Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СТРАТЕГИИ УПРАВЛЕНИЯ УСТРОЙСТВАМИ И ДОВЕРЕННЫЙ СЕАНС СВЯЗИ. ТОЧКИ СОПРИКОСНОВЕНИЯ

А.А. АЛТУХОВ

Национальный исследовательский ядерный университет «МИФИ»

Применение мобильных устройств для выполнения рабочих обязанностей становиться 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. На настоящий момент существует несколько стратегий управления мобильными устройствами. Каждая из них требует применения специальных методов по обеспечению безопасности.

Ниже будет показано, что обеспечение должного уровня защищённости оконечных мобильных устройств (*endpoint devices*) является необходимым условием безопасной реализации стратегии обеспечения мобильности предприятия.

В данной работе 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.

В первой части работы подробно будет рассмотрены существующие политики управления устройствами, укажем их плюсы и минусы. Во второй части работы будет сделан обзор методов защиты. В третьей будет сделан краткий обзор парадигмы ДСС и концепции Новой Гарвардской Архитектуры. В заключительной части будет показано, каким образом существующие решения и подходы в рамках парадигмы ДСС можно использовать для безопасного использования мобильных устройствами в рамках конкретных стратегий управления.

Стратегии управления устройствами.

На настоящий момент времени можно выделить три основных стратегии управления 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 выдаёт в пользование сотруднику мобильное устройство исключительно для выполнения рабочих задач. Плюсы подобной схемы заключаются в простоте управления для работодателя. Возможность выстроить грамотную и чёткую систему управления позволяет легко реализовать безопасность подобных устройств. При таком подходе все методы и стратегии, применяемые к стационарным автоматизированным рабочим местам (АРМ)[1], 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[2]. 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, использование определённого 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 обозначением *COPE* будет разуметь оба подхода: обычную стратегию *COPE* и расширенный вариант *COPE/COYD*.

COPE является развитием классической *COBO*, в рамках которого 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 даруется 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[3]. Компания IBM выделяет четыре базовых 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.

---

[1] В дальнейшем будем называть такие подходы и методы классическими подходами.

[2] Последнее ему может быть и не нужно.

[3] Данное утверждение верно и для *COPE*, но для *BYOD* это явно фиксируется в литературе.

Долгое время *BYOD* являлся 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 остудили пыл. Хотя число активных призывов к использованию данной стратегии уменьшилось, но бизнес по-прежнему жаждет её использовать [12].

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

Гибридные стратегии также существуют. Немногие работодатели будут использовать одну конкретную стратегию. Возможны применения различные 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 использование для персональных нужд будет никак не ограниченно. С формальной точки зрения отличия *COPE* от *BYOD* заключается только в том, кто владелец устройства де-юре. В зависимости от того, является ли владельцем работодатель (*COPE*) или сотрудник (*BYOD*), по-разному выстраивается взаимодействие работодателя и подчинённого. В случае *BYOD* работает запретительный подход для сотрудника со стороны работодателя. В случай *COPE* - разрешительный подход. Все это позволяет утверждать, что большая часть угроз безопасности, проблем управления одинаковы 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 сводиться к клиент-серверной модели.

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

Необходимыми условиями доверенности оконечного устройства является защита от воздействия вредоносного кода и несанкционированного доступа [19], что можно обеспечить следующими способами [Там же]:

доверенная загрузка ОС;

защита информации от НСД;

разграничение доступа к ресурсам;

антивирусная защита;

Способы организации доверенного сетевого соединения [15–16; 20–22]:

криптозащита трафика или

физическая изолированность от сетей общего пользования при расположении в контролируемой зоне.

Поскольку мобильное устройство может покидать периметр организации и не привязано к конкретному месту, то 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 уст-

ройства 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 серьёзных правовых, технических или организационных проблем для данной стратегии управления мобильными устройствами не возникает. Жизненный цикл устройства достаточно простой и не зависит от сотрудника. Все необходимые процедуры до передачи сотруднику, во время эксплуатации устройства и после завершения эксплуатации, можно чётко регламентировать.

Применяемые подходы для *COPE* во многом не отличаются от *COBO*. Большая часть угроз и методов их нейтрализации такие 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 и их перечень может расширяться в процессе работы. Также обговариваются действия, которые могут осуществлять работодатель и сотрудник над данными, которые будут получены в рамках персональной работы. Для компаний с высокими требованиями к ИБ данные, полученные в результате персональной деятельности, подвергаются аудиту со стороны работодателя. Данная 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 заранее может 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 данных, 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 счёт возможности строго контроля данные угрозы просто локализовать и нейтрализовать.

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

Приведём пять основных проблем безопасности, возникающие 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 устрой-

ствами, 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 незащищённым сетям (публичным Wi-Fi точкам доступа), не следуя никаким инструкциям. Все это создаёт серьёзные бреши в безопасности, которые могут быть использованы злоумышленниками. Все это в сочетании с тем фактом, что сотрудники могут не иметь необходимых средств защиты, например, антивирусной защиты, на своих мобильных устройствах, означает, 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 доступны для мониторинга работодателю и это означает, что 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 ещё 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 – ещё один вызов. *BYOD* требует внесения изменений в текущую инфраструктуру, чтобы обеспечить её 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 вышеприведённые 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 вышеописанными проблемами следует отметить, что внедрение *BYOD* требует проведения определённого набора работ [там же]:

провести полный аудит всей ИС, чтобы определить, настроена ли инфраструктура, 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 удалённого 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 удалённо 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 чёткого разграничения обязанностей и возможностей сотрудника и работодателя. В *BYOD* проблема усложняется тем, что фактически у мобильного устройства два владельца. Как и где провести границу между рабочими задачами и личными? Если дать сотруднику много свободы, то как гарантировать то, что сотрудник будет следовать всем указаниям безопасности? Что если он отключит систему доверенной загрузки, загрузиться в иную ОС? Нет никакой гарантии того, что сотрудник будет соблюдать все необходимые правила. Кто должен понести данные риски, работодатель? Должен ли он переложить данные риски на сотрудника? Даже если сотрудник готов принять все ограничения и де-факто передать устройство во владение работодателю, а также разрешит мониторинг всех своих данных, то возникает еще одна проблема. Компания должна безопасно обрабатывать частные данные сотрудника и в худшем случае эти данные могут оказаться такими, требования к обработки которых регламентируются местным законодательством. В этом случае работодатель должен решать и эту проблему. Можно обязать сотрудника не обрабатывать на его устройстве определённых данных. Система жёсткого регулирования и ограниченная *BYOD* могут решить проблемы, но тогда и смысл *BYOD* теряется.

Парадигма Доверенного сеанса связи и Новая гарвардская архитектура.

Парадигма ДСС разработана и сформулирована вот уже почти как десятилетие назад [25–30]. Изначально концепция нашла применение в продукте Средство Обеспечения Доверенного Сеанса Связи (СОДС) МАРШ! [31]. Есть 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 и комплексной защите средства вычислительной техники (СВТ), нужно создать условия для защищённой работы этого СВТ только на некоторое время. После вернуть СВТ в исходное состояние.

Парадигма ДСС является развитием парадигмы доверенных вычислений (ДВ) [25] и наследует многое, что было развито в парадигме доверенной вычислительной среды (ДВС) [36, С. 204]. Для реализации ДВС важно наличие резидентного компонента безопасности (РКБ) [Там же, С. 205], который устанавливается в СВТ и обеспечивается возможность создать ДВС. Аналогичный подход применяется и в парадигме ДСС, хотя реализация РКБ несколько иная [15, 37].

На настоящий момент, на мой взгляд, парадигма ДСС используется для решения узкого круга задач, а нестандартное её 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 созданию оного.

Например, когда поступила определённая 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. Используя все ту же идею, был создан новый продукт под новую задачу, и все возражения были сняты [Там же].

Идея новой гарвардской архитектуры [39-41], если и не является развитием парадигмы ДСС, то точно использует те же идеи, которые находятся в основании парадигмы ДСС и восходят к ДВС. В этом нет ничего удивительного, если принять во внимание, что базовые идеи доверенных вычислений и идея РКБ были вдохновлены теми преимуществами, которые имеет гарвардская архитектура, над архитектурой фон-Неймана.

В итоге все выше приведённые парадигмы описываются 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, мы разграничиваем среду для безопасного удалённого 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* сводиться к невозможности в рамках одного устройства, одной вычислительной среды отделить личное от рабочего. Как 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 для сотрудника:

Обеспечить максимальный контроль устройства, его среды и данных на нём используя организационные меры и технические программные средства (MDM);

Делегировать часть ответственности и обязанностей по обеспечению безопасности сотруднику;

Проводить постоянное обучение сотрудников мера 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.

Серьёзно ограниченные варианты *BYOD* могут решить проблему человеческого фактора, технически запретив сотруднику многое, в том числе возможность менять ОС на своём устройстве, ставить обновления не из одобренных работодателем источников. В таком случае сотрудник остаётся, владельцем устройства только де-юре и основная идея *BYOD* (возможность работы на своём 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 её 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 её загрузки по необходимости. На стороне ИС нужно организовать возможность подключения только из доверенной среды. Подобный подход уже был использован для задач обеспечения безопасного удалённого доступа [43].

Общий подход к организации взаимодействия будет следующим. Сотрудник приносит своё 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 учётных 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, то учётные данные блокируются, а РКБ извлекается из устройства сотрудника.

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

Используя технологию, лежащую в основе аппаратной составляющей СОДС МАРШ! возможно 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.

Ещё 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 выше для ноутбуков и планшетов, однако на настоящий момент нет примеров реализаций, подходящих РКБ, которые можно было бы установить на смартфон. Однако реализация подобного РКБ является выполнимой задачей.

Применение парадигмы ДСС для обеспечения безопасности мобильных устройств в политике BYOD даёт 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 рабочею среду для поддержания совместимости, либо отказывать сотруднику в возможности использовать данное устройство.

Выше приведённый подход также применим и к *COPE*. Однако для *COPE* особый интерес представляют устройства, реализующие концепцию «Новой Гарвардской архитектуры» [39, 40, 41, 46]. В рамках *COPE* у работодателя есть возможность выбора устройств. Он может приобрести устройство с динамической архитектурой. В состав подобных устройств с динамической архитектурой уже входит необходимый РКБ. Приобретая подобное устройство, не нужно тратить 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.

Список литературы

1. *Ghosh A. K., Swaminatha T. M.* Software security and privacy risks in mobile e-commerce //Communications of the ACM. – 2001. – Т. 44. – №. 2. – С. 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. – С. 321-330.
3. *Ghosh A., Gajar P. K., Rai S.* Bring your own device (BYOD): Security risks and mitigating strategies //Journal of Global Research in Computer Science. – 2013. – Т. 4. – №. 4. – С. 62-70.
4. Mobile Device Management Software - ManageEngine Mobile Device Manager Plus [Электронный ресурс]. URL:https://www.manageengine.com/mobile-device-management/ (дата обращения: 24.04.17).
5. SimpleMDM [Электронный ресурс]. //URL:http://www.capterra.com/mobile-device-management-software/spotlight/149414/SimpleMDM/SimpleMDM (дата обращения: 10.04.17).
6. SureMDM [Электронный ресурс]. //URL:http://www.capterra.com/mobile-device-management-software/spotlight/154149/SureMDM/42Gears%20Mobility%20Systems (дата обращения: 26.04.17).
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 05.02.17).
10. *Jaramillo D. et al*. Cooperative solutions for bring your own device (BYOD) //IBM journal of research and development. – 2013. – Т. 57. – №. 6. – С. 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: 20.04.17).
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. – Т. 2012. – №. 12. – С. 5-8.
14. *Minnaar A.* Cybercrime, Cyberattacks, and Problems of Implementing Organizational Cybersecurity //Global Issues in Contemporary Policing. – CRC Press, 2017. – С. 121-138.
15. *Конявский В. А.* ДБО – как сделать это безопасным. Часть II //Информационная безопасность. — М., 2012. № 3. С. 8—9.
16. *Конявский В. А.* ДБО – как сделать это безопасным //Информационная безопасность. — М., 2012. N 2. С. 32—33.
17. *Конявский В. А.* Серебряная пуля для хакера (Окончание) //Защита информации. Инсайд. — СПб., 2013. № 5. С. 69-73.
18. *Конявский В. А.* Серебряная пуля для хакера //Защита информации. Инсайд. — СПб., 2013. № 4. С. 54-56.
19. Об утверждении требований о защите информации, не составляющей государсвенную тайну, содержащейся в государсвенных информационных системах: приказ ФСТЭК России от 11 февраяля 2013 г. N17.
20. *Конявский В. А.* Организация безопасного ДБО на основе СОДС «МАРШ!» // Национальный банковский журнал.— М., 2011. № 9. С.
21. *Акаткин Ю. М., Конявский В. А.* Безопасный доступ к корпоративным облачным приложениям. //Information Security/Информационная безопасность. — М., 2014. № 1. С. 23.
22. *Конявская С. В.* Ответьте центру! //Information Security/Информационная безопасность. —М., 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. – Т. 7. – №. 1, 2. – С. 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. – Т. 2017.

25. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем – на старт, внимание, МАРШ! // Комплексная защита информации. Материалы XV международной научно-практической конференции (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. Вып. 4. М., 2010. С. 140–143.

27. *Чугринов А. В.* Доверенные сеансы связи и средства их обеспечения // Information Security/Информационная безопасность. 2010. № 4 (август-сентябрь). С. 54–55.

28. Съемный носитель информации. Патент на полезную модель № 102139. 10.02.2011, бюл. № 4.

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

30. Съемный носитель информации на основе энергонезависимой памяти с расширенным набором функций информационной безопасности. Патент на полезную модель № 130441. 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 //Комплексная защита информации: материалы XXI научно-практической конференции, 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 //Information Security/Информационная безопасность. М., 2014. № 2. С. 22-23.

39. *Конявский В. А.* «Доверенная гарвардская» архитектура – компьютер с динамически изменяемой архитектурой. //Комплексная защита информации. Материалы XX научно-практической конференции. 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. М., 2015. С. 186.

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

42. *Алтухов А. А.* Концепция персонального устройства контроля целостности вычислительной среды //Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ», 2014. Вып. 4 (107). С. 64-68.

43. *Алтухов А. А.* Доверенный сеанс связи на службе академического процесса //Новые Информационные Технологии и Системы, Сборник научных статей XII Международной научно-технической конференции г. Пенза 23-25 ноября 2016г., С. 217-219.

44. *Кравец В. В.* Доверенная вычислительная среда на планшетах Dell. «МАРШ!» //Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ», 2014. Вып. 4 (107). С. 32-33.

45. *Счастный Д. Ю.* Ноутбук руководителя //Комплексная защита информации. Материалы XX научно-практической конференции. Минск, 19-21 мая 2015 г. – Минск: РИВШ, 2015. С. 112-113.

46. *Конявская С. В.* Про ДБО и планшеты //Национальный Банковский Журнал. М., 2014. № 10 (октябрь). С. 101.

ПАРАДИГМА БЕЗОПАСНОСТИ ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

В.А. АРТАМОНОВ

МНОО «Международная академия информационных технологий»

Технология «Облачные вычисления» появилась в информационной терминологии относительно недавно. Термин «Облачные вычисления» («Cloud Computing») начал применяться с конца 2007 - начала 2008 года, постепенно вытесняя понятие «Грид-вычисления» («Grid Computing»), фактически придя ему на смену. Одной из первых компаний, давших миру данный термин, стала компания IBM, развернувшая в начале 2008 года проект «Blue Cloud» и спонсировавшая Европейский проект «Joint Research Initiative for Cloud Computing». Метафорический образ «облако» уже давно используется специалистами в области сетевых технологий для изображения на сетевых диаграммах сложной вычислительной инфраструктуры (или же Интернета как такового), скрывающей свою внутреннюю организацию за определенным интерфейсом**.** Не задерживаясь на множестве определений, отражающих различные точки зрения и акценты авторов на эту информационную технологию (ИТ), остановимся на двух, которые отражают национальную стандартизацию данного понятия в общем контексте семантических отношений ИТ.

Национальный институт стандартов и технологий (НИСТ) США, 2011: *Облачные вычисления – информационно-технологическая концепция, подразумевающая обеспечение повсеместного и удобного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру.*

Минкомсвязи РФ (опубликовано на Федеральном портале нормативных правовых актов), **2016**: *Облачные вычисления – информационные технологии, включающие в том числе государственную инфраструктуру облачных вычислений, обеспечивающие дистанционную обработку данных более чем одной информационной системой.* Отметим сразу, что это определение, достаточно радикальное и на наш взгляд вполне адекватное по сути, принципиальным образом отличается от общепринятого понимания облачных вычислений, под которыми подразумеваются не технологии, а модель взаимоотношений между поставщиком и потребителем ИТ.

Облачные вычисления обеспечивают практически неограниченную мощность, устраняя проблемы масштабируемости и открывают доступ к программным и аппаратным активам, которые большинство пользователей не могли бы себе позволить. В том числе, разработчики приложений, используя управляемые через Интернет облачные вы-