РАЗДЕЛ II. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Белов В.Н., Пушкова К.С.

Защита учетной записи пользователя в современных гаджетах

Арзамасский филиал ННГУ
(Россия, Арзамас)

doi:10.18411/spc-12-12-2017-03

idsp: 000001:spc-12-12-2017-03

Аннотация

В работе приведен анализ способов защиты учетных записей пользователя на различных платформах смартфонов, а так же их детальное описание. Дается сравнение их характеристик, описываются преимущества и недостатки каждого метода защиты.

Ключевые слова: защита учетной записи; гаджеты; платформа IOS; платформа Windows Phone; платформа Android.

Abstract

The article provides an analysis of the ways to protect user accounts on various smartphone platforms, as well as their detailed description. Comparison of their characteristics is given, advantages and disadvantages of each method of protection are described.

Keywords: account protection; gadgets; the IOS platform; Windows Phone platform; Android platform.

С развитием гаджетов, наиболее востребованным способом хранения персональных данных является учетная запись пользователя. В ней содержатся персональные данные необходимые пользователю. Она значительно упростила доступ к данным пользователя и открыла доступ переносить данные с одного гаджета на другой по средствам сети Интернет [1]. Для безопасности персональных данных на платформах смартфонов присутствуют различные аутентификации. Опишем этапы защиты персональных данных в платформах таких видов как: IOS, Android, Windows Phone.

Платформа IOS использует двухфакторную аутентификацию для идентификатора Apple ID, которая гарантирует, что доступ к учетной записи получит только пользователь, даже если пароль от учетной записи известен кому-либо еще. При двухфакторной аутентификации доступ к учетной записи пользователя возможен только с доверенных устройств на платформе IOS. При первом входе в учетную запись на новом устройстве пользователю потребуется ввести пароль от учетной записи и шестизначный цифровой проверочный код, который автоматически отображается на всех доверенных устройствах по средствам SMS или голосового вызова. После ввода шестизначного цифрового кода новое устройство попадает в список доверенных устройств. В нем перечислены устройства, с которых был выполнен вход в учетную запись пользователя. У каждого устройства в списке можно посмотреть модель, серийный номер и другую полезную информацию. Так же можно удалить доверенное устройство из этого списка - это приводит к прекращению отображения на нем шестизначных цифровых кодов и блокировке доступа к учетной записи пользователя до тех пор, пока не будет выполнен повторный вход в учетную запись пользователя с помощью двухфакторной аутентификации. За счет шестизначного цифрового кода при двухфакторной аутентификации недостаточно знать только пароль от учетной записи пользователя. Поэтому безопасность персональных данных существенно возрастает [3].

Платформа Windows Phone использует систему Windows Hello, она предназначена для удобного, а самое главное безопасного входа пользователя в

учетную запись. Таким образом, пользователю не нужно запоминать пароль и тратить время на ввод логина. Система Windows Hello основывается на биометрических технологиях. Ее преимущество в том, что она способна распознавать пользователя по одной из биометрических характеристик такие как: распознавание лиц, сканирование отпечатка пальца или сканирование радужной оболочки глаза, после чего вводить пароль уже не требуется. Система Windows Hello использует RealSense-камеру, которая может отличить пользователя не только от других людей, но и от фотографии самого пользователя, так как для распознавания камере нужны объемные формы. А сканер радужной оболочки глаз работает в темном помещении и может применяться даже при использовании прозрачных контактных линз и очков. В тоже время в ней присутствует PIN-код и для каждого устройства он задается индивидуально, для того, чтобы пользователь мог передавать пользование смартфоном своим близким или родственникам. Последней линией защиты в случае утери или хищения смартфона является шифрование устройства. Оно скрывает информацию на смартфоне и делает смартфон не доступным для чтения информации в случае кражи. Прочитать информацию сможет только человек владеющий ключом [4,5].

Платформа Android на сегодняшний день одна из самых популярных. Этому способствует приемлемая цена, широкий ассортимент, простота использования данных гаджетов. Платформа Android, так же как и платформа IOS использует двухфакторную аутентификацию. Отличие этой платформы заключается в том, что Android использует всего один аккаунт учетной записи пользователя для всех сервисов Google, что очень удобно и полезно. Для входа в учетную запись потребуется ввести не только логин и пароль, но и специальный код который придет на смартфон по средствам SMS или голосового вызова. Чтобы не вводить специальный код при каждом входе в аккаунт, смартфон можно отметить как надежный, после чего при входе в учетную запись пользователя специальный пароль вводить уже не потребуется. Учетная запись пользователя по-прежнему останется под защитой, а при входе в аккаунт с другого гаджета система вновь потребует ввести специальный пароль. Для удобства пользователя компания Google, предусмотрела несколько вариантов, с помощью которых пользователь может получить специальный пароль даже в том случае, если гаджет пользователя находится вне зоны действия сети. Можно заранее записать специальные резервные пароли или установить на гаджет программу-генератор, которая будет самостоятельно их создавать. И даже если специальный пароль узнал посторонний человек, у него не получится войти в учетную запись пользователя, так как специальный пароль меняется каждые 30 секунд автоматически [2,6].

Рассмотрев этапы защиты персональных данных пользователя на платформах таких видов как: IOS, Android, Windows Phone. Можно с уверенностью сказать, что у каждой из этих платформ защита персональных данных составляет весьма не маловажную роль. Но стоит выделить одну платформу из ряда остальных. Платформа Windows Phone достигла более надежной защиты персональных данных и существенно упростила вход в учетную запись пользователя за счет биометрических технологий. С помощью трех биометрических характеристик система Windows Hello безошибочно может распознать своего пользователя среди остальных людей. Удобство этой системы заключается в том, что пользователю после биометрической проверки не потребуется вводить логин и пароль от своей учетной записи. Это не только упростит пользование, но и сэкономит время.

1. Белов В. Н., Ковалёв А.И.. Некоторые аспекты использования электронных ключей в подходах защиты информации // Математический вестник педвузов и университетов Волго-Вятского региона . - 2015 . - №17. - С. 318-324.
2. Двухступенчатая авторизация от Google: защищаем доступ к Google/Gmail – аккаунту с помощью новой технологии. // Журнал «Хакер». URL: <https://xaker.ru/2011/04/10/56227/> (дата обращения: 09.11.2017).
3. Двухфакторная аутентификация для идентификатора Apple ID // Apple. URL: <https://support.apple.com/ru-ru/HT204915> (дата обращения: 28.10.2017).

4. Система аутентификации WindowsHello // Ipkey. URL: <http://ipkey.com.ua/faq/990-windows-hello.html> (дата обращения: 08.11.2017).
5. Функции безопасности в Windows 10 Mobile // SecurityLab. URL: <http://www.securitylab.ru/blog/personal/bezmaly/300626.php> (дата обращения: 05.11.2017).
6. Крижепольский Павел. Google Двухэтапная аутентификация // Android для чайников №10. Двухэтапная аутентификация. - 2014. - № 10. URL: <http://android.mobile-review.com/articles/28556/> (дата обращения: 09.11.2017).

Гусева К.Р., Князев В.Н.

Вопросы разработки и исследования автоматизированных информационных систем предприятий

*Пензенский государственный университет
(Россия, Пенза)*

doi:10.18411/spc-12-12-2017-04

idsp: 000001:spc-12-12-2017-04

Введение. В современном мире в условиях рыночной экономики хозяйственно-экономическая деятельность любого предприятия, как правило, проводится с активным использованием информационных технологий и средств автоматизации. Информационные технологии в значительной степени ускоряют процессы учета и управления в различных сферах деятельности фирм и компаний, позволяют решать такие задачи, как планирование, финансовый анализ, подготовка аналитических отчетностей. Предприятия и фирмы, которые не применяют активно информационные технологии, рискуют потерять свою конкурентоспособность и отстать в развитии.

Полномасштабное и интенсивное развитие информационных технологий в Российской Федерации является одним из наиболее важных и приоритетных направлений государственной политики. В частности, принята и реализуется Государственная программа Российской Федерации «Информационное общество» с периодом действия на 2011-2020 годы. [1]

Основной целью программы является повышение конкурентоспособности экономики страны за счет снижения издержек и улучшения качества продукции и услуг, повышение эффективности государственного и муниципального управления, обеспечение роста качества жизни населения.

Современное материальное производство и другие сферы деятельности нуждаются в информационном обслуживании, переработке огромного количества информации. Воздействие информатизации касается экономической и социальной сфер, науки и образования, культуры и образа жизни людей, сферы права, государства и институтов гражданского общества.

Кроме того, "Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года" предусматривает масштабное применение в информационном обществе мобильных устройств: «Прогнозируется активный рост мобильных приложений и уменьшение грани между мобильными и стационарными устройствами». [2]

Предметная область. Идея использования информационных систем для обработки заявок возникала неоднократно. Автоматизированные системы учета и управления заявками начинают все более активно использоваться в мебельных компаниях. С помощью автоматизированных систем удастся структурировать товарные и денежные потоки, снизить себестоимость производства, повысить производительность и качество труда, тем самым увеличивая количество получаемой прибыли. Автоматизированная система по обслуживанию заявок существенно ускоряет процесс выполнения заявок, исключает возможности их потери, позволяет осуществлять контроль за исполнением работы.