УДК 004.056.53 **DOI:10.30837/rt.2020.1.200.16**

И.Е. АНТИПОВ, д-р техн. наук, Б.В. БОЧАРОВ, Д.Р. НАЙДЕНОВА

ОЦЕНКА БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-БАНКИНГА

Введение

Дистанционное банковское обслуживание или Интернет-банкинг (ИБ) – технология, позволяющая удаленно осуществлять финансовые операции и контролировать движение средств, прочно вошла в нашу жизнь. Ее удобства и преимущества неоспоримы. К сожалению, уязвимости у этой технологии тоже существуют.

В публикациях часто описываются различные приемы, которыми пользуются мошенники для хищения средств и даются советы о том, как им противостоять. Но они, в основном, носят частный, разрозненный характер. Авторы статьи полагают, что проблема обеспечения безопасности ИБ должна рассматриваться комплексно. Для этого необходимо решить следующие задачи:

- систематизировать уязвимости пользователей ИБ;
- предложить методику их численной оценки;
- предложить меры по противодействию угрозам;
- предложить методику оценки эффективности их применения.

В статье рассмотрены и систематизированы угрозы для пользователей интернет-банкинга, обусловленные уязвимостями мобильных телефонов и мобильной связи, контрмеры, доступные пользователю, а также способы численной оценки уязвимостей и эффективности контрмер.

Анализ и обобщение уязвимостей для пользователей ИБ

При подготовке статьи был рассмотрен ряд публикаций, в которых описаны пути несанкционированного доступа к сервисам ИБ [2 – 14]. Не исключено, что в скором времени будут изобретены новые способы доступа, а ныне известные потеряют свою актуальность. В рамках научной статьи будет уместно рассмотреть, обобщить и систематизировать основные пути, которыми пользуются злоумышленники.

Итак, на основании анализа [2 – 14], мы выделили четыре основные уязвимости:

1. Похищение телефона вместе со всей имеющейся в нем информацией;
2. Методы социальной инженерии (СИ), при которых мошенническим путем извлекаются необходимые данные (телефон при этом – просто средство связи);
3. Перехват данных, передаваемых или хранящихся на мобильном устройстве;
4. Похищение данных sim-карты (физически sim-карта при этом остается у пользователя).

Две последние группы могут быть разделены на подгруппы, что требует дополнительных пояснений.

Перехват данных может осуществляться путем установки вредоносного программного обеспечения (ПО) на устройство пользователя, либо через уязвимость сети связи. Это наиболее распространенный способ похищения данных. Как отмечается в [12], до 43 % ПО для мобильных телефонов, находящегося в открытом доступе, потенциально опасно. Кроме того, встречаются сообщения о случаях «открытого» копирования данных пользователей с использованием административного ресурса[*] (на границах при въезде/выезде в некоторые страны и районы) [5, 6].

Установка вредоносного ПО может происходить при использовании программ из непроверенных источников и при переходе по фишинговым ссылкам [2]. Отмечаются случаи уста-

[*] Предполагается, что административный ресурс, упоминаемый здесь и далее в этой статье, доступен только уполномоченным государственным органам и применяется исключительно в благих целях. Однако, как показывает практика, такое предположение не всегда верно, о чем свидетельствуют [7, 8].

новки вредоносного ПО еще на этапе производства мобильного устройства [4]. Намеренная установка вредоносного ПО может произойти при временной передаче устройства в чужие руки (на ремонт, под предлогом «посмотреть», «позвонить» и т. д.) Также имеют место случаи установки такого ПО с использованием административного ресурса [5].

Перехват данных через сеть (без доступа к устройству пользователя) может быть осуществлен с использованием уязвимостей сетей мобильной связи, а также с использованием административного ресурса. Отдельно следует выделить опасность перехвата данных при подключении через Wi-Fi сети, которые уступают по защищенности сетям мобильной связи.

Для похищения данных sim-карты не обязательно иметь к ней физический доступ. Хакерские технологии позволяют создать «клон» sim-карты, используя уязвимости сетей мобильной связи [3, 9]. Также некоторые операторы мобильной связи позволяют восстановить утерянную (или «якобы утерянную») sim-карту с помощью нового стартового пакета [10]. Это дает возможность мошенникам, используя различные приемы, получить дубликат sim-карты, попутно заблокировав при этом карту законного пользователя [13, 14]. Также есть случаи получения дубликата sim-карты с использованием административного ресурса [11].

Рассмотренные уязвимости схематично показаны на рис. 1.

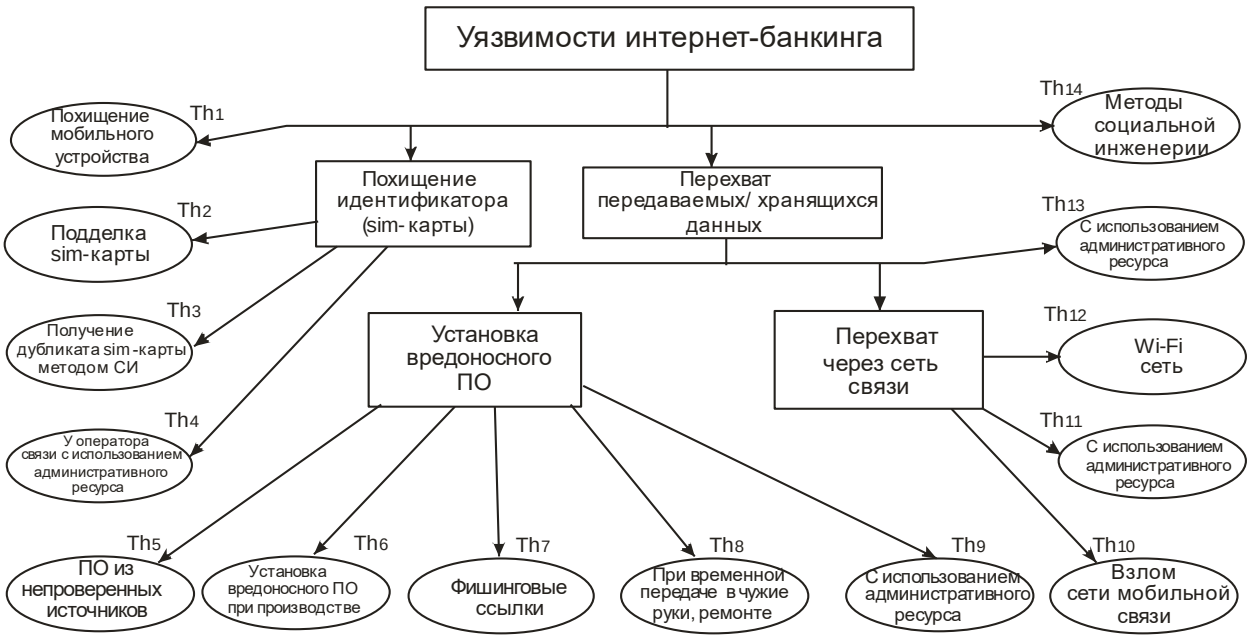

Рис. 1. Схематическое представление уязвимостей для пользователей ИБ

Известная методика численной оценки

Перейдем к рассмотрению указанных уязвимостей с точки зрения одной из базовых угроз информационной безопасности – конфиденциальности данных, которые позволяют злоумышленнику получить доступ к счету пользователя. Для каждой уязвимости должен быть рассчитан уровень угрозы Th_i. Согласно [15], это величина является безразмерной и означает критичность воздействия данной угрозы на ресурс. В ней также учитывается вероятность реализации данной угрозы. Выражение для расчета уровня угрозы:

$$Th_i = ER_i \times P_i, \quad (1)$$

где P_i – вероятность реализации каждой угрозы (отношение количества успешных попыток реализации угрозы для некоторой уязвимости к общему числу попыток, предпринимаемых злоумышленниками), ER_i – критичность реализации угрозы, которая отражает меру нанесенного ущерба по отношению к максимально возможному ущербу, если она будет реализована.

После определения уровня угрозы Th_i, согласно [15], необходимо рассчитать уровень угрозы для всех уязвимостей

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i). \quad (2)$$

Далее оценивается стоимость ресурса C и суммарный риск:

$$R = C \times CTh. \quad (3)$$

Таким образом, для расчета уровней угроз согласно методике [15] необходимо составить таблицу вида (табл. 1):

Таблица 1

Номер	Угроза/уязвимость	Вероятность реализации *P, %*	Критичность реализации *ER, %*
1	Угроза 1 / Уязвимость 1	P_{11}	ER_{11}
..	…	…	…
N	Угроза 3 / Уязвимость m	P_{3m}	ER_{3m}

Методика оценки уязвимости пользователей ИБ

Для нашего случая таблица принимает вид табл. 2.

Таблица 2

Уязвимость / пути реализации			Вероятность реализации	Критичность реализации	Уровень угрозы
Похищение телефона			P_1	ER_1	Th_1
Похищение данных sim-карты		- путем подделки sim-карты	P_2	ER_2	Th_2
		- путем получения дубликата средствами СИ	P_3	ER_3	Th_3
		- у оператора связи с использованием админресурса	P_4	ER_4	Th_4
Перехват/ копирование данных телефона	- путем установки вредоносного ПО	- из непроверенных источников	P_5	ER_5	Th_5
		- на этапе производства	P_6	ER_6	Th_6
		- через фишинговые ссылки	P_7	ER_7	Th_7
		- при передаче в чужие руки	P_8	ER_8	Th_8
		- с использованием админресурса	P_9	ER_9	Th_9
	- через сеть	- путем «взлома» сети	P_{10}	ER_{10}	Th_{10}
		- Wi-Fi	P_{11}	ER_{11}	Th_{11}
		- с использованием админресурса	P_{12}	ER_{12}	Th_{12}
	- с использованием админресурса		P_{13}	ER_{13}	Th_{13}
Методы социальной инженерии			P_{14}	ER_{14}	Th_{14}

Для ее заполнения необходимо знать вероятности P_i и критичности реализации ER_i. Они могут быть получены из анализа полицейских сводок, данных о попытках взломов и их результативности, что по силам только службам безопасности банков. Эти данные могут различаться для разных местностей и меняться с течением времени, но именно они могут служить точным исходным материалом для оценки уязвимости согласно [15] и использоваться для совершенствования систем безопасности со стороны банков.

Авторам статьи такие данные недоступны, поэтому для получения хотя бы оценочных значений уязвимостей был применен следующий подход.

У каждого пользователя ИБ имеется свое представление об угрозах, связанных с безопасностью их банковских счетов. Оно формируется на основании личного опыта, опыта

ближайшего окружения, публикаций в СМИ, социальных сетях и т. д. Опрос даже ограниченного количества пользователей может помочь получить требуемые оценки.

Сложность опроса состояла в том, что далеко не все пользователи различают и готовы разбираться в понятиях «вероятность реализации угрозы», «критичность реализации» и др. Поэтому опрашиваемым было предложено ответить на такой вопрос:

- допустим, имеется 1000 пользователей ИБ, ведущих такой же образ жизни, применяющих то же оборудование и практикующих тот же подход к мерам безопасности в ИБ, что и они. Сколько из них могут стать жертвами злоумышленников в результате той или иной уязвимости?

Результаты опроса, нормированные к числу гипотетических одинаковых пользователей, представлены в табл. 3 как уровень угрозы.

Удобство такого подхода состоит в том, что каждый пользователь, если он заинтересован в повышении своей безопасности в ИБ, может изучить элементарные сведения о существующих уязвимостях и путях их реализации (хотя бы, в рамках данной статьи) и самостоятельно оценить уровень угроз для себя.

Таблица 3

Уязвимость / пути реализации			Уровень угрозы	
Похищение телефона			Th_1	0.001
Похищение данных sim-карты	- путем подделки sim-карты		Th_2	0.001
	- путем получения дубликата средствами СИ		Th_3	0.005
	- у оператора связи с использованием админресурса		Th_4	~0
Перехват/ копирование данных телефона	- путем установки вредоносного ПО	- из непроверенных источников	Th_5	0.01
		- на этапе производства	Th_6	~0
		- через фишинговые ссылки	Th_7	0.01
		- при передаче в чужие руки	Th_8	~0
		- с использованием админресурса	Th_9	~0
	- через сеть	- путем «взлома» сети	Th_{10}	~0
		- Wi-Fi	Th_{11}	0.001
		- с использованием админресурса	Th_{12}	~0
	- с использованием админресурса		Th_{13}	~0
Методы социальной инженерии			Th_{14}	0.1

Меры повышения безопасности пользователей ИБ

Рассмотрим теперь, какие контрмеры может принять пользователь ИБ для повышения свой безопасности.

1. Отказ от смартфона в пользу простого телефона без операционной системы.

При применении данной контрмеры исключаются уязвимости, связанные с установкой вредоносного ПО. Вероятность утечки данных через небезопасное Wi-Fi-соединение также окажется равна нулю – в простых телефонах нет функции доступа к Wi-Fi сетям. Кроме того, уменьшается вероятность похищения мобильного устройства, поскольку такие телефоны не представляют особой ценности для злоумышленников. Даже в случае похищения телефона критичность реализации будет невысока, поскольку статический пароль в простом телефоне не хранится.

2. Функция разблокировки по отпечатку пальца.

Эта функция не позволит мошеннику получить доступ к функциям телефона даже в случае его похищения, а также сделает невозможной установку вредоносного ПО на устройство, оставленное без присмотра. Это позволит защитить устройство от целого ряда уязвимостей.

3. Установка антивирусного ПО на смартфон делает его гораздо более устойчивым к атакам с использованием вредоносного ПО. Вероятность реализации угроз уменьшается.

4. Использование именной (не анонимной) sim-карты затруднит для злоумышленника получение ее дубликата методами СИ, что уменьшит вероятность реализации угрозы.

5. Использование отдельного смартфона для финансовых операций уменьшает вероятность взлома, связанную с наличием вредоносного ПО, при условии, что этот смартфон не

используется ни для чего больше, кроме как для финансовых операций. Также снижается вероятность атак с использованием методов СИ, если номер этого телефона не используется для других целей кроме ИБ. Уменьшаются также вероятности применения других способов взлома, если это устройство ни при каких обстоятельствах не передается в чужие руки.

6. Использование простого телефона для финансовых операций объединяет достоинства п. 1 и 5.

7. Использование sim-карты иностранного оператора связи затрудняет злоумышленникам и даже спецслужбам процедуру получения дубликата, следовательно, снижаются вероятности кражи и клонирования sim-карты. Кроме того, мошенники неохотно совершают дорогие международные звонки, что снижает вероятность атак методами СИ. Также сам пользователь, вероятнее всего, не будет использовать дорогой роуминговый интернет для посещения сторонних интернет-ресурсов и открывать фишинговые ссылки, что снижает вероятность установки вредоносного программного обеспечения.

8. Обязательное отключение телефона на ночь позволит избежать звонков от мошенников в то время, когда критичность восприятия получаемой информации снижается, а доверие к собеседнику возрастает [16]. При этом снижается вероятность использования методов СИ. Неактивность телефона в ночное время уменьшит возможность несанкционированного доступа к нему через Wi-Fi соединение в случае взлома роутера.

9. Отключение функции геолокации в смартфоне затруднит определение местоположения для потенциальных мошенников и сделает пользователя менее уязвимым к атакам методами СИ.

10. Отсутствие у пользователя профиля в социальной сети также усложняет для злоумышленников сбор информации о нем и ее использование при атаках методами СИ (при этом вовсе не обязательно, чтобы доступ к аккаунту осуществлялся с того же устройства). Также снизятся вероятности установки вредоносного ПО, поскольку утверждение, что социальные сети являются «рассадниками» вредоносного ПО, не лишено оснований.

Методика оценки эффективности контрмер

Для оценки эффективности перечисленных мер был проведен опрос экспертов, которым было предложено оценить, как повлияет каждая из предлагаемых мер на ту или иную уязвимость. Подчеркнем, что в отличие от предыдущего опроса (опроса пользователей), здесь опрос проводился именно среди специалистов, знакомых с принципами организации и работы мобильной связи и др. Качественные (лингвистические) оценки, данные экспертами, были переведены в численные значения K, названное коэффициентом ослабления угрозы по шкале, приведенной в табл. 4. В табл. 5 представлены осредненные по всем экспертам значения К для каждой из предлагаемых контрмер и по каждой из рассмотренных уязвимостей.

Таблица 4

Ответ эксперта	K
никак не повлияет	1
повлияет незначительно	0,8
повлияет умеренно	0,5
повлияет значительно	0,2
полностью устранит	0

Индексы коэффициентов $K_1 ... K_{14}$ соответствуют номерам уязвимостей из табл. 3.

Для расчета эффективности вводимых контрмер необходимо перемножить все соответствующие коэффициенты K_i. Тогда результирующие коэффициенты ослабления угроз определяются как

$$K_i^* = \prod_j K_i^j \,. \qquad (4)$$

где K_i^j – коэффициенты из табл. 4, причем индекс i соответствует уязвимости, индекс j – контрмере (номер строки из табл. 4). Перемножаются только коэффициенты, соответствующие принятым контрмерам.

Таблица 5

№	Уязвимость / Контрмера	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}
1	Отказ от смартфона в пользу телефона без ОС	0.7	1	1	1	0	0.23	0	0.23	0.3	0.8	0.05	1	0.3	1
2	Функция разблокировки по отпечатку пальца	0.28	0.88	1	0.88	1	1	1	0.38	0.38	1	1	1	0.88	1
3	Антивирусноее ПО на смартфоне	0.88	1	1	1	0.4	0.7	0.23	0.78	0.7	0.88	0.7	0.95	0.95	0.95
4	Использование именной sim-карты	0.95	0.65	0.23	0.78	1	1	1	1	1	1	1	1	1	1
5	Отдельный смартфона для финансовых операций	0.7	0.75	0.75	0.95	0.3	0.95	0.35	0.3	0.68	1	0.95	1	0.75	0.53
6	Отдельный телефон для финансовых операций	0.48	0.68	0.75	0.88	0.35	0.55	0.1	0.05	0.48	0.83	0.2	0.95	0.45	0.5
7	Использование роуминго-вой sim-карты	1	0.3	0.2	0.1	0.6	0.95	0.4	0.83	0.75	0.68	0.58	0.55	0.55	0.58
8	Обязательное отключение телефона на ночь	0.83	0.7	0.88	1	0.95	1	0.95	1	1	0.73	0.58	0.75	0.75	0.63
9	Отключение функции геолокации	0.95	1	1	1	1	1	1	0.95	1	1	1	0.95	0.95	0.85
10	Отсутствие профиля в социальной сети	0.88	0.95	0.83	0.95	1	1	1	1	1	1	0.95	1	1	0.7

Например, если пользователь установил антивирусное ПО на свой смартфон и пользуется sim-картой иностранного оператора (контрмеры 3 и 7), то уязвимость, вызванная потерей данных при переходе по фишинговой ссылке (столбец 7), будет оцениваться как:

$$K_7^* = K_7^3 \times K_7^7 = 0,23 \times 0,4 = 0,092.$$

Тогда уровень угрозы для всех уязвимостей с учетом принятых контрмер можно рассчитать как

$$CTh_{NEW} = 1 - \sum_{i=1}^{n} \left(1 - Th_i K_i^*\right). \quad (5)$$

Далее, применив выражение (3), можно вычислить риск, после чего оценить результирующую эффективность контрмер(ы) как

$$E = \frac{R_{OLD} - R_{NEW}}{R_{OLD}}. \quad (6)$$

Предложенные методики могут быть полезны для оценки эффективности не только мер, которые перечислены в данной статье, но и других, например предложенных в [17].

Выводы

1. Обобщены и проанализированы угрозы для пользователей ИБ, связанные с использованием телекоммуникационных сетей и средств связи. Следовательно, можно отметить, что для общего понимания угроз необходимо было наглядно показать все виды угроз, с которыми сталкивается ежедневно каждый пользователь ИБ.

2. Методом эвристического анализа и экспертных оценок предложена методика оценки уязвимости пользователя ИБ, обусловленная этими угрозами. Показано, что наибольшую угрозу представляют мобильные устройства с операционной системой, а также устройства, имеющие постоянный доступ к мобильной сети или Wi - Fi.

3. Также методом экспертных оценок обобщены способы повышения уровня защиты пользователей ИБ от угроз, связанных с использованием телекоммуникационных сетей и средств связи и предложена методика оценки их эффективности.

Список литературы:

1. Антипов И. Е., Найденова Д. Р. О численной оценки уязвимостей пользователей интернет-банкинга // Радіоелектроніка та молодь у XXI столітті, Харків, Україна, 2019. С. 152-153.

2. Названы основные способы кражи персональных данных россиян [Электронный ресурс]. Режим доступа: https://vz.ru/news/2019/7/13/987219.html

3. Операторы связи и ФСБ выступили против используемой в iPhone технологии [Электронный ресурс]. Режим доступа: https://www.rbc.ru/technology_and_media/08/04/2019/5ca8e3319a79470abf10b8ac?from=from_main

4. В компании Google рассказали об установленных еще до продажи вирусах в смартфонах с операционной системой Android. [Электронный ресурс]. Режим доступа: https://vz.ru/news/2019/6/10/981789.html

5. Шпион на границе: чем китайцы заражают телефоны туристов [Электронный ресурс]. Режим доступа: https://www.gazeta.ru/tech/2019/07/03/12473611/spying_china.shtml

6. Таможня США может проверять содержимое ваших девайсов, изымать их и даже запрашивать пароли [Электронный ресурс]. Режим доступа: http://nashiusa.com/novosti/tamojna-proverka-device/

7. СБУшник продавал данные о телефонных разговорах, в том числе известных людей [Электронный ресурс]. Режим доступа: https://inforesist.org/sbushnik-prodaval-dannye-o-telefonnyh-razgovorah-v-tom-chisle-izvestnyh-lyudej/

8. В Киеве банда торговала информацией из базы данных Нацполиции и МВД [Электронный ресурс]. Режим доступа: https://www.segodnya.ua/kiev/kaccidents/v-kieve-policeyskie-torgovali-informaciey-iz-bazy-dannyh-nacpolicii-i-mvd-1224346.html

9. Клонирование SIM-карт – так ли это просто? [Электронный ресурс]. Режим доступа: https://tech-geek.ru/sim-card-cloning/

10. Операции с SIM/ USIM-картами и номером [Электронный ресурс]. Режим доступа: http:// https://www.vodafone.ua/ru/support/sim-usim-card-operation

11. МТС на службе ФСБ? Как взломали аккаунты оппозиционеров в Telegram [Электронный ресурс]. Режим доступа: https://openrussia.org/notes/614328/

12. Три четверти мобильных приложений оказались небезопасными [Электронный ресурс]. Режим доступа: https://vz.ru/news/2019/6/19/983148.html

13. Как мошенники увели SIM-карту у киевского IT-аналитика и украли 285 000 грн. [Электронный ресурс]. Режим доступа: http://cripo.com.ua/investigations/kak-moshenniki-uveli-sim-kartu-u-kievskoj-it-analitika-i-ukrali-285-000-grn/

14. Мошенники придумали новый способ вламываться в «Приват-24» Электронный ресурс]. Режим доступа: https://minfin.com.ua/2017/09/28/30182177/

15. Методика оценки риска ГРИФ 2005 из состава Digital Security [Электронный ресурс]. Режим доступа: https://bugtraq.ru/library/security/grifarmet.html?k=9

16. Как отличить звонок мошенника от звонка сотрудника банка? [Электронный ресурс]. Режим доступа: https://aif.ru/money/mymoney/kak_otlichit_zvonok_moshennika_ot_zvonka_sotrudnika_banka

17. Антипов И. Е., Найденова Д.Р. Пути повышения защищенности абонента мобильной связи от определения местоположения // Радіотехніка та молодь у XXI столітті. Т. 3. С.113-114.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 07.02.2020