УДК 336.7

ГРАМОТНОЕ ИНФОРМАЦИОННОЕ ОБЩЕСТВО, ПРОТИВОСТОЯЩЕЕ КИБЕРУГРОЗАМ ПРИ ПОТРЕБЛЕНИИ ЦИФРОВЫХ ФИНАНСОВЫХ ПРОДУКТОВ

Анисимов Е. С.,

студент Факультета информационных технологий и анализа больших данных, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»,

г. Москва, Россия

Аннотация

Статья посвящена анализу роли высокого уровня знаний потребителей цифровых финансовых услуг о возможностях снижения рисков информационной безопасности. В рамках работы особое внимание уделяется существующим практикам просветительской деятельности в сфере повышения киберграмотности и статистическим данным, отражающим угрозы с высокой в текущих условиях вероятностью реализации. Благодаря этому была получена форма закрепления киберграмотности в структуре информационного общества, а также ряд примеров, отражающих потенциальный эффект от приобретения информационным обществом такого важного качества.

Ключевые слова: информационное общество, Банк России, киберграмотность, информационная безопасность, социальная инженерия, телефонное мошенничество.

LITERATE INFORMATION SOCIETY THAT RESISTS CYBER THREATS IN THE CONSUMPTION OF DIGITAL FINANCIAL PRODUCTS

Anisimov E. S.

student of the Faculty of Information Technology and Big Data Analysis

Financial University under the Government of the Russian Federation
Moscow, Russia

Abstract

The article is devoted to the analysis of the role of a high knowledge of consumers in using digital financial services about methods of reducing cyber risks. Within the framework of the article, special attention is paid to the existing practices of educational activities to increase cyber literacy and statistical data reflecting threats with a high probability of implementation in the current conditions. As the result of the review, a form of consolidation of cyber literacy in the structure of the information society was obtained, as well as some examples reflecting the positive effect of the acquisition this important quality by the information society.

Keywords: information society, Bank of Russia, cyber literacy, information security, social engineering, phone fraud.

В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы информационное общество определено как общество, в котором информация и уровень её доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан [7]. Сегодня нельзя не признавать занимаемое во всех сферах центральное место информации и информационных технологий, особенно в банковской и экономической сфере в целом. В ближайшее время начнётся тестирование и по его результатам запуск цифрового рубля. Данный проект отражает важность цифровизации для государства, а также перспективность использования информационных технологий даже в классических вопросах.

Выделение банковского сектора неслучайно, поскольку экономические условия тесно связаны с функционированием банков. Клиенты кредитных организаций во время использования дистанционных банковских сервисов и

совершения интернет-платежей зачастую осуществляют действия, приводящие к всевозможным инцидентам, среди которых серьёзный ущерб приносят хищения денежных средств. В связи с этой проблемой возникает две важные задачи: первая связана с повышением уровня киберграмотности потребителей финансовых услуг, вторая же заключается в необходимости повышенного внимания со стороны компаний к информационной безопасности. Высокий уровень знаний о рисках, связанных с информационными технологиями, позволит не поддаваться на противоправные мошеннические действия и самостоятельно не создавать условий для совершения атак. Второй важный вопрос допустимо раскрыть как неотъемлемую часть ответственного менеджмента, поскольку развитие информационной защиты положительно скажется на репутации организации, а также на её финансовой устойчивости. При этом очевидно, что внимание должно быть двунаправленным: внешним и внутренним. В рамках внешней информационной безопасности будет выполняться и первая поставленная в рамках статьи задача: в ходе обучающей работы с потребителями услуг специалисты компании будут формировать доверительное и внимательное отношение к ним, а клиенты благодаря этой работе увидят компетентность банка и повысят свою информационную грамотность.

Статистика Банка России за первое полугодие 2021 года подтверждает актуальность исследуемой проблемы. В большей степени необходимость принятия комплексных мер по повышению киберграмотности обуславливается высокими темпами роста операций без согласий клиента, а также большой долей социальной инженерии в ряде инцидентов. Серьёзные изменения в начале 2021 года на основании этих данных наблюдаются в направлении дистанционного банковского обслуживания юридических лиц, что отражено в таблице 1 [2; 3; 4; 5 с. 9].

Таблица 1. Количество операций без согласия клиентов по каналам дистанционного банковского обслуживания юридических лиц в 2020 году и I полугодии 2021 года

Период	Число операций без согласия, ед.	Доля социальной инженерии, %
I кв. 2020 года	576	44
II кв. 2020 года	809	29
III кв. 2020 года	558	34
IV кв. 2020 года	990	31
I кв. 2021 года	1504	79
II кв. 2021 года	984	74

Рассматривая дополнительную информацию, касающуюся объёма произошедших инцидентов у юридических лиц, приходим к подтверждению сформулированного в начале тезиса о тесной взаимосвязи экономических условий общества с использованием банковского обслуживания. Снижение среднего чека операции без согласия в I квартале 2021 года относительно аналогичного периода предшествующего года (401,1 тысячи рублей в I кв. 2020 года и 373,9 тысячи рублей в I кв. 2021 года) не явилось существенным прогрессом, поскольку среднее за I квартал 2021 года оказалось выше, чем за весь 2020 год (средний объём операции в 2020 году составил 347,8 тысяч рублей). А если рассматривать динамику того же среднего размера операции без согласия клиента в рамках первого полугодия текущего года, то он вырос во втором квартале на 31% по сравнению с первым, составив 489,7 тысяч рублей [3; 4; 5 с. 9]. Помимо этого, в тот же период почти 4 из 5 инцидентов произошло в результате воздействия социальной инженерии. Приведённые в качестве примера аналитические данные Центрального банка Российской Федерации подтверждают потребность в координированных действиях участников банковской системы России.

Прежде чем провести анализ отечественной практики, можно обратиться к зарубежному опыту развития у потребителей финансовых услуг знаний об угрозах информационной безопасности, рисках, а также действиях по их недопущению, что вместе и составляет в узком смысле понятие

киберграмотности. Анализируя официальные пресс-релизы иностранных компаний и органов власти, а также статьи в средствах массовой информации, приходим к выводу, что негативное явление социальной инженерии, направленной на клиентов финансовых организаций, носит международный характер [11, 12]. Например, в США многочисленные раскрытия персональных данных граждан и существенные денежные хищения послужили поводом к инициированию 22 июня 2021 законопроекта, посвященного киберграмотности [9]. В случае принятия этого американского закона будет официально закреплена кампания по регулярному повышению уровня знаний в сфере информационной безопасности у жителей США. Подобные превентивные меры можно найти и среди внутренних нормативных документов зарубежных организаций, в которых руководство ответственно подходит к вопросам защиты информации и не хочет, чтобы сотрудники теряли бдительность, нанося ущерб себе или компании [10].

В России на государственном уровне работа по обучению потребителей, связанных с финансовыми услугами, началась ещё раньше, чем в приведённом шаге со стороны американских конгрессменов. С правильным прицелом в будущее и в качестве верного ответа на настоящие вызовы Банк России в 2020 году продолжил запускать комплекс мероприятий по повышению грамотности при пользовании цифровыми финансовыми продуктами. Началась работа и ранее, например, Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России ещё в 2019 году получил премию за проведение онлайн-уроков для детей по безопасности в киберпространстве [1]. В отмеченном 2020 году масштабность планомерной работе была придана за счёт запуска Всероссийского диктанта по финансовой киберграмотности. Стоит отметить большую заслугу Центрального банка Российской Федерации в значительном объёме позитивной для общества работы, потому что этому событию предшествовали планомерные действия в виде пилотных проектов, успешно написанных пробных межрегиональных диктантов и упомянутых ранее онлайн-уроков.

Сформулированная модель двунаправленной ориентации мероприятий по повышению киберграмотности уже присутствует в ряде кредитных организаций. Пример обращения внимания на своих клиентов: один из самых атакуемых банков в Европе – Сбербанк – в одном из своих пресс-релизов 2021 года подчеркнул, что в приоритеты работы банка входит безопасность финансов пользователей. Аналогично отмечается, что киберграмотность граждан позволит предотвращать инциденты социальной инженерии. Результатом комплекса мер стал, на основании информационного сообщения, ежегодный рост уровня киберграмотности населения [6].

Таким образом, в настоящее время отмечается высокая отрицательная активность в финансовой сфере со стороны злоумышленников. Модели поведения мошенников носят самый разнообразный характер, однако общей характерной особенностью является высокая доля использования социальной инженерии. Данный механизм мошенники вносят в случаях попыток хищения денежных средств у физических и юридических лиц. Это свидетельствует о высокой диверсификации противоправной деятельности. Данная ситуация – катализатор решительных мер противодействия со стороны государства. В этом направлении значительных успехов достигает Центральный банк Российской Федерации. Показательным является разнонаправленное противодействие мошенникам со стороны регулятора. Он не только проводит работу по повышению осведомлённости потребителей об угрозах при пользовании цифровыми финансовыми продуктами, но и выявляет средства совершения правонарушений. Популярное телефонное мошенничество в скором времени примет обратный тренд к снижению, причиной чему среди прочего является деятельность Банка России. Во II квартале 2021 года регулятор выявил на 94% больше мошеннических телефонных номеров, чем за I квартал этого же года. Их состав представлен в таблице 2 [3; 4]. Увеличению результативности способствовало в том числе принятие закона, вносящего изменения в

Федеральный закон «О связи» в части блокировки операторами звонков с подменных номеров [8].

Таблица 2. Выявленные Банком России мошеннические телефонные номера

Номер\Период	I кв. 2021 года	II кв. 2021 года
Городские телефонные номера	4185	8475
Мобильные телефонные номера	1786	3166
Номера 8800	133	208
Всего	6104	11849

Подводя итог проведённому исследованию, главным его выводом стало формулирование метода борьбы с распространённым видом мошенничества – социальной инженерией. Методика основывается на необходимости широкой программы по повышению киберграмотности. Программа должна быть в формах, доступных для всех возрастов. Она необходима как для граждан – потребителей цифровых финансовых услуг, так и для сотрудников различных организаций. Это проявление сформулированной двунаправленной модели работы по повышению осведомлённости.

По убеждению автора, подобная программа заслуживает место в системе национальных проектов Российской Федерации, поскольку у грамотного в цифровой сфере информационного общества будет расти уровень экономических условий жизни. Помимо этого, такое общество станет лучше понимать преимущества и принципы использования цифрового рубля, переходя тем самым от традиционных форм денежных средств к вводимой в скором времени гораздо активнее.

Библиографический список

1. Банк России получил Премию Рунета за обучение детей киберграмотности. [Электронный ресурс]. – Режим доступа – URL: https://www.cbr.ru/press/event/?id=5241 (Дата обращения: 10.09.2021)

2. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. III квартал 2019/2020 года. Банк России. [Электронный ресурс]. – Режим доступа – URL: https://www.cbr.ru/analytics/ib/review_3q_2020/ (Дата обращения: 15.09.2021)

3. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. I квартал 2021 года. Банк России. [Электронный ресурс]. – Режим доступа – URL: https://www.cbr.ru/analytics/ib/review_1q_2021/ (Дата обращения: 16.09.2021)

4. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. II квартал 2021 года. Банк России. [Электронный ресурс]. – Режим доступа – URL: https://www.cbr.ru/analytics/ib/review_2q_2021/ (Дата обращения: 16.09.2021)

5. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2020 год. Банк России. [Электронный ресурс]. – Режим доступа –URL: https://www.cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf (Дата обращения: 16.09.2021)

6. Сбер завоевал три награды международной премии Cyber Security Excellence Awards. [Электронный ресурс]. – Режим доступа – URL: https://www.sberbank.ru/ru/press_center/all/article?newsID=fef5bfda-60b7-420a-92e4-2e9b6debbec0&blockID=1303&regionID=77&lang=ru&type=NEWS (Дата обращения: 20.09.2021)

7. Указ Президента Российской Федерации от 9 мая 2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»

8. Федеральный закон от 2 июля 2021 года № 319-ФЗ «О внесении изменений в Федеральный закон «О связи»

9. H.R.4055 — American Cybersecurity Literacy Act. 117th Congress (2021-2022). [Электронный ресурс]. – Режим доступа – URL:

https://www.congress.gov/bill/117th-congress/house-bill/4055/text (Дата обращения: 14.09.2021)

10. Social Engineering Education Policy. *Version 2*. University of Dallas, 2020. [Электронный ресурс]. – Режим доступа – URL: https://udallas.edu/offices/technology/_documents/Social%20Engineering%20Education%20Policy.pdf (Дата обращения: 20.09.2021)

11. Sushruth Venkatesha, K. Rahul Reddy, B. R. Chandavarkar. Social Engineering Attacks During the COVID-19 Pandemic. *Springer Nature Computer Science.* 2021; 2(2): 78.

12. The psychology of social engineering – the “soft” side of cybercrime. Diana Kelley, Microsoft. [Электронный ресурс]. – Режим доступа – URL: https://www.microsoft.com/security/blog/2020/06/30/psychology-social-engineering-soft-side-cybercrime/ (Дата обращения: 20.09.2021)

Оригинальность 76%