**УДК 004.9**

**Д.К. Дедович[1], М.Н. Евдокименко[1], М.С. Журавлев[1],**
**В.Л. Николаенко[3], Г.В. Сечко[3], Т.Г. Таболич[2]**

# АНАЛИЗ МЕТОДОВ БОРЬБЫ С УГРОЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СЛУЖЕБНЫХ ГАДЖЕТОВ МАЛОГО БЕЛОРУССКОГО ПРЕДПРИЯТИЯ

[1]Общество с ограниченной ответственностью «Стрим центр» (Минск)
[2]БелНИИТ «Транстехника» (Минск)
[3]Белорусский государственный университет информатики и радиоэлектроники(Минск)

Проводится анализ и сравнение методов борьбы с угрозами информационной безопасности относительно малого по меркам Беларуси предприятия (100-150 работающих), выдающего своим сотрудникам служебные гаджеты. Рассматриваются современные запатентованные зарубежные решения. Предлагаются рекомендации по выбору таких методов для малого белорусского предприятия.

***Ключевые слова:*** служебный гаджет, информационная безопасность, предприятие, зарубежный патент, мобильное облако, Республика Беларусь.

**Вводная часть. Постановка задачи**

Новейший американский патент 2018 года [1], правообладателем которого является International Business Machines Corporation, в своем описании констатирует: «… Предприятия поощряют использование мобильных смартфонов на рабочем месте для повышения производительности. В первом варианте сотрудники покупают свои собственные смартфоны и устанавливают корпоративное программное обеспечение на телефоны, чтобы повысить производительность. Однако во многих отраслях промышленности, например, в сфере финансов и обороны, работникам предоставляются стандартизированные смартфоны *из-за проблем безопасности.* Эти стандартизированные смартфоны «заблокированы» и имеют ограниченную функциональность. Например, на этих устройствах отключены порты универсальной последовательной шины (USB), веб-браузер javascript и обновления программного обеспечения на популярных торговых площадках (iTunes, Android). Можно установить только корпоративные приложения с защищенного портала».

В американском патенте 2018 года [2], правообладателем которого является United Parcel Service of America, Inc., в описании сообщается похожая информация: «…Предприятия могут предоставлять сотрудникам портативные устройства (например, в соответствии с [1] портативные компьютеры, планшетные компьютеры, сотовые телефоны и смартфоны, в том числе платформы для смартфонов на базе Android и iPhone, которые коммерчески доступны от Apple Incorporated, Купертино, Калифорния) для сбора информации о местонахождении и деятельности сотрудников в зависимости от времени. Компьютерные системы также могут использоваться для отслеживания активности сотрудников независимо от местоположения (например, системы с программным обеспечением для хранения времени, используемые в офисных средах, производственные системы, используемые на заводах для отслеживания и управления производственным процессом и др.».

Следует отметить однако, что предоставление отдельного заблокированного телефона каждому сотруднику имеет ряд недостатков как для сотрудников, так и для предприятий или учреждений. Например [1], пользователи разочарованы тем, что телефоны не являются полностью функциональными и не могут использоваться для личного пользования, что побуждает некоторых пользователей носить с собой два телефона – один для бизнеса и второй для личного пользования. Кроме того, предприятия, предоставляющие эти телефоны, несут как капитальные, так и эксплуатационные расходы от поддержки работы этих телефонов.

Тем не менее, в [3] и [4] содержится информация о том, что наиболее состоятельные учреждения разных стран уже выдают своим сотрудникам служебные гаджеты. Например, полицейские Нью-Йорка бесплатно получили[3]в феврале 2018 года новые смартфоны модели iPhone 7 и iPhone 7 Plus. В 2017 году было куплено [4] 15000 гаджетов для «Почты России».

Таким образом, как следует из [1-4], выдача предприятиями и учреждениями служебных гаджетов (портативных компьютеров, сотовых телефонов и гаджетов других видов) своим сотрудникам становится все более массовым явлением в мире. Цель этой выдачи – отслеживания активности сотрудников, сбор информации о местонахождении и деятельности сотрудников[2], повышение оперативности работы полицейских при появлении их на месте преступления до получения вызова от диспетчера[3], повышение производительности труда сотрудников[1, 4], а также почти во всех случаях выдачи – обеспечение информационной безопасности предприятия или учреждения.

Вопросы информационной безопасности предприятия, выдающего своим сотрудникам служебные гаджеты, впервые были поставлены в [5] в первой половине 2010-х годов (мнение Эндрю Хуга (AndrewHoog), генерального директора одной из ведущих в мире по вопросам информационной безопасности мобильных приложений американской компании «Now Secure». В [5], в частности, Эндрю Хуг пишет: «Специалисты по информационной безопасности должны … начать разрабатывать проактивные стратегии для борьбы со всем *разнообразием угроз*, представляемых мобильными устройствами».

В этих условиях целью настоящей работы является анализ и сравнение методов борьбы с угрозами информационной безопасности и разработка рекомендацийпо выбору таких методов для относительно небольшого по меркам Беларуси предприятия (100-150 работающих), выдающего своим сотрудникам служебные гаджеты.

**Теоретический анализ**

Патенты [1, 2] сходятся на том, что для защиты информации в служебных гаджетах необходимы виртуальные среды и программные гипервизоры. В [2], например, предлагается способ защиты конфиденциальной информации компании в служебном гаджете с программным гипервизором. Владелец служебного гаджета при использовании этого способа может получить доступ к ресурсам компании из любого географического местоположения, используя любой компьютер компании и / или ее сеть. Способ включает в себя 1) запрос пользователем недоверенной [6] виртуальной машины, выполняемой процессором гаджета, на установку соединения с удаленным компьютером или сетью компании, 3) запуск управляющей виртуальной машины гаджета в ответ на запрос и соединение после этого гаджета с компьютером или сетью компании. Способ обеспечивается установкой гипервизора на каждый мобильный телефон. Однако такой подход, по мнению [1], требует сотрудничества как производителей мобильных устройств, так и поставщиков услуг, которые жестко контролируют телефоны.

Для устранения этого недостатка в [1] предлагается *виртуализация в мобильном облаке*, которая, по мнению [1], если она выполнена правильно, может решить большинство проблем безопасности. При этом в [1] оговаривается, что виртуализация не защитит гаджет, в котором злоумышленник до виртуализации установил каким-либо образом вредоносное ПО (rootkit; в [1] для этого используется фраза «руткит работает ниже уровня гипервизора (but notwhen a rootkit operates below the hyper visor layer)»).

Виртуализация по патенту [1] предлагает 4 составные части способа защиты смартфона, которые объединены, чтобы обеспечить безопасный доступ к образам мобильного телефона, работающим в облаке. К этим частям относятся:

1) запуск образ мобильного устройства в мобильном облаке, которое может быть расположено, например, в базовых станциях, контроллере радиосети (RNC) или базовой сети;

2) использование протокола отображения, аналогичного архитектуре независимых вычислений Citrix (ICA) или протоколу удаленного рабочего стола Microsoft (RDP), который мо-

жет использоваться сотрудниками для доступа к виртуализированному образу со своих смартфонов;

3) наличие скремблера и дескремблера, которые шифруют и дешифруют данные, поступающие в виртуальный образ и обратно на смартфон;

4) использование защелкивающегося дисплея (Lockscreen, экран блокировки смартфона, который нужен, чтобы избежать случайных нажатий в ждущем режиме).

На рисунке, приведенном ниже, показана блок-схема последовательности операций, иллюстрирующая вариант осуществления способа для безопасной виртуализации мобильного сотового устройства согласно [1].

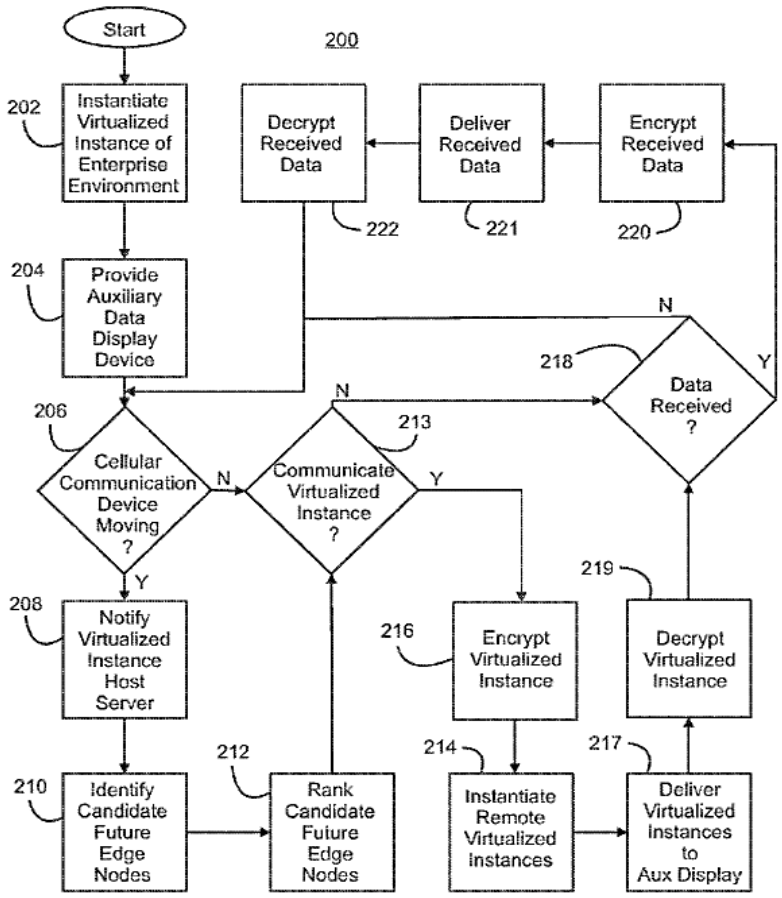


Рис.1. Блок-схема последовательности операций, иллюстрирующая вариант осуществления способа для безопасной виртуализации мобильного сотового устройства согласно [1]

На наш взгляд, безопасная виртуализация мобильного сотового устройства (служебного гаджета) согласно [1] приемлема, как вариант, для больших предприятий, способных нести крупные затраты на виртуализацию. Даже если предположить, что стоимость аренды облачного хранилища незначительна, предприятию придется затратить (по нашим предварительным расчетам) не менее 10 тысяч человеко-часов на разработку ПО для доступа к образу мобильного устройства в мобильном облаке и последующего клонирования разработанного образа на гаджет каждого сотрудника предприятия. Кроме того, надо будет купить готовое стороннее решение (или разработать его самостоятельно) для виртуальных машин, реализующих виртуализацию. Для американских корпораций International Business Machines Corporation (патентовладелец [1]) и United Parcel Service of America, Inc. (патентовладелец [2]) вышеперечисленные затраты посильны, но для малого по меркам Беларуси предприятия (100-150 работающих) это очень дорого.

**Методика решения проблемы и экспериментальная часть**

Для борьбы с угрозами информационной безопасности для относительно небольшого белорусского предприятия, выдающего своим сотрудникам смартфоны с операционной системой Android, в первом приближении можно использовать дешевое программное приложение[7]. Приложение устанавливается на служебный смартфон и блокирует доступ сотрудника ко всем веб-ориентированным приложениям кроме тех, которые разрешены для использования отделом информационной безопасности фирмы с целью выполнения сотрудниками фирмы своих служебных обязанностей. При этом на отдел информационной безопасности предприятия совместно с отделом администрирования сети возлагается обязанность централизованной защиты служебных гаджетов сотрудников. Во-первых, служебным гаджетам технически запрещѐн доступ к вредоносным сайтам. Во-вторых, атаки злоумышленников на служебные гаджеты с целью проникновения в сеть предприятия отражаются централизованно.

В настоящее время минское ООО «Стрим центр»продолжает работы по защите служебных гаджетов сотрудников в направлении специальной прошивки смартфона с операционной системой Android. Прошивка запрещает возможность подключения смартфона к другим сетям, кроме корпоративной сети предприятия, в том числе и к интернету, оставляя возможность доступа к информации, хранящейся в корпоративной сети. При этом права доступа к информации для различных категорий сотрудников (директор, бухгалтер, программист и т. д.) управляются политиками безопасности активной директории.

**Результаты и выводы**

Проведенный анализ и сравнение методов борьбы с угрозами информационной безопасности предприятия, выдающего своим сотрудникам служебные гаджеты, показал, что в настоящее время современные запатентованные зарубежные решения борьбы с такими угрозами для малого по меркам Беларуси предприятия (100-150 работающих) пока слишком дороги. Поэтому сегодня для парирования угроз информационной безопасности такого предприятия рекомендуется использовать дешевое программное приложение [7]. В дальнейшем возможна специальная прошивка смартфона с операционной системой Android, запрещающая возможность подключения смартфона к другим сетям, кроме корпоративной сети предприятия.

**Библиографический список**

1. Secure virtualized mobile cellular device: пат. США 10,009,322, МПК (Current International Class) H04L 29/06 (20060101); G06F 21/84 (20130101); G06F 21/53 (20130101); G06F 9/455 (20180101); H04W 12/02 (20090101); H04W 88/12 (20090101) / D. Agrawal, B. O. Anthony, Jr.,C. Bisdikian, M. Srivatsa, D. Verma; заявительInternational Business Machines Corporation; заявл. 31.03.16; опубл. 26.06.18 // Портал патентного ведомства США [Электронный ресурс]. – Режим доступа: https://www.uspto.gov/. – Дата доступа: 15.01.2019.

2. Systems and methods for assessing vehicle and vehicle operator efficiency: пат. США 9,858,732, МПК (Current International Class) G06G 7/76 (20060101); G08G 1/123 (20060101); G07C 5/06 (20060101); G07C 5/00 (20060101); G08G 1/00 (20060101); H04W 4/02 (20090101); G07C 5/02 (20060101); G06Q 10/08 (20120101); G06Q 10/06 (20120101) / M. J. Davidson; заявительUnited Parcel Service of America, Inc.; заявл. 12.02.15; опубл. 02.01.18 // Портал патентного ведомства США [Электронный ресурс]. – Режим доступа: https://www.uspto.gov/. – Дата доступа: 15.01.2019.

3. Служебные смартфоны порой позволяют полицейским Нью-Йорка ... [Электронный ресурс]. – Режим доступа: https://www.ixbt.com/news/2018/02/08/ sluzhebnye-smartfony-porojpozvoljajut-policejskim-njujorka-okazatsja-na-meste-prestuplenija-do-poluchenija-vyzova.html. – Дата доступа: 15.01.2019.

4. Федеральные чиновники будут пользоваться смартфоном на российской ОС [Электронный ресурс]. – Режим доступа: https://habr.com/post/412181/. – Дата доступа: 15.01.2019.

5. Хуг, Эндрю Мобильная безопасность: битва вокруг вредоносного ПО / Эндрю Хуг// Безопасность ИТ-инфраструктуры. – 2014. – № 7 (85). – С. 4–6.

6. Медведовский, И. Д. Атака на Internet[Электронный ресурс]. – Режим доступа: https://royallib.com/book/medvedovskiy_ilya/ataka_na_internet.html. – Дата доступа: 15.01.2019.

7. Угрозы информационной безопасности при использовании мобильных устройств на рабочих местах и в школах и их парирование / В. Д. Аленин, В. Л. Николаенко, А. А. Охрименко, В. И. Пачинин, Г. В. Сечко, Т. Г Таболич, И. И. Шпак // Труды XXIII МНТК «Информационные системы и технологии» ИСТ–2017, посвященной 100-летию НГТУ – Нижегородского политехнического института, Нижний Новгород (21 апреля 2017 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2017. – С. 569–573.

**D.K. Dedovich[1], M.N. Evdokimenko[1], M.S. Zhuravlev[1], V.L. Nikolaenko[3], G.V. Sechko[3], T.G. Tabolic[2]**

## ANALYSIS OF METHODS FOR DEALING WITH INFORMATION SECURITY THREAT OFFICIAL DEVICES INSMALL BUSINESS

«Stream Center» Limited Liability Company (Minsk)[1]
Belarusian Scientific Research Institute Transtekhnika (Minsk)[2]
Belarusian State University of Informatics and Radio Electronics (Minsk)[3]

Comparative analysis and methods for combating information security threats is relatively small by the standards of Belarus for a small business (100-150 employees), issuing service gadgets to its employees. The modern patented foreign solutions are considered. Recommendations on the choice of such methods for a small Belarusian enterprise are offered.

***Keywords:*** service gadget, information security, enterprise, foreign patent, mobile cloud, Republic of Belarus.