УДК [004.42:373]: 004.056.5

ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ СОТРУДНИКОВ ПРЕДПРИЯТИЙ И ШКОЛЬНИКОВ – ОДНА ИЗ ОСНОВ УСПЕШНОЙ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ И СОЦИАЛЬНОЙ СФЕРЫ БЕЛАРУСИ

И.И. ШПАК, В.Д. АЛЕНИН, Н.И. БАХУР

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»,
г. Минск, Республика Беларусь

Введение

Цифровизация экономики и всех сфер жизнедеятельности белорусского общества, в соответствии с Государственной программой [1], предусматривает не только внедрение информационно-коммуникационных технологий (ИКТ) и передовых производственных технологий во все отрасли народного хозяйства и социальную сферу, но также требует **обеспечения защиты информации**.

Решение задач по защите информации выполняется путем реализации мероприятий в рамках отдельной подпрограммы: “Информационная безопасность и “цифровое доверие”. Реализация указанной подпрограммы должна обеспечить повышение уровня информационной безопасности во всех сферах человеческой деятельности, защиты прав и законных интересов граждан [1].

Одной из важнейших задач по обеспечению защиты информации является разработка организационных и программных способов защиты мобильных устройств сотрудников предприятия на рабочих местах от вредоносного программного обеспечения (ВПО), от хищения персональных данных, а также от хищения служебного контента [2]. Аналогичные способы можно использовать для защиты мобильных телефонов школьников во время занятий в «Электронной школе» [3]. Весьма перспективной для указанных целей является технология *Byod (Bring your own device)* [4].

1. Анализ, достоинства и ограничения технологии *BYOD* «Принеси свое собственное устройство»

В 2004 году Рафаэль Баллагос *(Rafael Ballagas)* с соавторами опубликовал статью «*Byod: Bring your own device»* [4], в которой предложил подход к организации учебного процесса на предприятии с большими публичными дисплеями. *BYOD* на русский язык переводится как «Принеси свое собственное устройство». В настоящее время синонимами слова «подход *BYOD*» стали термины технология, стратегия, концепция, политика.

При применении *BYOD* обучаемый использовал принадлежащее ему устройство для доступа к информационным ресурсам учебного заведения или предприятия. При этом в статье [4] под устройством понимался мобильный телефон Nokia 6600 с камерой. *BYOD* по Баллагосу не только вносил в обучение эффект новизны и привлекал внимание обучаемого, но и позволял ученикам работать онлайн с электронными методическими пособиями, наглядными материалами и проверочными заданиями. Такой подход экономил время: больше не нужно было искать страницу в учебнике, перерисовать график или выписывать термины в тетрадь, а результаты теста можно было узнать сразу после прохождения [4]. Так, на конференциях *Digital Learning*, посвященных развитию цифровых технологий в обучении, провозглашался лозунг: «Зарегистрируйтесь по промокоду mobile2019 — и создавайте собственные курсы» [4]

В последующие годы использование технологии *BYOD* как концепции использования личных персональных гаджетов (смартфонов, планшетов, ноутбуков, жестких дисков или USB-накопителей, коммуникаторов (гибридов мобильного телефона и карманного компьютера, снабженных рядом программ) и т д.) сотрудников в рабочих целях стало повсеместным за счет ускорения бизнес-процессов: *BYOD* позволяет в рабочее время практически мгновенно получать актуальную информацию и упрощает коммуникацию сотрудника с коллегами. Мобильные технологии существенно изменили подходы к обучению. Сам процесс обучения стал более комфортным и быстрым. Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), совместно с Институтом ЮНЕСКО по информационным технологиям в образовании (ИИТО ЮНЕСКО), ввела специальный термин «мобильное обучение» и разработала рекомендации по его широкому внедрению [5]

Концепция *BYOD* достигла популярности после ее внедрения компанией «*Intel Corp.»* (США, Пенсильвания), крупнейшим в мире разработчиком и производителем электронных устройств и компьютерных компонентов (микропроцессоров и др.). По данным *Intel* количество мобильных устройств, используемых на работе служащими Intel, в 2009-2010 годах выросло с 10 до 30 тысяч. Предполагалось, что к 2014 году примерно 70% работников *Intel* будут использовать на работе собственные личные устройства [6].

Усилиями компьютерных фирм США *«Unisys Corp.»* (Пенсильвания), *«VMware Co.»* (Калифорния) и «Citrix Systems, Inc.» (Флорида) стратегия *BYOD* получила новый импульс к развитию, и ее техническая реализация оказалась вполне доступной [7]. *BYOD* стали использовать известные международные корпорации со штаб-квартирами в США *«Cisco Systems Inc.»* (Калифорния), *«IBM Corp.»* (штат Нью-Йорк), *«Oracle Corp.»* (Техас), а также канадская *«BlackBerry Ltd.»* (организационно-правовые формы компаний США (*Co, Corp. LP, Inc., Ltd.* и др.) кратко рассмотрены в [8].

Достоинствами *BYOD* являются [6]:

Экономия бюджета. *BYOD* также может положительно сказаться на расходах работодателей, поскольку они не оплачивают покупку устройства заранее или не тратят средства на расходы по обслуживанию/обновление в будущем;

Эффективность. Сотрудникам легче, быстрее и комфортнее выполнять рабочие обязанности с того устройства, которое им знакомо и привычно. В свою очередь это повышает производительность труда и максимизирует прибыль от бизнеса.

Лояльность. Позволяя использовать личное оборудование в работе, компания повышает уровень доверительных отношений с сотрудниками.

Таким образом, если работники предприятия почти не расстаются со смартфонами, они начинают и заканчивают свой день, проверяя рабочую почту, и находятся в постоянном доступе [7].

Однако при перечисленных преимуществах, у *BYOD* имеются и недостатки, сводящие на «нет» достоинства преимуществ:

Опасность заражения личного смартфона сотрудника вирусами и шпионскими программами. Вирус препятствует работе сотрудника. При заражении им сотрудник утрачивает возможность использовать смартфон, что снижает производительность труда сотрудника.

Шпионская программа позволяет злоумышленнику считать с зараженного смартфона служебную информацию, которой сотрудник пользуется во время работы. Этот объем конфиденциальной информации и информации, составляющей коммерческую тайну, может интересовать конкурентов предприятия, а ее утечка непосредственно влияет на производственную безопасность предприятия.

*Опасность кражи и утери личного смартфона. У*стройство сотрудника может быть украдено или утеряно вместе со всей служебной информацией.

Для устранения этих недостатков существует практика административного запрета сотрудникам во время работы использовать личные смартфоны. Вместо личных устройств сотрудника, ему в часы его работы выдается служебный смартфон предприятия, контролируемый службой информационной безопасности (СИБ).

2. Результаты проведенных работ по защите мобильных устройств сотрудников предприятий и школьников в Беларуси

Решение поставленной задачи целесообразно начать с рассмотрения существующих в рамках технологии *BYOD* моделей, сложившихся к настоящему времени. В интернет-ресурсе 2021 года [9] перечислены следующие модели *BYOD* и их аббревиатуры, отражающие весь спектр устройств:

BYOT – Bring Your Own Technology - Принеси свою собственную технологию;

BYOP – Bring Your Own Phone - Принеси свой собственный телефон;

BYOPC – Bring Your Own Personal Computer - Принеси свой собственный персональный компьютер.

BYOM – Bring Your Own Meeting – Организуй свою собственную встречу (коммуникатор);

используемых в рамках концепции *BYOD* и решаемых с ее помощью задач. Применительно к *BYOP* это могут быть две подмодели:

POCE (Personally-Owned, Company Enabled) – смартфон в личной собственности сотрудника, но с поддержкой компании. Эта модель похожа на *BYOD*, при этом компания берет на себя ответственность за часть возможностей устройства, используемых в бизнес-целях. Доступ к корпоративной сети осуществляется через портал, программно отделенный от частной части устройства.

COBO (Corporate-Owned, Business-Only) – сотрудник получает служебный смартфон, который используется только для бизнеса. Эта модель наиболее востребована специалистами СИБ.

В подмодели *COBO* смартфон проще и эффективнее защищать, используя общепринятые мировые практики защиты *BYOD* [9]. В служебных смартфонах доля смешивания личных и профессиональных данных мала, поэтому некоторые ограничения свободы действий пользователя оправданы и целесообразны. В этом случае баланс смещен более в сторону защиты данных, нежели удобства использования. Для этих целей можно использовать как специализированные устройства *(Blackberry)*, так и специальные превентивные меры по предотвращению утечек.

Одной из таких мер является внедрение *MDM (Mobile Device Management)* – (Управление мобильными устройствами). Системы класса *MDM* позволяют СИБ удаленно (централизованно) управлять множеством мобильных устройств (в т. ч. и смартфонов), будь то устройства, предоставленные сотрудникам компанией, или собственные устройства сотрудников.

Управление мобильными устройствами обычно включает в себя такие функции, как удаленное обновление политик безопасности (без подключения к корпоративной сети), распространение приложений и данных, а также управление конфигурацией для обеспечения всех устройств необходимыми ресурсами.

MDM-решения составляют основную часть программного обеспечения (ПО), активно продаваемого на рынке ПО *BYOD*. По данным *Global Industry Analysts, Inc*, в 2022 году объем рынка *BYOD* достигнет почти $94,2 млрд. Для сравнения, в 2014 году это значение составляло $30 млрд [10].

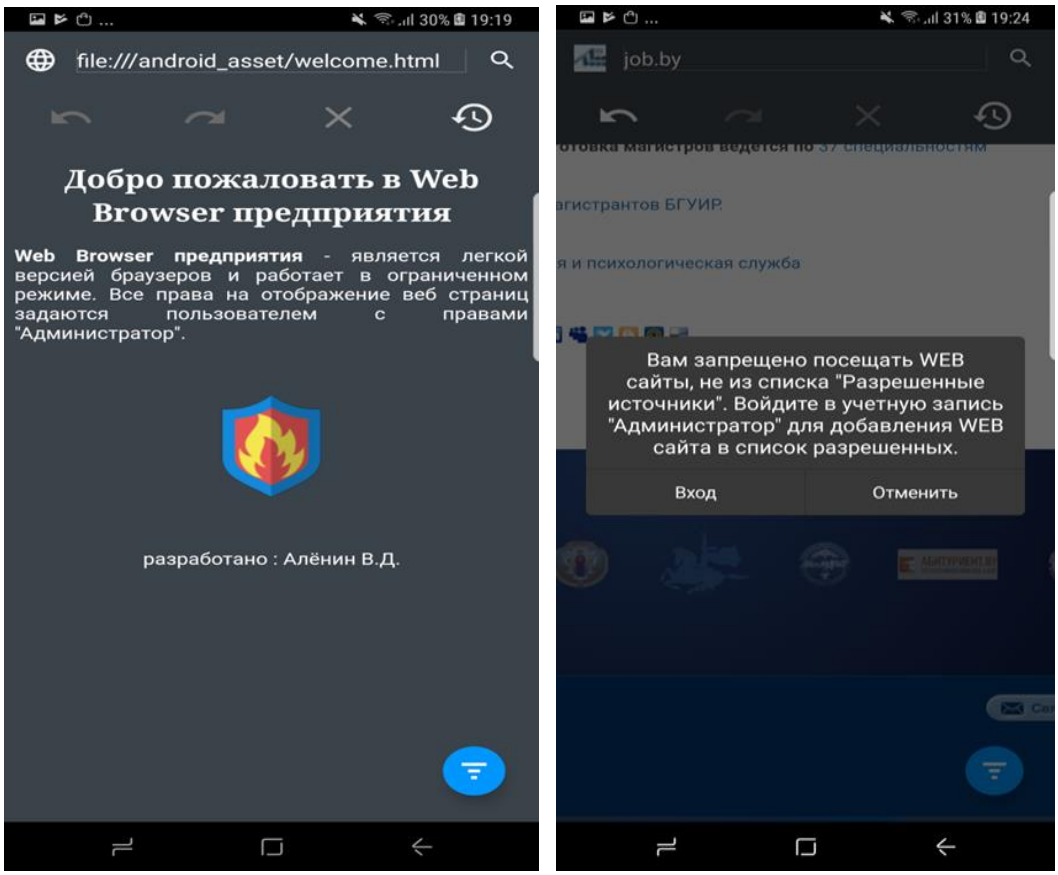
Внедрение *BYOD/COBO* на белорусских предприятиях, на наш взгляд, невелико, так как в Беларуси нет предприятий в сфере телекоммуникаций и информатики, сравнимых по чистому годовому доходу (прибыли, ЧД) с вышеупомянутыми *Oracle*

(ЧД $13,7 млрд), *Cisco* (ЧД $10,6 млрд), *IBM* (ЧД $5,59 млрд) или даже *Citrix* (ЧД $536 млн).

Самое крупное белорусское предприятие Белтелеком получило в 2020 году чистую прибыль всего $83 млн. Поэтому предприятия Беларуси практически не защищают свои корпоративные ЛВС путём покупки за рубежом дорогостоящих *MDM*-решений.

Таким образом, в Беларуси на рабочем месте белорусского сотрудника не то что предпочтительнее, а в силу недостатка денег, до сих пор используется личный смартфон (чистый *BYOD* по Баллагосу или изредка *BYOD/ POCE* с *MDM*-решениями белорусских программистов.

Однако после введения санкций, запрещающих передачу России и Беларуси передовых информационных технологий, рынок *MDM* и *BYOD* для Беларуси вообще стал закрытым. В этих условиях в Институте информационных технологий Белорусского государственного университета информатики и радиоэлектроники (ИИТ БГУИР) разработано простое *MDM*-решение «Б» для установки на смартфонах с мобильной операционной системой *Android* [11]. Экранные формы приложения «Б» приведены на рисунке 1.



а) б)

Рисунок – Экранные формы приложения «Б»

Приложение «Б» реализовано на языке программирования *Java* и имеет объём 27Mb. Смартфоны с *Android* были выбраны потому, что в соответствии с годовым отчётом *CISCO* по информационной безопасности за 2014 год 99 % мобильного вредоносного ПО было нацелено на устройства под управлением *Android* [12]. Приложение «Б» может устанавливаться как на личный смартфон, работающий по технологии *BYOD*, модель *BYOP*, подмодель *POCE*, так и на служебный смартфон (подмодель *COBO*). В свое время приложение «Б» прошло апробацию на личных

смартфонах школьников в проекте «Электронная школа» (руководитель апробации от ИИТ БГУИР – Н.И. Бахур [3].). Приложение «Б» при использовании подмодели *COBO* блокирует доступ пользователя смартфона ко всем веб-ориентированным приложениям кроме тех, которые разрешены для использования администратором сети или СИБ предприятия, с целью выполнения пользователем своих служебных обязанностей. В число заблокированных попадают адреса вредоносных сайтов, содержащих вирусы или шпионские программы, а также адреса игровых сайтов (на работе трудись, а не играй!). Для подмодели *POCE* блокируются только адреса вредоносных сайтов.

На рисунке 1 а) показана экранная форма приложения «Б» для задания адреса разрешённого сайта, а на рисунке 1 б) – форма, которую видит владелец смартфона при попытке посетить заблокированный неразрешённый сайт [11].

Заключение

1. Рассмотрены технологии и модели, используемые для защиты мобильных устройств сотрудников предприятий и школьников в Беларуси.
2. Проведен анализ возможностей и состояние внедрения *BYOD* на белорусских предприятиях и в школах.
3. Для безопасности личных смартфонов по модели «чистый *BYOD* по Баллагосу» или *BYOD/ POCE* предложено *MDM*-решение собственной разработки, защищающее смартфоны с операционной системой *Android*.

Список литературы

1. Государственная программа «Цифровое развитие Беларуси» на 2021 – 2025 годы. [Электронный ресурс]. – Режим доступа: https://mpt.gov.by/ru/gosudarstvennaya-programma-cifrovoe-razvitie-belarusi-na-2021-2025-gody /. – Дата доступа 22.04.2022.
2. Алёнин, В.Д. Угрозы информационной безопасности при использовании мобильных устройств на рабочих местах и в школах и их парирование / В.Д. Алёнин и др./ - Информационные системы и технологии ИСТ-2017, 2017 С. 569-573.
3. Бахур, Н. И. Модели и средства обеспечения управления информационной безопасностью на примере проекта «Цифровая школа»: автореф. дисс. на соискание степени магистра технических наук: 1-98 80 01 / Н. И. Бахур; науч. рук. И. И. Шпак. - Минск : БГУИР, 2016. - 10 с.
4. Мобильное обучение. [Электронный ресурс]. – Режим доступа: https://we.study/blog/mobile/. – Дата доступа 22.04.2022.
5. Рекомендации по политике в области мобильного обучения. [Электронный ресурс]. – Режим доступа: https://iite.unesco.org/pics/publications/ru/files/3214738.pdf /. – Дата доступа 22.04.2022.
6. Что такое *BYOD*? [Электронный ресурс]. – Режим доступа: https://unitsolutions.ru/blog/terminologiya/chto-takoe-byod /. – Дата доступа 22.04.2022.
7. Темная сторона *BYOD*. [Электронный ресурс]. – Режим доступа: https://ko.com.ua/temnaya_storona_byo_99426 /. – Дата доступа 22.04.2022.
8. Николаенко В.Л., Сечко Г.В., Таболич Т.Г. Технологии радиочастотной идентификации на автомобильном транспорте. Современное состояние и история развития по патентам США. Гродно: ЮрСаПринт, 2021. 238 с.
9. *BYOD* — Удобство против безопасности. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/281463/. – Дата доступа 22.04.2022.
10. Что такое *BYOD*? Модели *BYOD*. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/ipmatika/blog/584014/. – Дата доступа 22.04.2022.

11. Алёнин, В.Д. Информационная безопасность мобильных систем *Android*: диссертация на соискание степени магистра технических наук: 1-98 80 01 / В.Д. Алёнин; науч. рук. И. И. Шпак. - Минск : БГУИР, 2017. - 63 с.

12. Хуг, Эндрю. Мобильная безопасность: битва вокруг вредоносного ПО // Безопасность ИТ-инфраструктуры. 2014. N 7 (85). С. 4–6.