УДК 004.056.53

Специальный съемный носитель как среда передачи журналов средств доверенной загрузки

А. А. Алтухов
Закрытое акционерное общество "ОКБ САПР", Москва, Россия
Московский физико-технический институт (государственный университет), г. Долгопрудный, Московская область, Россия
Национальный исследовательский ядерный университет "МИФИ", Москва, Россия

Рассматриваются стратегии управления мобильными устройствами и возникающие при их применении проблемы информационной безопасности. Предлагаются способы использования парадигмы доверенного сеанса связи для решения проблемы безопасного применения мобильных устройств в стратегиях BYOD и COPE.

Ключевые слова: стратегии управления мобильными устройствами, BYOD, COPE, COBO, доверенный сеанс связи, новая гарвардская архитектура, доверенные вычисления, безопасность мобильного телефона, безопасность информации, безопасность мобильных устройств, мобильность, удалённый доступ, безопасность смартфона, безопасность планшета.

Применение мобильных устройств для выполнения рабочих обязанностей становится обычным явлением. В существующих информационных системах (ИС) активно стараются поддержать такую возможность. При проектировании новых ИС такую возможность закладывают заранее.

Угрозы, связанные с доступом с мобильных устройств к корпоративным или государственным ИС, не остаются без внимания специалистов в области информационной безопасности (ИБ). Данный факт подтверждается работами, связанными с анализом рисков и угроз, возникающих при использовании мобильных устройств [1—4]. Существует и большой список продуктов, решающих задачу обеспечения ИБ мобильных устройств в инфраструктуре [4—8].

Использование новых технологий и подходов обусловлено в первую очередь задачами бизнеса, необходимостью улучшения производства. Условием использования мобильных устройств предполагается наличие стратегии управления последними. Существует несколько стратегий управления мобильными устройствами. Каждая из них требует применения специальных методов по обеспечению безопасности.

Далее будет показано, что обеспечение должного уровня защищенности оконечных мобильных устройств (*endpoint devices*) является необходимым условием безопасной реализации стратегии обеспечения мобильности предприятия. Будут рассмотрены существующие методы обеспечения безопасности и показана ключевая проблема ИБ, возникающая при использовании мобильных устройств. Будет продемонстрирована возможность применения парадигмы доверенного сеанса связи (ДСС) с целью обеспечения безопасности при использовании различных стратегий управления мобильными устройствами [9].

В первой части работы подробно рассмотрены существующие политики управления устройствами, указаны их плюсы и минусы. Во второй части работы будет сделан обзор методов защиты. В третьей части сделан краткий обзор парадигмы ДСС и концепции новой гарвардской архитектуры. В заключительной части показано, каким образом существующие решения и подходы в рамках парадигмы ДСС можно использовать для безопасного применения мобильных устройств в рамках конкретных стратегий управления.

Стратегии управления устройствами

Можно выделить три основные стратегии управления мобильными устройствами. Давайте рассмотрим их по отдельности.

Традиционной стратегией управления мобильными устройствами является *Corporate Owned, Business Only (COBO)*. Данная стратегия широко используется в органах государственной власти, здравоохранении, финансах и других аналогичных отраслях. В рамках *COBO* работодатель выдает в

Алтухов Андрей Андреевич, программист 1-й категории группы программирования ПО СЗИ, ассистент, аспирант.
E-mail: altuhov@okbsapr.ru

Статья поступила в редакцию 5 июня 2017 г.

пользование сотруднику мобильное устройство исключительно для выполнения рабочих задач. Плюсы подобной схемы заключаются в простоте управления для работодателя. Возможность выстроить грамотную и четкую систему управления позволяет легко реализовать безопасность подобных устройств. При таком подходе все методы и стратегии, применяемые к стационарным автоматизированным рабочим местам (АРМ) (в дальнейшем будем называть такие подходы и методы классическими подходами), применимы и для мобильных устройств, использующихся в рамках данной стратегии.

Отрицательным моментом является необходимость для сотрудника использовать в общем случае два устройства: одно для служебного пользования и одно для личного (последнее ему может быть и не нужно). Естественно, все служебные устройства и необходимое ПО приобретает работодатель.

Второй стратегией является *Corporately Owned, Personally Enabled (COPE).* В *COPE* работникам также предоставляется устройство компании. Данное устройство они могут использовать как для решения рабочих задач, так и для личного пользования (электронной почты и приложений). Часто на личное использование накладываются серьёзные ограничения: запрет доступа в социальные сети, посещения определённых ресурсов, использования определенного ПО.

COPE часто применяется совместно с подходом *Choose Your Own Device (CYOD)*. Данный подход предоставляет сотруднику возможность выбора из нескольких различных моделей устройств от разных производителей, утверждённых работодателем. Часто в литературе стратегии *COPE* и *COYD* не разделяются и обозначаются *COPE/COYD*. Далее под *COPE* будет подразумеваться оба подхода: обычная стратегия *COPE* и расширенный вариант *COPE/COYD*.

COPE является развитием классической *COBO,* в рамках которой предпринята попытка решить проблему неудобства использования двух устройств. Поскольку работодатель является владельцем мобильного устройства, он оставляет за собой право полного контроля над данной вычислительной средой (ВС). Однако в рамках данной стратегии у сотрудника появляется возможность использования устройства для решения некоторых своих личных задач. Степень свободы, которая дается сотруднику, может различаться в зависимости от конкретных обстоятельств. Определить границы использования устройства для личного и служебного пользования, разработать необходимую политику ИБ, реализовать организационно-технические меры — все это требует дополнительных затрат со стороны работодателя. Как и в случае с *COBO*, работодатель приобретает устройства.

Bring Your Own Device (BYOD) — это стратегия, в рамках которой сотруднику позволяется использовать его персональные мобильные устройства (в том числе персональный ноутбук) для доступа к корпоративным данным, системам или ресурсам. Следует отметить, что конкретные реализации *BYOD* различаются степенью строгости (данное утверждение верно и для *COPE*, но для *BYOD* это явно фиксируется в литературе). Компания IBM выделяет четыре базовые разновидности [10, 11]:

- неограниченный доступ к корпоративным системам для персонального устройства;
- доступ только к незначительным системам или данным;
- доступ к ресурсам при полном или частичном контроле службы IT и ИБ работодателя персонального устройства, включая приложения и данные;
- доступ к корпоративным ресурсам при предотвращении возможности локально сохранять данные на персональном устройстве.

Долгое время *BYOD* являлась трендом в индустрии ИТ. Тренд был настолько сильный, что затронул не только сферу здравоохранения, но и органы государственной власти. Однако проблемы, в частности связанные с рисками использования *BYOD,* несколько снизили популярность. Хотя число активных призывов к использованию данной стратегии уменьшилось, бизнес по-прежнему стремится ее использовать [12].

Плюсы *BYOD* заключаются в возможности использования одного устройства для личного пользования и решения рабочих задач. Также работодатель не несет затрат, связанных с приобретением устройств. Однако указанные плюсы в то же самое время являются причинами огромных проблем, связанных с управлением и безопасностью [13, 14].

Гибридные стратегии также существуют. Немногие работодатели будут использовать одну конкретную стратегию. Возможны применения различных стратегий на различных организационных уровнях на основе ролей пользователей и требований.

Следует отметить, что, с одной стороны, сильно ограниченная *BYOD* может выродиться в *COBO*. С другой стороны, возможны варианты *COPE*, при которых сотрудник будет обладать правами локального администратора операционной системы (ОС) мобильного устройства и его

использование для персональных нужд будет никак не ограниченно. С формальной точки зрения отличие *COPE* от *BYOD* заключается только в том, кто является юридическим владельцем устройства. В зависимости от того, является ли владельцем работодатель (*COPE*) или сотрудник (*BYOD*), поразному выстраивается взаимодействие работодателя и подчинённого. В случае *BYOD* работает запретительный подход для сотрудника со стороны работодателя, в случае *COPE* — разрешительный. Все это позволяет утверждать, что большая часть угроз безопасности, проблем управления одинакова для обеих стратегий.

Обеспечение безопасности для каждой стратегии управления мобильными устройствами

Несмотря на различные модели угроз, огромное количество существующих технологий, схема доступа к корпоративным или государственным ИС в подавляющем большинстве случаев сводятся к клиент-серверной модели.

Для данной модели нужно обеспечить доверенность оконечного устройства, безопасность канала связи и безопасность серверной части (самой инфраструктуры) [15—18].

Необходимым условием доверенности оконечного устройства является защита от воздействия вредоносного кода и несанкционированного доступа (НСД), что можно обеспечить следующими способами [19]:

- доверенная загрузка ОС;
- защита информации от НСД;
- разграничение доступа к ресурсам;
- антивирусная защита.

Способы организации доверенного сетевого соединения [15,16, 20—22]:

- криптозащита трафика;
- физическая изолированность от сетей общего пользования при расположении в контролируемой зоне.

Поскольку мобильное устройство может покидать периметр организации и не привязано к конкретному месту, любое мобильное устройство может быть потеряно или украдено. Подобные угрозы также должны приниматься во внимание.

В случае *COBO* модель угроз во многом будет схожа с любым немобильным АРМ, который используется внутри периметра организации. Все подходы к обеспечению ИБ для немобильных АРМ применимы и для мобильных *COBO*-устройств. Дополнительные угрозы, возникающие из-за свойства мобильности, например потеря устройства или его кража, нейтрализуются криптографическими методами [23]. Несмотря на важность применения специализированных решений по управлению мобильными устройствами (*MDM*), в рамках *COBO* можно прекрасно нейтрализовать угрозы и классическими методами, обойдясь только обеспечением доверенной среды, разграничением доступа и криптографическими операциями.

Поскольку устройства являются собственностью работодателя, никаких серьезных правовых, технических или организационных проблем для данной стратегии управления мобильными устройствами не возникает. Жизненный цикл устройства достаточно прост и не зависит от сотрудника. Все необходимые процедуры до передачи сотруднику, во время эксплуатации устройства и после завершения эксплуатации можно четко регламентировать.

Применяемые подходы для *COPE* во многом совпадают с *COBO*. Большая часть угроз и методов их нейтрализации такая же, как и для *COBO*. Аналогично происходит настройка рабочей среды для сотрудника. Однако устанавливается и дополнительное ПО для решения личных задач сотрудника. Данные задачи и ПО обговариваются, документально фиксируются, их перечень может расширяться в процессе работы. Также обговариваются действия, которые могут осуществлять работодатель и сотрудник над данными, будут получаемыми в рамках персональной работы. Для компаний с высокими требованиями к ИБ данные, полученные в результате персональной деятельности, подвергаются аудиту со стороны работодателя. Подобная строгость обусловлена в том числе задачей предотвращения возможных утечек данных. В связи с возможностью выполнения личных задач в данной стратегии появляются дополнительные угрозы, не характерные для *COBO*. Эти угрозы нейтрализуются простыми системами *MDM* или классическими методами. Наличие данных для персонального использования на мобильном устройстве усложняет жизненный цикл последнего. В отличие от *COBO* при завершении использования сотрудником устройства необходимо осуществить дополнительные операции над личными данными, особенно если их нужно передать сотруднику. Поскольку владельцем устройства является работодатель, все спорные моменты он может заранее решить в свою пользу и оговорить их в трудовом договоре. Примерами могут служить запрет на локальное хранение личных данных, невозможность копирования данных из ВС, отказ в предоставлении сотруднику любых дан-

ных, хранящихся на мобильном устройстве, передача всех авторских прав на продукт, созданный на устройстве компании. Таким образом, несмотря на наличие новых угроз в данной стратегии, за счет возможности строгого контроля подобные угрозы просто локализовать и нейтрализовать.

В случае применения *BYOD* угрозы во многом схожи с *COPE*, но их сложнее локализовать и нейтрализовать в силу меньшей возможности контроля. Появляются и новые угрозы, характерные для *BYOD.*

Приведем пять основных проблем безопасности, возникающих при использовании *BYOD* [3, 10] и прокомментируем каждую из них.

Увеличение рисков утечки данных. При активном вовлечении мобильных устройств в рабочий процесс увеличивается количество возможных утечек данных и новых угроз. Для защиты от этих угроз необходимо не только установить специальные средства защиты и управления, но и поддерживать устройства сотрудников в безопасном состоянии. Установка нового и обновление ранее установленного ПО, изменение настроек безопасности для различных моделей мобильных устройств и ОС — все это требует дополнительных ресурсов.

Рост числа уязвимостей, которые может эксплуатировать злоумышленник. Службы ИТ и ИБ имеют меньше контроля над используемыми в организации устройствами, из чего с неизбежностью следует более высокий риск реализации атак на инфраструктуру. Количество различных моделей устройств, версий ОС, установленного ПО в общем случае может быть велико, что тоже является причиной роста числа уязвимостей. Сотрудники загружают приложения и подключаются к различным незащищенным сетям (публичным Wi-Fi точкам доступа), не следуя никаким инструкциям. Все это создает серьезные бреши в безопасности, которые могут быть использованы злоумышленниками. Кроме того, сотрудники могут не иметь необходимых средств защиты, например антивирусной защиты, на своих мобильных устройствах. Таким образом, что они более уязвимы для атак.

Смешивание личных и бизнес-данных. Одной из наиболее очевидных проблем безопасности *BYOD* является хранение корпоративных и персональных данных на одном устройстве. В конечном итоге с высокой долей вероятности данные, предназначенные для персонального пользования, станут доступными для мониторинга работодателю, следовательно, эти данные нужно правильно обрабатывать и обеспечивать их безопасность. В самом худшем случае среди этих данных для персонального пользования могут оказаться персональные данные, тогда работодатель в соответствии с местным законодательством может невольно стать оператором персональных данных.

Плохая забота об устройствах. Потеря или кража устройств сотрудника — еще один риск. Более половины нарушений безопасности происходит, когда устройства украдены. Для решения этой проблемы крайне важно, чтобы применялись методы шифрования, обеспечивающие защиту устройства от подобных угроз, и чтобы работодатель побуждал сотрудников использовать пароли и ПИН-коды.

Настройка инфраструктуры — еще один вызов. *BYOD* требует внесения изменений в текущую инфраструктуру, чтобы обеспечить ее соответствие требованиям безопасного применения *BYOD*. Необходимо определить, какие приложения используют сотрудники для взаимодействия с корпоративными данными. Предприятиям необходимо гарантировать, что данные не только защищены, но и соответствуют текущей инфраструктуре. Необходимо провести тестирование на проникновение, чтобы выявить какие-либо уязвимости текущего состояния.

Следует отметить, что перечисленные угрозы и проблемы актуальны для любых мобильных устройств, однако в случае политики *BYOD* из-за меньшего контроля со стороны работодателя, а также большого количества моделей устройств и операционных систем решение подобных проблем представляется более сложным [24] и невозможно за счет использования исключительно методов, применяемых для стационарных АРМ.

В связи с описанными проблемами следует отметить, что внедрение *BYOD* требует проведения определенного набора работ [24]:

- провести полный аудит всей ИС с целью определения, настроена ли инфраструктура на то, чтобы поддержать возможность безопасного устройства мобильных устройств;
- реализовать приемлемые политики и процедуры использования;
- внедрить VPN для защиты канала и предотвращения несанкционированного доступа к ИС;
- использовать специальное ПО управления корпоративной мобильностью (*MDM/EMM*), чтобы отслеживать и обнаруживать риски до того, как они окажут катастрофическое воздействие;
- реализовать возможность удаленного стирания и анализа данных на мобильном устройстве.

Для отраслей с высокими требованиями к ИБ применение стратегии *BYOD* возможно только с ограничениями и тщательным управлением. Устройства должны быть снабжены функциями

безопасности, которые дадут возможность удаленно заблокировать, просмотреть и стереть корпоративные данные, а также должны наблюдаться и обслуживаться. Сотрудники обязаны подписать отказ от претензий, в котором указать, что их работодатель может контролировать их звонки и передачу данных.

Фундаментальная проблема стратегий управления мобильными устройствами, предполагающих использование мобильного устройства в личных и служебных целях, заключается в необходимости четкого разграничения обязанностей и возможностей сотрудника и работодателя. В *BYOD* проблема усложняется тем, что фактически у мобильного устройства имеются два владельца. Как и где провести границу между рабочими задачами и личными? Если дать сотруднику много свободы, то невозможно гарантировать, что сотрудник будет следовать всем указаниям безопасности. Он может отключить систему доверенной загрузки, загрузиться в иную ОС. Нет никакой гарантии того, что сотрудник будет соблюдать все необходимые правила. Должен ли работодатель сам понести данные риски или переложить их на сотрудника? Даже если сотрудник готов принять все ограничения и фактически передать устройство во владение работодателю, а также разрешить мониторинг всех своих данных, возникает еще одна проблема. Компания должна безопасно обрабатывать частные данные сотрудника, и в худшем случае эти данные могут оказаться такими, требования к обработке которых регламентируются местным законодательством. Тогда работодатель должен решать и эту проблему. Можно обязать сотрудника не обрабатывать на его устройстве определенные данные. Система жесткого регулирования и ограниченная *BYOD* могут решить указанные проблемы, но тогда смысл *BYOD* теряется.

Парадигма доверенного сеанса связи и новая гарвардская архитектура

Парадигма доверенного сеанса связи (ДСС) разработана и сформулирована почти десятилетие назад [25—30]. Изначально концепция нашла применение в продукте "Средство обеспечения доверенного сеанса связи (СОДС) МАРШ!" [31]. Имеются примеры успешного использования данной парадигмы [32, 33]. Можно найти примеры схожих подходов [34, 35].

Суть концепции заключается в том, что если нет необходимости в постоянной полноценной комплексной защите средства вычислительной техники (СВТ), нужно создать условия для защищенной работы этого СВТ только на некоторое время, после чего вернуть СВТ в исходное состояние.

Парадигма ДСС является развитием парадигмы доверенных вычислений (ДВ) [25] и наследует многое, из развитого в парадигме доверенной вычислительной среды (ДВС) (см. [36, с. 204]. Для реализации ДВС важно наличие резидентного компонента безопасности (РКБ) (см. [36, с. 205]), который устанавливается в СВТ и обеспечивает возможность создания ДВС. Аналогичный подход применяется и в парадигме ДСС, хотя реализация РКБ несколько иная [15, 37, 38].

На взгляд, автора парадигма ДСС используется для решения узкого круга задач, а нестандартное ее использование для решения новых и нетиповых задач не вошло в практику. Возможно, ключевая проблема заключается в том, что парадигма – это не конечный продукт, а лишь подход к его созданию.

Например, когда поступила определенная критика к продукту, основанному на парадигме ДСС [33], осмысление возражений привело к пониманию, что появилась новая задача, решение которой не предполагалось исходным продуктом. Был сделан вывод, что нужен новый продукт. На основе все той же идеи был создан новый продукт под новую задачу, и все возражения были сняты [33].

Идея новой гарвардской архитектуры [39—41], если и не является развитием парадигмы ДСС, то точно использует идеи, что и находящиеся в основании парадигмы ДСС и восходящие к ДВС. В этом нет ничего удивительного, поскольку базовые идеи доверенных вычислений и идея РКБ были подсказаны теми преимуществами, которые имеет гарвардская архитектура над архитектурой фон-Неймана.

В итоге все указанные парадигмы описывают идею реализации двухконтурных ЭВМ. В данных ЭВМ РКБ гарантирует разграничения между двумя средами. В случае СДЗ — одна среда призвана проверять доверенность другой среды, производя измерения параметров среды и сравнивая их с эталоном [36, 42]. В случае с ДСС среда разграничивается для безопасного удаленного доступа к инфраструктуре и для повседневного использования [25, 26].

Предлагается рассмотреть возможность использования парадигм ДСС и новой гарвардской архитектуры, а также уже разработанных на их базе технологий для решения проблем обеспечения безопасности использования мобильных устройств в рамках стратегий управления *BYOD* и *COPE*.

BYOD и доверенный сеанс связи

Как отмечалось ранее, ключевая проблема безопасности *BYOD* сводится к невозможности в рамках одного устройства, одной вычислительной среды отделить личное от рабочего. Необходимо обеспечить возможность работы с личными и с рабочими данными и при этом учесть интересы работодателя и сотрудника.

Все существующие решения и подходы сводятся к поиску компромисса между контролем со стороны работодателя и свободой сотрудника:

- обеспечить максимальный контроль устройства, его среды и данных на нем, используя организационные меры и технические программные средства (MDM);
- делегировать часть ответственности и обязанностей по обеспечению безопасности сотруднику;
- проводить постоянное обучение сотрудников мерам безопасности;
- грамотная многоуровневая организация системы безопасности инфраструктуры, к которой будет подключаться сотрудник.

Корректная работа средств обеспечения безопасности предполагает наличие доверенной среды на мобильном устройстве. В силу делегирования ответственности и части обязанностей сотруднику в рамках стратегии *BYOD*, в частности по организации доверенной среды, получаем человеческий фактор как одну из основных угроз. Обучение сотрудников не ликвидирует возможность случайных ошибок и злого умысла.

Серьезно ограниченные варианты *BYOD* могут решить проблему человеческого фактора, технически запретив сотруднику многое, в том числе менять ОС на своем устройстве, ставить обновления не из одобренных работодателем источников. В таком случае сотрудник остается владельцем устройства только юридически и основная идея *BYOD* (возможность работы на своем устройстве с личными и рабочими данными) почти полностью компрометируется.

Однако основную проблему *BYOD* можно решить и по-другому. Вместо модификации вычислительной среды сотрудника и поддержки ее в безопасном состоянии для выполнения рабочих и личных задач можно установить в устройство сотрудника дополнительную среду (стандартную для работодателя) и РКБ, обеспечивающий безопасность данной среды и возможность ее загрузки по необходимости. На стороне ИС нужно организовать возможность подключения только из доверенной среды. Подобный подход уже был использован для задач обеспечения безопасного удаленного доступа [43].

Общий подход к организации взаимодействия будет следующим. Сотрудник приносит свое устройство: планшет, ноутбук или мобильный телефон. Отдел ИТ или ИБ производит установку и настройку РКБ в устройстве сотрудника. Подготавливаются необходимые данные для подключения к ИС, настраивается рабочая среда, производится регистрация среды и учетных данных в системе управления доступом ИС. Задача РКБ — изолировать предназначенную для работы среду от среды для персонального пользования. В задачу РКБ также входит нейтрализация актуальных для работодателя угроз. Когда мобильное устройство сотрудника должно быть лишено возможности работать с корпоративной ИС, учетные данные блокируются, а РКБ извлекается из устройства сотрудника.

Реализации РКБ в приведенном сценарии можно использовать такие же, как в уже существующих решениях. Для планшетов с возможностью загрузки с внешнего устройства можно использовать подход, который был применен для организации ДСС на планшете DELL [44].

Используя технологию, лежащую в основе аппаратной составляющей СОДС МАРШ!, можно создать вариант РКБ, удовлетворяющий всем актуальным для модели угроз работодателя требованиям к безопасности мобильного устройства [20, 43]. Данный РКБ возможно использовать на любых ноутбуках или планшетах, поддерживающих загрузку с внешних устройств.

Еще одним вариантом РКБ для ноутбуков может послужить решение, выполненное на основе платы расширения, аппаратной составляющей продукта Аккорд-АМДЗ. Подобное решение используется в продукте "Ноутбук руководителя" [45]. Процедуру подготовки ноутбука руководителя также можно адаптировать в процедуру подготовки мобильных устройств в рамках *BYOD*.

Следует отметить, что для мобильных телефонов можно использовать те же схемы, что были предложены для ноутбуков и планшетов, однако примеров реализаций подходящих РКБ, которые можно было бы установить на смартфон, пока нет. Вместе с тем реализация подобного РКБ является выполнимой задачей.

Применение парадигмы ДСС для обеспечения безопасности мобильных устройств в политике *BYOD* дает решение, которое обладает следующими плюсами:

- простой способ подготовки мобильного устройства;

- разделение среды для работы и личного пользования с помощью РКБ;
- отсутствие необходимости поиска компромиссов между личным и рабочим;
- гарантированное создание доверенной среды на устройстве;
- перенос ответственности с пользователя на РКБ;
- возможность для пользователя использовать свою вычислительную среду.

Следует отметить, что реализацию РКБ и доверенной среды для рабочих задач необходимо проверять на совместимость с устройством сотрудника и в случае несовместимости либо модифицировать РКБ или рабочую среду для поддержания совместимости, либо отказывать сотруднику в возможности использовать данное устройство.

Приведенный подход также применим и к *COPE*. Однако для *COPE* особый интерес представляют устройства, реализующие концепцию "новой гарвардской архитектуры" [39—41, 46]. В рамках *COPE* у работодателя есть возможность выбора устройств. Он может приобрести устройство с динамической архитектурой. В состав устройств с динамической архитектурой уже входит необходимый РКБ. Приобретая подобное устройство, не нужно прилагать дополнительных усилий на встраивание РКБ.

Таким образом, используя технологии, разработанные в рамках концепций ДСС и "новая гарвардская архитектура", можно решить проблему обеспечения безопасности мобильных устройств в стратегиях управления *BYOD* и *COPE* не перекладывая ответственность на сотрудника и излишне не усложняя процедуру управления.

Литература

1. *Ghosh A. K., Swaminatha T. M.* Software Security and Privacy Risks in Mobile E-commerce // Communications of the ACM. 2001. V. 44. №. 2. P. 51—57.
2. *Tagoe F. T., Sharif M. S.* The Future of Enterprise Security with Regards to Mobile Technology and Applications: International Conference on Global Security, Safety, and Sustainability. – Springer, Cham, 2017. P. 321—330.
3. *Ghosh A., Gajar P. K., Rai S.* Bring your own device (BYOD): Security risks and mitigating strategies // Global Research in Computer Sci. 2013. V. 4. №. 4. P. 62—70.
4. Mobile Device Management Software — ManageEngine Mobile Device Manager Plus [Электронный ресурс]. URL:https://www.manageengine.com/mobile-device-management/ (дата обращения: 24.04.2017).
5. SimpleMDM [Электронный ресурс]. URL: http://www.capterra.com/mobile-device-management-software/spotlight/149414/SimpleMDM/SimpleMDM (дата обращения: 10.04.2017).
6. SureMDM [Электронный ресурс]. URL: http://www.capterra.com/mobile-device-management-software/spotlight/154149/SureMDM/42Gears%20Mobility%20Systems (дата обращения: 26.04.2017).
7. *Джон Х.* Обеспечение безопасности мобильных устройств с помощью MDM 2008 SP1 // WINDOWS IT PRO/RE. 2010. № 11. С. 25—33.
8. *Михайлов Д. М., Жуков И. Ю., Ивашко А. М.* Защита мобильных телефонов от атак. — М.: Фойлис. 2011. С. 8—10.
9. *Ватутин А.* Mobile Device Management. Управление жизненным циклом мобильных устройств [Электронный ресурс]. URL: http://library. croc. ru/download/4914/16a48de7ae24c493a445d3c60aa79e15. Pdf (дата обращения 05.02.2017).
10. *Jaramillo D. et al*. Cooperative Solutions for Bring your own Device (BYOD) // IBM J. Research and Development. 2013. V. 57. № 6. P. 5:1—5:11.
11. Ten rules for Bring Your Own Device (BYOD) [Электронный ресурс]. //URL: https://www-01.ibm.com/ marketing/iwm/dre/signup?source=urx-14836&S_PKG=ov37871&disableCookie=Yes (дата обращения: 20.04.2017).
12. *Bhandari B.* Analysis of market trends in mobility and possible next steps. 2017.
13. *Morrow B.* BYOD Security Challenges: Control and Protect Your Most Sensitive Data // Network Security. 2012. V. 2012. № 12. P. 5—8.
14. *Minnaar A.* Cybercrime, Cyberattacks, and Problems of Implementing Organizational Cybersecurity: Global Issues in Contemporary Policing. — CRC Press, 2017. P. 121—138.
15. *Конявский В. А.* ДБО – как сделать это безопасным. Ч. II // Информационная безопасность. 2012. № 3. С. 8—9.
16. *Конявский В. А*. ДБО — как сделать это безопасным // Информационная безопасность. 2012. № 2. С. 32—33.
17. *Конявский В. А.* Серебряная пуля для хакера (окончание) // Защита информации. Инсайд. 2013. № 5. С. 69—73.
18. *Конявский В. А.* Серебряная пуля для хакера // Защита информации. Инсайд. 2013. № 4. С. 54—56.
19. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
20. *Конявский В. А.* Организация безопасного ДБО на основе СОДС «МАРШ!» // Национальный банковский журнал. 2011. № 9. С. 88, 89.
21. *Акаткин Ю. М., Конявский В. А.* Безопасный доступ к корпоративным облачным приложениям // Информационная безопасность. 2014. № 1. С. 23.
22. *Конявская С. В.* Ответьте центру! //Information Security/Информационная безопасность. 2010. № 6. С. 47.
23. *Friedman J., Hoffman D. V.* Protecting Data on Mobile Devices: A Taxonomy of Security Threats to Mobile Computing and Review of Applicable Defenses // Information Knowledge Systems Management. 2008. V. 7. № 1, 2. P. 159—180.
24. *Vorakulpipat C. et al.* A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives // Security and Communication Networks. 2017. V. 2017.
25. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ!: мат. XV Межд. научно-практической конф. "Комплексная защита информации". Иркутск (Россия). 1–4 июня 2010 г. — М., 2010.

26. *Каннер А. М.* Средство организации доверенного сеанса как альтернатива доверенной вычислительной среде // Информационные технологии управления в социально-экономических системах. 2010. Вып. 4. С. 140—143.

27. *Чугринов А. В.* Доверенные сеансы связи и средства их обеспечения // Информационная безопасность. 2010. № 4. С. 54—55.

28. Съемный носитель информации. Патент на полезную модель № 102139. Опубл. 10.02.2011. Бюл. № 4.

29. Съемный носитель информации с безопасным управлением доступом. Патент на полезную модель № 123571. Опубл. 27.12.2012. Бюл. № 36.

30. Съемный носитель информации на основе энергонезависимой памяти с расширенным набором функций информационной безопасности. Патент на полезную модель № 130441. Опубл. 20.07.2013. Бюл. № 20.

31. Сайт программно-аппаратного комплекса «Средство обеспечения доверенного сеанса "МАРШ!"» [Электронный ресурс]. URL: http://www.sodsmarsh.ru (дата обращения: 20.04.2017).

32. "МАРШ!" в защиту персональных данных // Уездный доктор. Апрель 2013. С. 20—21.

33. Совещание по итогам эксплуатации СОДС "МАРШ!" в образовательных организациях [Электронный ресурс]. URL: http://www.temocenter.ru/o-nas/info/novosti/106-soveshchanie-po-itogam-ekspluatatsii-sods-marsh-v-obrazovatelnykh-organizatsiyakh.html (дата обращения: 20.04.2017).

34. СПДС "ПОСТ" [Электронный ресурс]. URL: http://www.s-terra.com/products/productline/post (дата обращения: 20.04.2017).

35. Электронная подпись в доверенной среде на базе загрузочной Ubuntu 14.04 LTS и Рутокен ЭЦП Flash [Электронный ресурс]. URL: http://habrahabr.ru/company/aktiv-company/blog/253619/ (дата обращения: 20.04.2017).

36. *Конявский, В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией: библиотека журнала «УЗИ»: Кн. 2. — Мн.: Беллитфонд, 2004. — 282 с.

37. *Счастный Д. Ю.* M&M! — платформа для защищенных мобильных систем: мат. XXI Научно-практической конф. "Комплексная защита информации". Смоленск, 17—19 мая 2016 г. — М., 2016. С. 58—60.

38. *Конявская С. В., Кравец В. В.* Защищенное ДБО: несколько слов о самых популярных возражениях // Информационная безопасность. 2014. № 2. С. 22—23.

39. *Конявский В. А.* "Доверенная гарвардская" архитектура – компьютер с динамически изменяемой архитектурой: // мат. XX Научно-практической конф. "Комплексная защита информации". Минск, 19—21 мая 2015 г. — Минск: РИВШ, 2015. С. 32—37.

40. *Конявская С. В.* Планшет: служебный, защищенный, отечественный // Информационные технологии, связи и защита информации МЧС России — 2015. 2015. С. 186.

41. *Конявский В. А.* Защищенный микрокомпьютер МК-TRUST — новое решение для ДБО // Национальный банковский журнал. 2014. № 3. С. 105.

42. *Алтухов А. А.* Концепция персонального устройства контроля целостности вычислительной среды // Вопросы защиты информации, 2014. № 4. С. 64—68.

43. *Алтухов А. А.* Доверенный сеанс связи на службе академического процесса: Сб. научных статей XII Межд. научно-технической конф. "Новые информационные технологии и системы", г. Пенза 23—25 ноября 2016 г., С. 217—219.

44. *Кравец В. В.* Доверенная вычислительная среда на планшетах Dell. "МАРШ!" // Вопросы защиты информации. 2014. № 4. С. 32—33.

45. *Счастный Д. Ю.* Ноутбук руководителя // мат. XX Научно-практической конф. "Комплексная защита информации". Минск, 19—21 мая 2015 г. — Минск: РИВШ, 2015. С. 112—113.

46. *Конявская С. В.* Про ДБО и планшеты // Национальный банковский журнал. 2014. № 10. С. 101.

The trusted communication sessions concept as method of mobile device safe use in the enterprise

A. A. Altukhov
Closed Joint Stock Company "OKB SAPR", Moscow, Russia
Moscow Institute of Physics and Technology (state university), Dolgoprudny, Moscow region, Russia
National Research Nuclear University "MEPhI", Moscow, Russia

The paper discusses strategies for managing mobile devices and the arising issues of information security. A way of using the trusted communication session paradigm is proposed to solve the problem of secure use of BYOD and of COPE mobile devices.

Keywords: mobile device management strategies, BYOD, COPE, COBO, trusted session, new Harvard architecture, trusted computing, cell phone security, information security, mobile device security, mobility, remote access, smartphone security, tablet security.

Bibliography — 46 references. *Received June 5, 2017*