УДК 330.131.7

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ РЕАЛИИ

© **Грошева Е. К., Невмержицкий П. И., 2017**
Иркутский государственный университет, г. Иркутск

В статье рассматривается понятие информационной безопасности, ее общий смысл, способы ее укрепления, рассмотрены способы защиты личных данных, рассмотрено понятие защиты информации. Даны некоторые советы рядовым пользователям.

Ключевые слова: информационная безопасность, информационные технологии, защита информации

Информационные технологии используются повсеместно, и многие уже не могут представить свою жизнь без них: социальные сети, мессенджеры, интернет-магазины, онлайн-банкинг — все эти средства связи и коммуникаций мы используем, и все эти точки доступа потенциально уязвимы. Именно поэтому информационная безопасность играет крайне важную роль в нашей жизни. С развитием технологий все сложнее становится защита личных данных. В этой статье мы хотели бы рассмотреть возможности решения данной проблемы.

Рассмотрим вопросы информационной безопасности при работе с мобильными банковскими приложениями. Сегодня клиенты общаются с банками в рамках следующих приложений:

- банк-клиент или онлайн-банкинг через персональные компьютеры;
- мобильные онлайн приложения;
- социальные сети и мессенджеры.

Каналы общения, по мнению Б. Кинга, выглядят следующим образом:

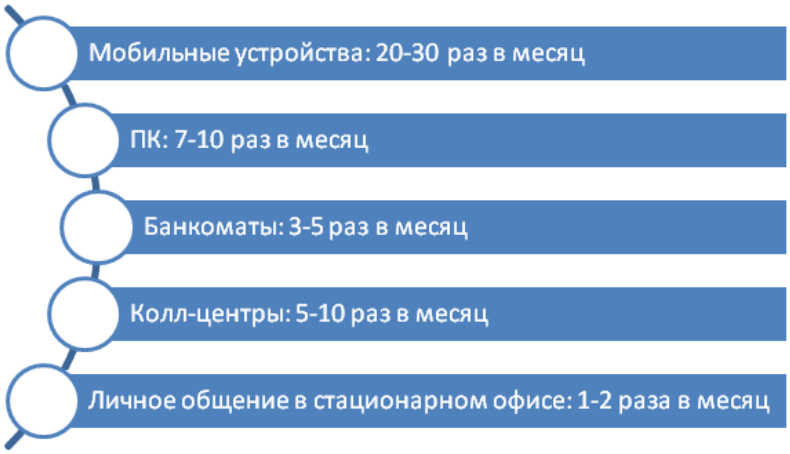

Рис.1. Каналы коммуникации банка и клиента. Составлено по [1]

При этом клиент проводит транзакции, сообщает персональные данные, и фактически уязвим.

Более 10 лет в сети ходят анекдоты про искусственный интеллект, который от имени банка дает советы клиентам. Популярный сегодня маркетинговый тренд «smart data» предполагает максимальный персонифицированный сбор данных о клиентах, где на основе одного общего поля-индикатора (мобильного телефона или адреса электронной почты) можно получить комплексный портрет клиента.

Казалось бы, причём тут информационная безопасность? Подписывая «согласие на рассылку информации рекламного характера», автоматическое нажатие кнопки «согласен», регистрация в большом количестве Интернет-ресурсов с одним и тем же логином — это все приводит к верификации вас как клиента, позволяет собирать и использовать личную информацию.

Отметим такие случаи, как анализ профилей в социальных сетях при приеме на работу, контекстная реклама и многие другие.

Неудивительно, что защита персональных данных в частности и информационная безопасность в целом волнуют клиентов.

Обычно под информационной безопасностью подразумевают качество защищенности объекта, коим чаще всего выступает информация, данные, ресурсы системы и т.д.

Безопасность информации — состояние защищенности данных, при которых обеспечены их доступность, конфиденциальность и целостность. В данном случае под доступностью данных подразумеваются их свойство, определяющее возможность их получения и дальнейшего использования по требованию уполномоченных лиц, под конфиденциальностью — свойство, связанное с тем, что эти данные не станут доступны для третьих лиц без согласия уполномоченных лиц, а под целостностью — неизменность информации в процессе хранения или передачи. Иными словами, для защиты информации информация должна быть:

1. достаточно защищена от взлома извне;
2. оперирована достаточно образованным лицом;
3. недоступна для неуполномоченных лиц.

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Многие организации выстраивают собственные системы информационной безопасности, проводят проверки и анализ защищенности данных. Это касается как персональных данных клиентов и персонала, так и информации о текущей деятельности, финансовом состоянии. Как правило, реализация мер защиты включает в себя организационные мероприятия, например, назначение ответственных за информационную безопасность лиц, разработку правил и инструкций для пользователей, внедрение политики резервного копирования и другое. Современные организации используют требования международных стандартов для построения систем менеджмента информационной безопасности и используют лучшие мировые практики [2].

Вне зависимости от того, в каком виде информация сохраняется, каким образом используется, необходимо реализовывать адекватные меры защиты. Каждый руководитель должен объективно оценивать текущее состояние информационных систем, видеть и понимать нужды в информационном обеспечении и существующие информационные проблемы.

Именно для этого в организации должно проводиться обучение ответственных лиц и пользователей определенным моментам работы с данными, в том числе основам информационной безопасности. Устанавливаются программные средства защиты, программное обеспечение, регулярное обновление антивирусных программ, шифрование данных.

Для улучшения защиты данных организации проводится модернизация или ремонт существующей локальной сети, установка дополнительного оборудования — видеокамер, дополнительные серверы, источники

бесперебойного питания и др. Благодаря мерам защиты значительно снижаются риски утечки деловой информации, риски разного рода воздействия, вызывающие отказы в работе информационных систем, таких как мошеннические программы, хакерские атаки.

Не менее актуальной является и построение личной информационной безопасности пользователей. Использование компьютеров, планшетов, смартфонов стало неотъемлемой частью жизни каждого студента. Современное поколение с легкостью осваивает информационные технологии и зачастую уделяет недостаточное внимание рискам, которые возникают при работе в системе Интернет, использовании съемных носителей информации и т.д. Иногда только потеря информации или внезапно возникшие проблемы с компьютером заставляют обратить внимание на усиление средств защиты и изучение проблемы информационной безопасности.

В быту защита информации в основном рассматривается как защита от вирусных программ, или вирусов. Компьютерный вирус — вид вредоносного программного обеспечения. Оно способно создавать собственные копии, внедряться в код других программ, загрузочные секторы или системные области памяти, а также распространять собственные копии по различным каналам связи. Компьютерный вирус неспроста был назван так — можно сравнить его распространение с биологическим вирусом. У него есть множество видов: Черви, Троянские программы, Полиморфные вирусы и многие другие. Каждый из этих вирусов действует по-своему, и постоянно появляются все новые и новые вирусы. Однако существуют и средства противодействия. Они так и называются — антивирусы.

Антиви́рус — это специализированная программа, предназначенная для обнаружения, устранения и предотвращения появления компьютерных вирусов. Также одной из функций антивируса является восстановление зараженных вирусами файлов.

Защитить важную для себя информацию может любой человек. Для этого достаточно не игнорировать некоторые угрозы. Так, например, не использовать простые пароли. Пароли «0000» на вашем телефоне или «parol1» на почте вполне могут привести к утере важных для вас данных. Чтобы ваш пароль был надежен, в идеале он должен состоять из букв и цифр, иметь больше 8 знаков, содержать как заглавные, так и прописные буквы, а так же не совпадать ни с одним словарным словом. Необходимо использовать защиту от вирусов. На рынке существуют множество антивирусов, подобрать простой и эффективный достаточно легко. Однако, перед установкой лучше проконсультироваться со специалистом. Кроме того, установленный антивирус следует периодически обновлять.

Необходимо учиться лучше пользоваться компьютером. Для вашего компьютера самый опасный хакер — вы сами. А если кто-то другой собирается работать с вашими данными, вы должны быть уверены в его/ее компетентности и благонадежности. Иначе ваши данные могут как быть утеряны, так и быть использованы не по назначению. Периодически следует обновлять программное обеспечение, включая веб-браузер. Весьма опасным является переход на подозрительные страницы в интернете, а также на всплывающую рекламу. Там могут быть вирусы. Пользователям необходимо использовать только надежные устройства хранения данных. Если устройство чужое и вы о нем ничего не знаете, есть риск подключить к компьютеру устройство с вирусом.

Для того, чтобы обезопасить пользование компьютером, необходимо также должны помнить о некоторых моментах работы в Интернете. Ни в коем случае нельзя сообщать в Интернете свое имя, номер телефона, номер кредитной карты, адрес проживания, пароль и т.д. если нет 100% уверенности в благонадежности источника. Необходимо блокировать спам и рекламу. Реклама также может быть источником вируса в некоторых случаях.

Если что-то в работе компьютера кажется вам неестественным или тревожным, лучше обратиться к специалистам.

Используя различные способы защиты по максимуму, пользователи создают собственную систему информационной безопасности, позволяющую сохранить свои данные, снизить до минимума риски несанкционированного доступа к различного рода сведениям, имеющим важное значение в жизни.

Теперь обратимся к вопросам информационной безопасности при использовании мобильных банковских приложений. Потенциальная уязвимость клиента — взлом пароля, несанкционированное использование данных о банковских картах и счетах, доступ к информации о расходах и доходах, получение информации о паролях.

Советы клиентам тут следующие:

- не использовать пароли в интернет и онлайн-банкинг, которые уже задействованы в других сервисах.
- тщательно проверять, куда и кому вы платите.
- не посылать данные своей банковской карты, логины и пароли в онлайн-сервисы на непроверенные сайты.
- не хранить средства на той карте, с которой вы рассчитываетесь через интернет.
- не использовать платежи на посторонних сайтах.

- проверять (или перезванивать в банк) при поступлении смс-сообщений с просьбой о финансовой информации.
- при регистрации на массовых сайтах, например, на Avito, использовать не основной электронный адрес и номер телефона. ■

1. Кинг Б. Банк 3.0. / Бретт Кинг. – М. ЗАО «Олимп-Бизнесс», 2014. – 474 с.
2. ISO/IEC 27001:2005. Информационные технологии. Методы обеспечения безопасности – Системы управления информационной безопасностью. Требования. – 2005. – 36 с.
3. ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management [Электронный ресурс] // Интернет-портал – URL: http://www.iso.org/iso/catalogue_detail?csnumber=56742 (Дата обращения: 18.09.2017)
4. Базовая информация о информационной безопасности [Электронный ресурс] // Интернет-портал – URL: http://bezopasnik.org/article/1.htm (Дата обращения: 18.09.2017)
5. Федеральный закон «О персональных данных». 27 июля 2006 года № 152-ФЗ. Принят Государственной Думой 8 июля 2006 года

СПИСОК ЛИТЕРАТУРЫ

ISO/IEC 27001:2005. Информационные технологии. Методы обеспечения безопасности – Системы управления информационной безопасностью. Требования. – 2005. – 36 с.

ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management [Электронный ресурс] // Интернет-портал – URL: http://www.iso.org/iso/catalogue_detail?csnumber=56742 (Дата обращения: 18.09.2017)

Базовая информация о информационной безопасности [Электронный ресурс] // Интернет-портал – URL: http://bezopasnik.org/article/1.htm (Дата обращения: 18.09.2017)

Кинг Б. Банк 3.0. / Бретт Кинг. – М. ЗАО «Олимп-Бизнесс», 2014. – 474 с.

Федеральный закон «О персональных данных». 27 июля 2006 года № 152-ФЗ. Принят Государственной Думой 8 июля 2006 года

Information security: modern realities

In this article we review the definition of the information security, its main meaning, ways to strengthen the security, ways to protect the personal data, also we review the definition of data protection. Some advices were given to a regular users.

Keywords: information security, information technologies, data protection