Copyright © 2021 by Sochi State University

Published in the Russian Federation
Sochi Journal of Economy
Has been issued since 2007.
ISSN: 2541-8114
2021, 15(1): 4-11

www.vestnik.sutr.ru

Articles

UDC 336

Cybercrime in the Financial Sphere

Alla Yu. Baranova [a, *], Polina Gasparyan [a]

[a] Sochi State University, Russian Federation

Abstract

Cybercrime is a crime in a virtual (Internet) space. Cyberspace (virtual space) is a simulated information space using computers and other devices, in which various data are located: Information on objects, persons, facts, phenomena, events and processes presented in mathematical, symbolic or any other form, as well as in motion on local and global computer networks, or information stored in the memory of any real or virtual device, as well as other media specifically designed for their storage, processing and transfer of data.

The relevance of this topic is confirmed by the increase in crimes in cyberspace. Cyber fraud and other types of crime in the IT environment – they have absolutely no borders, they are not stopped by state borders, nor by other continents, nor by any other restrictions existing in the real world. Unfortunately, official statistics only describe the tip of the iceberg, and therefore we increasingly hear about new cases, schemes and methods of cybercrime. The twenty-first century is the century of the emergence of scientific discoveries and new technologies in the IT field. An increasing number of people are victims of Internet scams. And at the same time, user awareness remains at the same, insufficient level. In the context of the accelerating development of high technologies, it is necessary to study the development of crimes on the Internet.

The purpose of the article is to develop proposals to ensure the safety of consumers of financial services.

Keywords: cybercrime, Internet security, financial services.

1. Введение

Преступление, совершенное в киберпространстве, — это виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ (Иванова, 2019: 27-28; Бутусова, 2016: 49; Чекунов, 2013: 7).

Но, несмотря на то, что международная киберпреступность становится всё более всеобъемлющей и опасной, причём не только в разрезе «классических» уголовных преступлений, таких как кражи, различные виды мошенничеств, в киберсреде всё больше происходит преступлений, связанных с актами терроризма, торговлей людьми, наркотиками, оружием, а также воздействием на инфраструктуру государств, которое может вполне влиять на жизни большого количества людей, усилия международного сообщества

* Corresponding author
E-mail addresses: baranovalla-77@mail.ru (A.Yu. Baranova)

всё ещё разрозненны, и страны больше заботятся о сохранности своих данных и национальном суверенитете.

2. Материалы и методы

В методологическую основу исследования положены следующие основные методы и подходы: абстрактно-логический, аналитический, статистический.

Объектом исследования являются преступления в интернет-среде, с которыми сталкиваются потребители финансовых услуг.

Предмет исследования: правовые и экономические аспекты киберпреступлений.

Теоретической и статистической базой исследования являются: теоретические разработки различных авторов, международные и российские нормативно-правовые акты, а также статистика МВД.

3. Обсуждение

Рассмотрим, какие международные усилия реализуются для расследования и предотвращений интернет-преступлений.

Главным и фактически единственным (по крайней мере, универсальным и международным) документом является «Конвенция Совета Европы о киберпреступности». Россия к ней не присоединилась, мотивируя это нежеланием, чтобы данные наших органов правопорядка в автоматическом режиме предоставлялись всем участником данного соглашения. Хотя, с другой стороны, в 2019 году Генеральная Ассамблея ООН приняла резолюцию, которая даёт старт разработки Конвенции о киберпреступлениях уже под эгидой ООН. Но пока ещё, большая часть сотрудничества происходит в двустороннем формате, или по линии определённых организаций, например, Интерпола (Конвенция о преступности..., 2001).

Конвенция Совета Европы о киберпреступности говорит о четырех типах компьютерных преступлений «в чистом виде», определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

1. Незаконный доступ — ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);
2. Незаконный перехват — ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);
3. Вмешательство в данные — ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);
4. Вмешательство в систему — ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных) (Конвенция о преступности..., 2001).

В Уголовном Кодексе Российской Федерации в статье 159.6 представлено следующее определение: «Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» (Уголовный кодекс Российской Федерации, 2020).

В Уголовном Кодексе РФ можно найти 6 статей о кибермошенничестве и киберпреступлениях:

- Статья 159.3. Мошенничество с использованием электронных средств платежа;
- Статья 159.6. Мошенничество в сфере компьютерной информации;
- Статья 272. Неправомерный доступ к компьютерной информации;
- Статья 273. Создание, использование и распространение вредоносных компьютерных программ;
- Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (Уголовный кодекс Российской Федерации, 2020).

Рассмотрим основные виды мошенничеств в киберсреде, с которыми сталкиваются потребители финансовых услуг (Сазанов, 2018: 55-58; Братусин, Власенко: 292-294; Бородкина, Павлюк, 2018: 135-137; Быков, 2016:9-11):

1. Фишинг – заключается в получении доступа к личным данным пользователя, чаще всего логинам и паролям, например от интернет-банков. Самый популярный способ – это заставить пользователя ввести свои данные (например, данные пластиковой карты) на поддельном сайте, который практически не отличается от настоящего.
2. Фарминг – подвид фишинга, где есть одно отличие, когда в компьютер пользователя внедряется вирус, скрытно и незаметно перенаправляющий человека на поддельные сайты, даже если человек удостоверился в названии домена и проверил сертификат безопасности сайта. Защититься от этого невозможно, как нельзя бороться с тем, о чём не подозреваешь даже. Лишь качественные антивирус поможет не пустить вирус.
3. Методы социальной инженерии заключаются в комбинировании технических и психологических методов влияния или давления на человека. В эту категорию и входят звонки от «Службы безопасности Сбербанка». Суть данного метода заключается в том, чтобы различными способами: доверие, спешка, давление или угрозы вывести человека из равновесия. Распространенным примером является сообщение потребителю финансовых услуг о том, что с его карты вот-вот спишется крупная сумма денег и для предотвращения этого необходимо сообщить полные данные карты.
4. Отравление SEO (Search Engine Optimization) — угрозы при вводе запроса, связанного популярными сайтами (соцсетями и интернет-банкинга). Защититься от таких угроз можно, используя актуальные версии шлюзового антивируса, проверяющего интернет-соединение в режиме реального времени, и системы предотвращения вторжений. Метод схож с фишингом.

Ранее мы рассмотрели относительно новые и развивающиеся методы обмана, связанные с появлением интернета. Далее (с 5 пункта) мы рассмотрим методы интернет-мошенничеств, которые процветали до эры интернета (Кочкина, 2017:1-8).

5. Мошенничество в интернет-магазинах – тут спектр достаточно обширен: цена на сайте отличается от фактической цены, товар может быть не доставлен покупателю или будет ненадлежащего качества. Метод предотвращения – пользоваться проверенными крупными площадками.
6. Мошенничество со сбором денег, начиная от краудфандинга на уважаемых и надежных площадках до сбора денег на лечение больных детей. Способ один – критичное мышление и проверка всей информации, включая банковские реквизиты.
7. Целый список отчасти «добровольных» методов мошенничества с применением социальной инженерии, куда включены финансовые пирамиды, бинарные опционы, биржевая торговля, рынок ФОРЕКС, различные бизнес-тренинги и семинары, другие различные схемы сетевого маркетинга.
8. Ещё больший список преступлений, только опосредованно связанных с интернетом (где интернет выступает лишь как средство коммуникации и координации преступлений в «офлайне»). К ним относятся: торговля людьми, наркотиками и оружием, распространение нелегальной информации, баз данных.
9. Хакерские атаки на инфраструктуру (конкурентов или неугодных стран), промышленный и международный шпионаж, взлом серверов государственных учреждений, спецслужб и военных объектов – это лишь неполный список киберпреступлений высшего уровня. Ущерб от таких атак составляет миллиарды долларов. Ещё несколько лет и хакерские атаки станут не менее разрушительным оружием, чем пушки и танки.

5. Результаты

За последние годы, количество преступлений в сфере высоких технологий растёт.

За этим могут стоять следующие предпосылки:

- всё большее проникновение новых технологий в повседневную жизнь, безналичный расчёт, интернет-покупки, мобильный банкинг;
- законодательная основа, которая недостаточно полно регулирует проблемы киберпространства;
- сложность расследования и раскрытия;
- сложность сбора доказательств и процесса доказывания по причине возникновения подобного определения как «виртуальный след»;

• отсутствие обобщенной судебной и следственной практики;
• отсутствие единой программы предотвращения и борьбы с киберпреступлениями;
• несогласованность в работе многих ведомств, комплексная совместная работа которых могла бы переломить негативный тренд.

На Рисунке 1 представлена статистика количества и раскрываемости кибермошенничества.

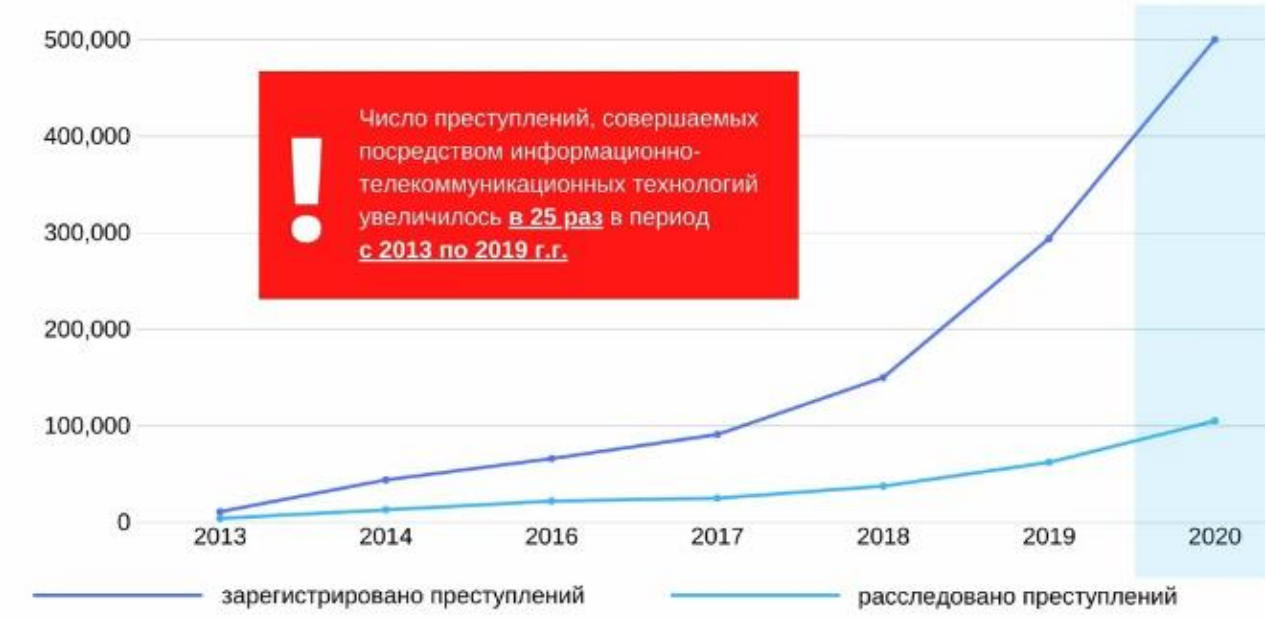

Рис. 1. Статистика киберпреступлений с 2013 года (Отчёт официального представителя МВД РФ, 2020)

По словам Ирины Волк, официального представителя МВД России: «Число преступлений, совершенных с использованием информационно-коммуникационных технологий, в 2020 году выросло на 94,6 %, в том числе тяжких и особо тяжких – на 129,7 %. При этом пластиковые карты использовались в преступных целях почти в 6 раз чаще, чем годом раньше, а средства сотовой связи – более чем в 2 раза чаще» (Отчёт официального представителя МВД РФ, 2020).

Негативным аспектом является не сам рост в абсолютных цифрах, а то, что раскрываемость данных преступлений критическим образом не успевает за ростом преступности в данной сфере. И если показатель раскрываемости колебался от ~50 % в 2014–2016 годах, то в 2020 году он уже составлял около 20 %.

Имеется ряд объективных трудностей в раскрытии преступлений в сфере высоких технологий. Одной из них является нежелание потребителей финансовых услуг заявлять о совершённом против них преступлении в полицию, другой – недостаточная финансовая грамотность людей, столкнувшихся с IT преступностью. Еще одна проблема раскрытия и предотвращения киберпреступлений – это высокий профессионализм киберпреступников, причем не только в техническом, но и психологическом аспектах.

Если в Конвенции Совета Европы о киберпреступности выделялось 9 типов киберпреступлений, то последние резолюции Генеральной Ассамблеи ООН выделяют уже 30 видов. Рост разнообразия преступлений не отстаёт от развития технологий (Официальное заявление МИД РФ о принятии Генасамблеей ООН резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях»).

Потребителям финансовых услуг можно предложить следующие основные правила, обеспечивающие безопасность в киберсреде:

1. Не переходить по подозрительным ссылкам, даже поступающим от знакомых людей.
2. При посещении важных сайтов, и особенно при вводе личных данных, проверять доменное имя и актуальность сертификатов безопасности.

3. Реже использовать публичный Wi-Fi, потому что через этот вид соединения могут быть похищены личные данные и проникнуть вирусы на устройство.
4. Не устанавливать программы из неизвестных источников.
5. Не использовать один и тот же пароль сразу для многих критических аккаунтов: например, для соцсетей, почты, интернет-банкинга.
6. Применять антивирусы.
7. Всегда обновлять программное обеспечение на компьютере и телефоне: операционную систему, браузеры и антивирусы.
8. По возможности раскрывать в киберпространстве как можно меньше информации, это будет сильно препятствовать мошенникам использовать эту информацию (Сбербанк поддержал создание..., 2018).
9. Критически относиться к утверждениям, которые звучат слишком хорошо, чтобы быть правдой. Различные способы заработать: казино, игровые автоматы, сетевой маркетинг, финансовые пирамиды, инновационные инвестиционные стратегии и прочие невероятные способы позволяют заработать лишь их создателям (Сериева, 2017: 104-106; Пять правил..., 2021).

5. Заключение

Киберпреступность и кибермошенничество являются объективным следствием глобализации и развития информационных процессов, появления глобальных компьютерных сетей. Информационные технологии всё больше проникают в нашу жизнь, онлайн смешивается с офлайном и сейчас уже сложно провести границу между ними. И чем больше это влияние, тем большая опасность исходит от интернет-мошенников.

По данным МВД России за последние 7 лет количество преступлений в интернете – выросло в 25 раз. И в то же время раскрываемость данных преступлений упала с 50 % до 20 %, и можно предположить, что она продолжит падать, если не будут предприняты существенные усилия в борьбе с киберпреступлениями.

Необходимость защиты от киберпреступников очевидна. Работа должна вестись не только в разрезе улучшения работы правоохранительных органов, необходимо совершенствовать системы безопасности банков, приложений и сайтов. Но главный вклад в борьбу с интернет-мошенниками – это осведомлённость и подготовленность потребителей финансовых услуг к атакам (техническим или психологическим) преступников. Борьба с киберпреступлениями должна носить комплексный и трёхсторонний характер: и бизнес (соцсети, банки), и государство, и граждане одинаково заинтересованы в уменьшении масштабов интернет-преступлений.

Литература

Бородкина, Павлюк, 2018 – *Бородкина Т.Н., Павлюк А.В.* Киберпреступления: понятие, содержание и меры противодействия // *Социально-политические науки*. 2018. № 1. С. 135-137.

Братусин, Власенко, 2019 – *Братусин А.Р., Власенко Е.Е.* О характерных индивидуально-типологических особенностях и поведенческих паттернах личности типичных жертв финансового мошенничества // *Проблемы современного педагогического образования*. 2019. №64-4. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/o-harakternyh-individualno-tipologicheskih-osobennostyah-i-povedencheskih-patternah-lichnosti-ti pichnyh-zhertv-finansovogo

Бутусова, 2016 – *Бутусова Л.И.* К вопросу о киберпреступности в международном праве // *Вестник экономической безопасности*. 2016. №2. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/k-voprosu-o-kiberprestupnosti-v-mezhdunarodnom-prave

Быков, 2016 – *Быков В. и др.* Совершенствование уголовной ответственности за преступления, сопряженные с компьютерными технологиями // *Уголовное право*. 2016. № 3. С. 9-11.

Иванова, 2019 – *Иванова Л.В.* Виды киберпреступлений по российскому уголовному законодательству // *Юридические исследования*. 2019. №1. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/vidy-kiberprestupleniy-po-rossiyskomu-ugolovnomu-zakonodatelstvu

Конвенция о преступности... – Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс]. URL: http://base.garant.ru/4089723/

Кочкина, 2017 – *Кочкина Э.Л.* Определение понятия «Киберпреступление». Отдельные виды киберпреступлений // *Сибирские уголовно-процессуальные и криминалистические чтения*. 2017. №3(17). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/opredelenie-ponyatiya-kiberprestuplenie-otdelnye-vidy-kiberprestupleniy

Отчёт официального представителя... – Отчёт официального представителя МВД РФ Ирины Волк о преступлениях за 2020 год [Электронный ресурс]. URL: https://rg.ru/2020/08/19/mvd-v-2020-godu-chislo-kiberprestuplenij-v-rossii-vyroslo-na-946.html

Официальное заявление МИД... – Официальное заявление МИД РФ о принятии Генасамблеей ООН резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях» [Электронный ресурс]. URL: https://www.mid.ru/main_en/-/asset_publisher/G51iJnfMMNKX/content/id/3988579

Пять правил... – Пять правил безопасного интернет-шопинга от Сбербанка [Электронный ресурс]. URL: https://www.sberbank.ru/ru/person/blog/buy_without_loss

Сазонов, 2018 – *Сазонов М.М.* Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения // *Виктимология*. 2018. №2(16). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/vidy-moshennichestv-s-bankovskimi-kartami-i-sovershenstvovanie-mer-viktimologicheskogo-preduprezhdeniya

Сбербанк поддержал создание... – Сбербанк поддержал создание Глобального центра по кибербезопасности [Электронный ресурс]. URL: https://lenta.ru/news/2018/01/24/sber_kiber/

Сериева, 2017 – *Сериева М.М.* Киберпреступность как новая криминальная угроза // *Новый юридический вестник*. 2017. №1 (1). С. 104-106.

Уголовный кодекс Российской Федерации... – Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 30.12.2020) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/

Чекунов, 2013 – *Чекунов И.Г.* Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности // Москва. 2013. [Электронный ресурс]. URL: https://static.freereferats.ru/_avtoreferats/01006767997.pdf

References

Borodkina, Pavlyuk, 2018 – *Borodkina, T.N., Pavlyuk, A.V.* (2018). Kiberprestupleniya: ponyatie, soderzhanie i mery protivodeistviya [Cybercrimes: concept, content and countermeasures]. *Sotsial'no-politicheskie nauki*. 1: 135-137. [in Russian]

Bratusin, Vlasenko, 2019 – *Bratusin, A.R., Vlasenko, E.E.* (2019). O kharakternykh individual'no-tipologicheskikh osobennostyakh i povedencheskikh patternakh lichnosti tipichnykh zhertv finansovogo moshennichestva [On the characteristic individual-typological characteristics and behavioral patterns of the personality of typical victims of financial fraud]. *Problemy sovremennogo pedagogicheskogo obrazovaniya*. 64-4. [Electronic resource]. URL: https://cyber leninka.ru/article/n/o-harakternyh-individualno-tipologicheskih-osobennostyah-i-povedenchesk ih-patternah-lichnosti-ti pichnyh-zhertv-finansovogo [in Russian]

Butusova, 2016 – *Butusova, L.I.* (2016). K voprosu o kiberprestupnosti v mezhdunarodnom prave [To the issue of cybercrime in international law]. *Vestnik ekonomicheskoi bezopasnosti*. 2. [Electronic resource]. URL: https://cyberleninka.ru/article/n/k-voprosu-o-kiberprestupnosti-v-mezhdunarodnom-prave [in Russian]

Bykov, 2016 – *Bykov. i dr.* (2016). Sovershenstvovanie ugolovnoi otvetstvennosti za prestupleniya, sopryazhennye s komp'yuternymi tekhnologiyami [Improving criminal liability for crimes associated with computer technology]. *Ugolovnoe pravo*. 3: 9-11. [in Russian]

Chekunov, 2013 – *Chekunov, I.*G. (2013). Kriminologicheskoe i ugolovno-pravovoe obespechenie preduprezhdeniya kiberprestupnosti [Criminological and criminal legal support for the prevention of cybercrime]. Moskva. [Electronic resource]. URL: https:// static.freere ferats.ru/_avtoreferats/01006767997.pdf [in Russian]

Ivanova, 2019 – *Ivanova, L.V.* (2019). Vidy kiberprestuplenii po rossiiskomu ugolovnomu zakonodatel'stvu [Types of cybercrimes under Russian criminal law]. *Yuridicheskie issledovaniya*. 1. [Electronic resource]. URL: https://cyberleninka.ru/article/n/vidy-kiberprestupleniy-po-rossiyskomu-ugolovnomu-zakonodatelstvu [in Russian]

Kochkina, 2017 – *Kochkina, E.L.* (2017). Opredelenie ponyatiya «Kiberprestuplenie». Otdel'nye vidy kiberprestuplenii [Definition of the concept of "Cybercrime". Certain types of cybercrimes]. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya*. №3(17).

[Electronic resource]. URL: https://cyberleninka.ru/article/n/oprede lenie-ponyatiya-kiberpres tuplenie-otdelnye-vidy-kiberprestupleniy [in Russian]

Konventsiya o prestupnosti… – Konventsiya o prestupnosti v sfere komp'yuternoi informatsii ETS N 185 (Budapesht, 23 noyabrya 2001 g.) [Convention on Crime in the Field of Computer Information ETS N 185 (Budapest, November 23, 2001)]. [Electronic resource]. URL: http://base.garant.ru/4089723/ [in Russian]

Ofitsial'noe zayavlenie MID… – Ofitsial'noe zayavlenie MID RF o prinyatii Genasambleei OON rezolyutsii «Protivodeistvie ispol'zovaniyu informatsionno-kommunikatsionnykh tekhnologii v prestupnykh tselyakh» [The official statement of the Ministry of Foreign Affairs of the Russian Federation on the adoption by the UN General Assembly of the resolution "Counteracting the use of information and communication technologies for criminal purposes"]. [Electronic resource]. URL: https://www.mid.ru/main_en/-/asset_publisher/G51iJnfMMNKX/content/id/3988579 [in Russian]

Otchet ofitsial'nogo predstavitelya… – Otchet ofitsial'nogo predstavitelya MVD RF Iriny Volk o prestupleniyakh za 2020 god [Report of the official representative of the Ministry of Internal Affairs of the Russian Federation Irina Volk on crimes for 2020]. [Electronic resource]. URL: https://rg.ru/2020/08/19/mvd-v-2020-godu-chislo-kiberprestuplenij-v-rossii-vyroslo-na-946.html [in Russian]

Pyat' pravil… – Pyat' pravil bezopasnogo internet-shopinga ot Cberbanka [Five rules for safe online shopping from Sberbank]. [Electronic resource]. URL: https://www.sberbank.ru/ru/person/blog/buy_without_loss [in Russian]

Sazonov, 2018 – *Sazonov, M.M.* (2018). Vidy moshennichestv s bankovskimi kartami i sovershenstvovanie mer viktimologicheskogo preduprezhdeniya [Types of fraud with bank cards and improving measures of victimological prevention]. *Viktimologiya*. 2(16). [Electronic resource]. URL: https://cyberleninka.ru/article/n/vidy-moshennichestv-s-bankovskimi-kartami-i-sovershenstvovanie-mer-viktimologicheskogo-preduprezhdeniya [in Russian]

Sberbank podderzhal sozdanie… – Sberbank podderzhal sozdanie Global'nogo tsentra po kiberbezopasnosti [Sberbank supported the creation of the Global Cybersecurity Center]. [Electronic resource]. URL: https://lenta.ru/news/2018/01/24/sber_kiber/ [in Russian]

Serieva, 2017 – *Serieva, M.M.* (2017). Kiberprestupnost' kak novaya kriminal'naya ugroza [Cybercrime as a new criminal threat]. *Novyi yuridicheskii vestnik*. 1(1): 104-106. [in Russian]

Ugolovnyi kodeks Rossiiskoi Federatsii… – Ugolovnyi kodeks Rossiiskoi Federatsii ot 13.06.1996 N 63-FZ (red. ot 30.12.2020) [The Criminal Code of the Russian Federation of 13.06.1996 N 63-FZ (as amended on 30.12.2020)]. [Electronic resource]. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ [in Russian]

УДК 336

Киберпреступность в финансовой сфере

[a] Сочинский государственный университет, Российская Федерация

Алла Юрьевна Баранова [a, *], Полина Гаспарян [a]

Аннотация. Киберпреступность – это преступления в виртуальном (интернет) пространстве. Киберпространство (виртуальное пространство) – это моделируемое с помощью компьютеров и других устройств информационное пространство, в котором находятся различные данные: сведения о предметах, лицах, фактах, явлениях, событиях и процессах, представленные в математическом, символьном или любом другом виде, а также находящиеся в движении по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого реального или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи.

Актуальность данной темы подтверждается участившимися преступлениями в киберпространстве. Кибермошенничества и другие виды преступлений в IT среде не имеют абсолютно никаких границ, их не останавливают ни государственные границы, ни другие

[*] Корреспондирующий автор
Адреса электронной почты: baranovalla-77@mail.ru (А.Ю. Баранова)

континенты, ни какие-либо другие ограничения, существующие в реальном мире. К сожалению, официальная статистика описывает лишь верхушку айсберга, и поэтому мы всё чаще и чаще слышим о новых случаях, схемах и методах киберпреступлений. Двадцать первый век – это век появления научных открытий и новых технологий в IT-сфере. Все большее количество людей становятся жертвами интернет-мошенников. И при этом информированность пользователей остаётся на одном и том же, недостаточном уровне. В условиях ускоряющегося развития высоких технологий необходимо изучать развитие преступлений на просторах интернета.

В статье представлены разновидности киберпреступлений, экономические и правовые аспекты борьбы с кибермошенничеством. Целью статьи является разработка предложений по обеспечению безопасности потребителей финансовых услуг.

Ключевые слова: киберпреступность, интернет-безопасность, финансовые услуги.