УДК 004.056.53
DOI: 10.15827/0236-235X.33: .324-327

Дата подачи статьи: 25.11.16
2017. Т. 30. № 2. С. 324–327

ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ СИСТЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

Т.А. Маркина, к.т.н., доцент, tmark812@mail.ru;

В.А. Хрупов, студент, od@mail.ifmo.ru

(Университет ИТМО, Кронверкский просп., 49, г. Санкт-Петербург, 197101, Россия)

В данной работе исследуется защищенность систем электронных платежей. Актуальность исследования обусловлена постоянным ростом количества преступлений в сфере электронных платежей, что подтверждается официальной статистикой. Пользователям систем электронных платежей необходимо иметь представление о защищенности этих систем, следовательно, и о защищенности своих денежных средств, хранящихся в них.

В процессе работы рассматривались разнообразные системы электронных платежей, проанализированы способы и методы, обеспечивающие безопасность систем, выявлены недостатки и достоинства способов и методов их защиты, определены критерии и подкритерии оценки защищенности, а для каждого из подкритериев определено значение показателя безопасности в процентах.

На основании значений показателей была произведена оценка защищенности систем электронных платежей, что позволяет сделать выводы о степени защищенности каждой из них.

Исследование позволяет дать оценку защищенности наиболее популярных систем электронных платежей на территории Российской Федерации и стран СНГ.

Ключевые слова: система электронных платежей, электронный платеж, электронные деньги, защищенность системы электронных платежей, мобильный сервис системы электронных платежей, немобильный сервис системы электронных платежей, карточная платежная система.

Информатизация современного общества несет в себе как позитивное, так и негативное начало. В связи с массовой компьютеризацией информационных процессов, увеличением ценности и значимости информационных ресурсов перед обществом встает острая проблема защиты информации и персонализированных данных, которые циркулируют в важных информационных системах, то есть предотвращение модифицирования, удаления и похищения для использования в криминальных целях.

Система электронных платежей (СЭП) – это технология (если говорить о реализации, то сервис), представляющая собой совокупность методов, договоренностей и подтехнологий и позволяющая производить расчеты между контрагентами по сетям передачи данных [1]. СЭП входят в сферу электронной коммерции. В настоящее время главной угрозой для электронной коммерции являются преступления в сфере информационных технологий, или киберпреступность [2]. Противоправные действия в области систем электронных платежей могут повлечь за собой нарушения в работе ЭВМ и привести СЭП, банк, а впоследствии и рыночную экономику к краху. Проблемами защиты данных в СЭП, в том числе электронных платежей, разработкой современных технических и клиентских средств защиты, а также усовершенствованием антивирусных систем сегодня занимаются многие отечественные и иностранные специалисты (см. [3, 4] и др.), а также крупные компании: Eset Software Ltd, Kaspersky AntiVirus [5] и многие другие. Существует значительное количество научных исследований и практических разработок, связанных с защитой СЭП, однако в силу постоянного разви-

тия технологий возникают новые проблемы, которые необходимо решать новыми способами [6].

Под защищенностью СЭП понимается совокупность технических и клиентских средств защиты, обеспечивающих требуемый уровень безопасности. В настоящий момент средства криптографической и технической защиты еще не имеют длительной истории успешной эксплуатации и безопасность (подделка, хищение, изменение номинала) не подтверждена широким обращением [2]. Теоретически возможны хищения электронных денег посредством инновационных методов в силу недостаточной зрелости технологий защиты [4]. Актуальность данного исследования подтверждена официальной статистикой. По данным МВД, в 2013 году зарегистрировано более 11 тысяч преступлений в сфере электронных платежей, а к середине 2014 года – более 7 тысяч [7]. По приведенной статистике можно судить о том, что количество преступлений в сфере электронных платежей растет с каждым годом. Это означает, что операторы СЭП не торопятся создавать и вводить новые методы и способы защиты платежей, а пользователям необходимо самим выбирать наиболее безопасные СЭП для оплаты товаров и услуг.

СЭП подразделяются на мобильные сервисы (приложения СЭП для мобильных устройств) и немобильные (браузерные СЭП, приложения СЭП для ПК). По видам оплаты СЭП подразделяют на карточные платежные системы и операторы электронных денег.

Платежные шлюзы – симбиоз карточных платежных систем и операторов цифровой наличности. Такие системы позволяют совершать практически все возможные транзакции в рамках одной

Таблица 1

Критерии и подкритерии безопасности (их особенности)

Table 1

Safety criteria and sub-criteria (their features)

Критерии и подкритерии безопасности (их особенности)		Значение показателя безопасности, %
1) Первичная защита аккаунта СЭП		
1. Защита аккаунта паролем (критерий 1)		
Наличие пароля аккаунта		10
Надежность пароля	Минимальный пароль 1 символ	0
	Минимальный пароль 5-6 символов	5
	Минимальный пароль 8 символов	10
	Наличие доп. условий (спец. символы, буквы верхнего регистра, цифры)	5
Наличие строки надежности пароля		2
Ограничение срока действия пароля СЭП		3
2. Использование безопасного соединения с веб-сайтом (критерий 2)		
Безопасность SSL-соединения	Не используется SSL-шифрование	0
	Применяется SSL-шифрование, но есть незащищенный контент, представляющий серьезную опасность	3
	Применяется SSL-шифрование, но обнаружен незащищенный контент	5
	Используется SSL-шифрование (безопасное соединение)	10
Используемый протокол	С протоколом TLS 1.1	5
	С протоколом TLS 1.2	10
2) Безопасность при авторизации в СЭП		
Подтверждение входа с помощью мобильного телефона, сервиса E-num или e-mail (критерий 3)	Мобильный телефон	5
	Сервис E-num	5
	E-mail	5
3) Авторизация с помощью технических настроек		
1. Возможность ограничения доступа по IP-адресу (критерий 4)		5
2. Выдача персонального цифрового сертификата для доступа в СЭП (критерий 5)		5
4) Подтверждение операций с кошельком дополнительным паролем		
Подтверждение операций (критерий 6)	С помощью SMS присылаемое на моб. телефон или e-mail	5
	С помощью сервисов E-num, Google Authenticator или другими подобными системами	5
	С помощью дополнительного платежного пароля	5
5) Дополнительные способы и методы, обеспечивающие безопасность денежных средств		
Возможность привязки почты/телефона к СЭП дополнительно (критерий 7)		3
1. Возможность выпуска или приобретения виртуальной карты с коротким сроком действия и лимитом средств (критерий 8)		3
2. Наличие идентификации с подтверждением документами пользователя (критерий 9)		3
3. Использование секретных вопросов или секретного слова (критерий 10)		3
4. Ограничение сессии – автоматический выход из системы по истечении времени неактивности пользователя (критерий 11)		3
6) Информационные способы обеспечения безопасности		
1. Информирование пользователя по SMS или e-mail об операциях, проводимых с электронным кошельком (критерий 12)		3
2. Наличие журнала посещений пользователем СЭП (критерий 13)		3
3. Наличие инструкций и рекомендаций по безопасности для пользователей СЭП (критерий 14)		3
4. Наличие службы поддержки (критерий 15)	По телефону	3
	Через форму обратной связи или e-mail	2

системы. Большинство СЭП можно отнести к шлюзам, но обычно каждая СЭП выделяет основной тип электронных платежей [3].

В ходе работы был проведен анализ способов и методов защиты мобильных и немобильных сервисов СЭП, таких как протоколы SSL и SET [1], объединенный протокол SSL и SET, CVV2- и CVK2-код, проверка адреса Address Verification Service, однофакторная и двухфакторная авторизация, электронные сертификаты пользователя,

E-num, электронный токен, привязка IP, биометрические данные и др. [8].

Анализ защиты мобильных сервисов СЭП показал, что у большинства методов и способов защиты выявлены недостатки и уязвимости, которые дают возможность хищения денежных средств пользователя. Однако законодательные и технические меры по ограничению платежей не позволяют похитить с помощью мобильных сервисов СЭП крупные денежные средства.

Также был проведен анализ защиты немобильных сервисов СЭП. Он показал, что у немобильных сервисов существует большое количество разных методов защиты и только половина из них имеют недостатки и уязвимости. Это позволяет использовать немобильные сервисы как безопасное средство платежей, однако именно через них злоумышленники крадут крупные денежные средства [9]. Исследование проводилось на сервисах СЭП, в частности, тех, которые используют в обороте эмитированные электронные деньги и не относятся к интернет-банкингам.

В процессе работы были определены критерии и подкритерии оценки защищенности СЭП (табл. 1). Если какой-то метод или способ безопасности отсутствует, значение безопасности данного критерия будет равно 0 %. В сумме все критерии дают оценку безопасности 100 %. Оценка защищенности системы зависит от количества набранных процентов из 100. Оценка А (отлично) – от 90 % (включительно) и выше, оценка В (хорошо) – от 80 % (включительно) до 90 %, оценка С (удовлетворительно) – от 70 % (включительно) до 80 %, оценка F (неудовлетворительно) – результаты менее 70 %.

Всего выделено 15 критериев безопасности, они разбиты на 6 групп по степени безопасности. Например, в первой подгруппе первый критерий –

защита аккаунта паролем, где подкритериями выступают наличие пароля, надежность пароля (то есть минимальный пароль начинается от 1, 5, 8 символов, необходимо ли вводить дополнительные символы), наличие строки надежности пароля, ограничение срока действия пароля системой (например несколько месяцев). Вторым критерием в группе является использование безопасного соединения веб-сайтом, где подкритериями являются безопасность SSL-соединения (то есть используется ли SSL-шифрование и есть ли незащищенный контент на веб-странице), вторым подкритерием является используемый протокол (TLS 1.1 или 1.2, в котором не используются небезопасные алгоритмы шифрования).

Для исследования были взяты 12 систем электронных платежей, имеющих интерфейс на русском языке и находящихся в доменной зоне RU [10]. Это обусловлено тем, что именно эти системы под прицелом у злоумышленников из-за большого количества пользователей. Выбор этих систем немаловажен для рядовых пользователей, так как каждый человек хочет иметь наиболее защищенный инструмент электронных платежей. Результаты исследования представлены в таблице 2.

Исследование показало, что лишь две СЭП – WebMoney и OKPAY – имеют оценку «хорошо» (В). Всего три СЭП (VISA QIWI-кошелек, PayPal,

Таблица 2

Защищенность систем электронных платежей

Table 2

Security of electronic payment systems

№	СЭП	Критерий															
		Защита аккаунта СЭП паролем		Безопасность при авторизации в СЭП	Авторизация с помощью технических настроек		Подтверждение операций с кошельком доп. паролем	Дополнительные способы и методы						Информационные способы обеспечения безопасности			Оценка, сумма показателей
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1	VISA QIWI-кошелек	27	20	0	0	0	5	3	3	3	0	3	3	0	3	6	C – 76 %
2	Яндекс. Деньги	18	15	0	0	0	5	3	0	3	3	0	3	3	3	6	F – 62 %
3	WebMoney	15	20	0	5	5	5	3	3	3	3	3	3	3	3	6	B – 80 %
4	PayPal	25	20	0	0	0	5	3	0	3	3	3	3	0	3	6	C – 74 %
5	RBK Money	18	20	0	5	0	5	3	0	3	3	3	3	0	3	6	C – 72 %
6	Rapida online	10	20	0	0	0	5	3	3	3	0	3	3	0	0	6	F – 56 %
7	Элекснет	10	8	0	0	0	5	3	0	3	3	3	3	0	0	6	F – 44 %
8	Wallet One	15	20	0	0	0	5	3	0	3	0	3	3	3	0	6	F – 61 %
9	Сомерау-кошелек	20	15	0	0	0	5	0	0	3	0	3	3	0	0	6	F – 55 %
10	Payeer-кошелек	20	15	5	0	0	5	3	0	3	3	3	3	3	0	6	F – 69 %
11	OKPAY	25	20	5	5	0	0	3	0	3	3	3	3	3	3	6	B – 82 %
12	MoneyMail	10	15	0	0	0	5	3	0	3	0	0	3	3	0	6	F – 48 %

РВК Money) получили оценку «удовлетворительно» (С). Все остальные СЭП получили оценку неудовлетворительно, среди них и Яндекс.Деньги. Для проведения электронных платежей можно рекомендовать использовать СЭП, получившие оценку «удовлетворительно» и выше, но при условии, что пользователь будет следовать инструкциям и рекомендациям СЭП, незамедлительно реагировать на подозрительные действия со своим электронным кошельком и сообщать об этом в службу поддержки СЭП, которую он использует.

Литература

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб: Питер, 2012. 960 с.
2. Иванов М.А., Михайлов Д.М., Чугунков И.В. Защита

информации в электронных платежных системах. М.: КНОРУС, 2011.

3. Голдовский И. Безопасность платежей в Интернете. СПб: Питер, 2005. 240 с.
4. Уэллс Т. Компьютерное мошенничество. Битва байтов. М.: Маросейка, 2010. 354 с.
5. Официальный веб-сайт лаборатории Касперского. URL: <http://www.kaspersky.com> (дата обращения: 15.07.16).
6. Ануреев С.В. Платежные системы и их развитие в России. М.: Финансы и статистика, 2005. 288 с.
7. Официальный веб-сайт делового портала TADVISER. URL: <http://www.tadviser.ru> (дата обращения: 15.07.16).
8. IT-сообщество Хабрахабр. URL: <http://habrahabr.ru> (дата обращения: 15.07.16).
9. Гризов А. Новые платежные технологии. Информационно-справочное издание. М.: Рекон Интернешнл, 2009. 468 с.
10. Официальный веб-сайт информационного агентства «Банки.ру». URL: <http://www.banki.ru> (дата обращения: 15.07.16).

Software & Systems

DOI: 10.15827/0236-235X.118.324-327

Received 25.11.16

2017, vol. 30, no. 2, pp. 324–327

INVESTIGATION OF SECURITY OF ELECTRONIC PAYMENT SYSTEMS

T.A. Markina¹, Ph.D (Engineering Sciences), Associate Professor, tmark812@mail.ru

V.A. Khrupov¹, Student, od@mail.ifmo.ru

¹ ITMO University, Kronverksky Ave. 49, St. Petersburg, 197101, Russian Federation

Abstract. The article investigates security of electronic payment systems. The relevance of this study is confirmed by the official statistics, which shows the increase of the number of crimes in the field of electronic payments year by year. Therefore, users of these systems need to be aware of the security of electronic payment systems, consequently, about the security of their money stored in these systems.

The work considers a variety of electronic payment systems, analyzes the ways and methods of ensuring the security of electronic payment systems, identifies advantages and disadvantages of techniques and methods of electronic payment system protection, the criteria and sub-criteria for evaluation of electronic payment system security, and determines value security index in percentage terms for each sub-criteria.

Based on the values of the indicators the authors assessed security of electronic payment systems and received an overall assessment for each electronic payment system. Based on the assessment, the paper shows some conclusions about the degree of security of an electronic payment system.

This study demonstrates the assessment of security of the most popular electronic payment systems in the Russian Federation and CIS countries.

Keywords: electronic payment systems, electronic payment, e-money, security, electronic payment systems, mobile service electronic payment system, no mobile service electronic payment systems, card payment system.

References

1. Tanenbaum A., Wetherall D. *Computer Networks*. 5th ed., Prentice Hall Publ., 2010, 962 p.
2. Ivanov M.A., Mikhaylov D.M., Chugunkov I.V. *Zashchita informatsii v elektronnykh platezhnykh sistemakh* [Data Protection in Electronic Payment Systems]. Moscow, KNORUS Publ., 2011.
3. Goldovsky I. *Bezopasnost platezhey v Internetе* [Secure Payments on the Internet]. St. Petersburg, Piter Publ., 2005, 240 p.
4. Wells J.T. *Computer Fraud Casebook: The Bytes that Bite*. Wiley Publ., 2009, 440 p. (Russ. ed.: Moscow, Maroseyka Publ., 2010, 354 p.).
5. *Kaspersky Lab*. Official website. Available at: <http://www.kaspersky.com> (accessed July 15, 2016).
6. Anureev S.V. *Platezhnye sistemy i ikh razvitie v Rossii* [Payment Systems and Their Development in Russia]. Moscow, Finansy i statistika Publ., 2005, 288 p.
7. *TADVISER*. Official website. Available at: <http://www.tadviser.ru> (accessed July 15, 2016).
8. *IT-community Habrahabr*. Available at: <http://habrahabr.ru> (accessed July 15, 2016).
9. Grizov A. *Novye platezhnye tekhnologii. Informatsionno-spravочное izdanie* [New Payment Technologies. Information and Reference Edition]. Moscow, Rekon Interneshnl Publ., 2009, 468 p.
10. *Banki.ru*. Official website. Available at: <http://www.banki.ru> (accessed July 15, 2016).