УДК 004.056.53

П. В. Смирнов, К. Л. Стойчин
Научный руководитель: д-р тех. наук, проф. С. В. Поршнев
Уральский федеральный университет, Екатеринбург

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ КОНЦЕПЦИИ BYOD

Аннотация. В статье рассмотрены проблемы информационной безопасности при использовании концепции BYOD для построения корпоративной информационной среды. Данное исследование имеет целью проведение анализа плюсов и минусов обозначенной концепции, выявление возможных проблем при ее использовании и выработку рекомендаций по их решению.

Ключевые слова: BYOD; корпоративная сеть; мобильные устройства; собственные устройства на рабочем месте.

В жизни современного общества непрерывно возрастает значение информации. Наиболее наглядно об этом может свидетельствовать тот факт, что термин «информационные технологии» стал для нас обыденным и устоявшимся. Именно этот термин используется для обозначения технологий, связанных с автоматизированной обработкой, хранением и передачей данных, и основную роль в выполнении данных задач занимают различные средства вычислительной техники.

В процессе развития средств вычислительной техники можно выделить два основных момента — повышение производительности устройств и уменьшение их размеров. Компактные и производительные устройства позволяют решать широкий спектр задач, в то же самое время позволяя их владельцу не быть привязанным к собственному рабочему месту. На использовании этих преимуществ базируется концепция BYOD.

Концепция BYOD (bring your own device — «принеси собственное устройство»), или концепция собственных устройств — использование своего собственного устройства (ноутбука, планшетного компьютера, смартфона) на рабочем месте вместо корпоративных устройств. Идея такой концепции появилась в середине 2000-х годов, однако наибольшую популярность начинает приобретать лишь в настоящее время в связи с развитием мобильных устройств, увеличением их возможностей и производительности, а также в связи с развитием сетевых технологий и облачных хранилищ.

В настоящий момент информация может считаться полноценным товаром, имеющим собственную ценность. В то же время утеря или разглаше-

ние информации может обернуться потенциальными убытками для обладателя этой информации. В связи с этим безопасность информации является наиболее важным фактором при выборе способов и средств ее обработки и хранения. Однако для концепции использования собственных устройств на данный момент не существует каких-либо общих принципов ее внедрения и обеспечения безопасности информации при ее использовании, в связи с этим для каждого конкретного случая необходимо проводить комплексный и всесторонний анализ информационной среды. Критерии и методы анализа при этом также остаются субъективными. Данное положение дел существенно затрудняет использование концепции BYOD и снижает потенциальный интерес к ней.

Как и любая концепция, BYOD имеет свои плюсы и минусы. К положительным сторонам данного подхода к организации рабочего процесса можно отнести:

- удобство для пользователя. Используя на рабочем месте собственное устройство, пользователь оказывается в привычной и комфортной для него рабочей среде, настроенной и персонализированной в соответствии с его предпочтениями. Это позволяет добиться повышения производительности труда сотрудника;
- возможность удаленной работы. Имея на собственном устройстве необходимые инструменты для работы и доступ к корпоративной среде предприятия, сотрудник может решать некоторые задачи, не находясь при этом непосредственно на рабочем месте. Это позволяет эффективнее использовать рабочее время сотрудника и увеличивать оперативность решения различных задач.

К актуальным проблемам при использовании данного подхода относятся:

- невозможность контроля за действиями сотрудника. Корпоративная офисные устройства зачастую имеют определенный и, как правило, ограниченный набор программ, что ограничивает возможную нерабочую деятельность сотрудника. К тому же на корпоративном устройстве может быть установлено программное обеспечение, отслеживающее действия сотрудника, что позволяет объективно оценить реальную производительность труда;
- возможные угрозы информационной безопасности. Собственные устройства пользователей могут оказаться уязвимы к атакам злоумышленников, нежели корпоративная среда с собственной политикой информационной безопасности.

С точки зрения возможного ущерба для компании, угрозы информационной безопасности являются более опасными, нежели посторонняя деятель-

ность сотрудников в рабочее время. Возможные угрозы зависят от конкретного типа используемого устройства.

При использовании портативных компьютеров существует вероятность внедрения на устройство вредоносного программного обеспечения. Для личного устройства эта вероятность намного выше, чем для корпоративного, поскольку за безопасность собственного устройства пользователь отвечает самостоятельно, и не всегда мер, которые предпринимаются для защиты устройства, бывает достаточно для обеспечения безопасности данных. Действия вредоносных программ могут быть совершенно различными — хищение конфиденциальной информации и данных для доступа к корпоративной среде, порча или уничтожение информации, хранящейся на устройстве. Стоит отметить, что риск порчи или утери данных существует даже без вмешательства извне, в случаях неисправности устройства, случайных ошибочных либо неверных действий пользователя.

Для смартфонов и планшетных компьютеров риск внедрения постороннего программного обеспечения несколько меньше, однако они также могут быть уязвимы для некоторых типов атак, связанных, в частности, с перехватом или получением доступа к аутентификационным данным.

Для всех личных устройств пользователя также существует риск их утери либо преднамеренного хищения. В таком случае посторонние лица получают практически полный доступ к данным и возможностям работы в корпоративной среде, которые имеет легальный пользователь.

При успешной реализации различных атак и угроз может быть нанесен значительный ущерб как обладателю устройства, так и компании в целом. Однако это не означает, что концепция собственных устройств создает прямую угрозу информационной безопасности компании в целом. Внедрение данного подхода лишь требует детального анализа состояния информационной безопасности обновленной информационной среды и выполнения определенных действий, направленных на минимизацию либо полное устранение наиболее значимых и актуальных угроз.

При внедрении концепции собственных устройств ключевым моментом является определение баланса между удобством и безопасностью. Зачастую именно от этого зависит принятие окончательного решения, поскольку полная защищенность лишает такой подход его преимуществ в удобстве для пользователя, а обеспечение максимального комфорта для пользователя непременно создает угрозы информационной безопасности.

Задача обеспечения информационной безопасности информационной среды, в которой используется концепция собственных устройств, может быть значительно упрощена. Для этого требуется определить наиболее актуальные угрозы и способы их устранения, а также подобрать программное обеспече-

ние и протоколы обмена данными, при использовании которых риск утечки либо утери информации будет минимален. При наличии некого упрощенного шаблона безопасной информационной среды будет существенно упрощен процесс внедрения концепции в реальные системы.

УДК 004.056 + 519.87

В. В. Царенко
Научный руководитель: доц. В. Ю. Бердюгин
Южно-Уральский государственный университет, Челябинск

МЕТОДОЛОГИЯ МОДЕЛИРОВАНИЯ И ОЦЕНКИ УГРОЗ ФИЗИЧЕСКОГО ДОСТУПА К ОБЪЕКТУ ЗАЩИТЫ

Аннотация. Для информационных систем, изолированных от глобальной сети, одними из наиболее актуальных угроз информационной безопасности и защиты информации являются угрозы физического доступа к элементам данных систем. Таким образом, возникает потребность в объективной оценке вероятности реализации этих угроз. В данной публикации рассмотрена возможность обращения к прикладным методам, составляющим инструментарий математического моделирования, посредством которых возможно представление объекта защиты и поиск путей реализации угроз физического доступа.

Ключевые слова: угрозы физического доступа; инженерно-техническая защита информации; система безопасности; охрана объектов; формализованное представление; безопасность; математическое моделирование; математические модели; математические методы; теория вероятностей; теория графов.

Ввиду разнообразия и уникальности каждого объекта информатизации и в общем случае каждого информационного ресурса, проектирование системы защиты является сложным процессом, в котором преимущественно применяются экспертные знания, опыт специалистов в области систем инженерно-технической защиты информации. Необходимым условием обеспечения комплексной защиты информации является создание определенных критериев, позволяющих оценить защищенность и определить достаточность мер, предпринятых для защиты от угроз. Моделирование позволяет унифицировать систему защиты и установить критерии оценки (показатели) защищенности объекта. Непосредственный интерес представляют математические модели, позволяющие на основании выбранных критериев оценить систему защиты объекта на соответствие предъявляемым требованиям, в частности, оценить