentestit/blog/281463/ (дата обращения: 03.10.2019).

11. Теория и практика принятия управленческих решений: учебник / Под ред. Москвитина Г.И. М: КНОРУС, 2017. 340 с.

12. Управление персоналом: учебное пособие / Карпов В.В., Моисеев А.В., Барчан Н.Н. и др., М: ВА РВСН им. Петра Великого, 2013. 359 с.

13. Что скрывается за понятиями BYOD, CYOD, COPE // Журнал сетевых решений/LAN 2013 № 06 URL: https://www.osp.ru/lan/2013/06/13036077 (дата обращения: 01.10.2019).

14. 5 мифов о безопасности BYOD // URL: https://www.devicelock.com/ru/articles/5-mifov-o-bezopasnosti-byod.html (дата обращения: 06.10.2019).

15. BYOD: когда защиты периметра уже недостаточно // URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/343512.php (дата обращения: 08.10.2019).

16. BYOD: концепция, технологии и решения // URL: https://skomplekt.com/solution/byod.htm/ (дата обращения: 21.09.2019).

17. BYOD: when protecting the perimeter is not enough // URL: https://www.pandasecurity.com/mediacenter/business/byod/ (дата обращения: 03.10.2019).

Останина Елена Анатольевна. E-mail: neka1818@mail.ru

Дата поступления: 18.10.2019 Дата принятия к публикации 10.12.2019

INFORMATION SECURITY IN THE IMPLEMENTATION OF BYOD CONCEPT

DOI: 10.25629/HC.2019.12.12

Ostanina E.A.
Moscow Aviation Institute (National Research University)
Moscow, Russia
Peter the Great Military Academy of Strategic Missile Forces
Balashikha, Russia

Abstract. The dynamics of the modern world dictates its working conditions for current companies. The introduction of new concepts in the organization's work, along with the positive aspects, is associated with many emerging risks. The article shows the integration process of Bring Your Own Device (BYOD) in organizations of different countries, the ratio of its supporters and opponents in a number of states. The issues of information security of the activities of organizations adopting the BYOD concept in its various manifestations are considered. The possible consequences of introducing this concept without proper support by the information security service are shown, the nuances of protecting mobile devices of various manufacturers that can be used by employees for work purposes are disclosed. The main directions of the work of information security services in the implementation of the BYOD concept in solving basic problems are indicated and examples of solutions are considered. A general security strategy is described. A formula is proposed that describes the general BYOD security strategy, which should be supplemented by a distributed personal component that takes into account the personal characteristics of the social engineering exposure of the organization's employees. The general recommendations for ensuring security when working in the BYOD concept are formulated, which include the installation of MDM / MAM for managing the security of mobile devices, organizing the connection of all devices only via VPN, preventing unauthorized access by using strong passwords with regular updates, encrypting data on devices, installing company-approved antivirus software, attracting third-party consultants, fixed control of any images eny to valuable files, the implementation of access control lists, and firewall settings for suspicious activity alerts, setting restrictions on downloading and installing programs, implementation of a comprehensive IT policy.

Keywords. Information security, Bring Your Own Device (BYOD) concept, personal technical devices, mobility, privacy, motivation, vulnerabilities, targeted attacks, corporate network, cloud technologies.

Ostanina Elena Anatolyevna. E-mail: neka1818@mail.ru

Date of receipt 18.10.2019 Date of acceptance 10.12.2019