Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

IRSTI 10.77.21
Article

https://doi.org/10.32523/2616-6844-2024-146-1-247-257

The role of the Internet in the evolution of fraud: a historical aspect

N.M. Apsimet*[1], A.B. Smanova[1], Utegenova G.A.[2]

[1]*Al-Farabi Kazakh National University, Almaty, Kazakhstan*
[2]*Korkyt Ata Kyzylorda University, Kyzylorda, Kazakhstan*

(E-mail: [1]Apsimet.nurdaulet@gmail.com, [1]akmaral.smanova@kaznu.edu.kz, [2]gulzat-utegenova@mail.ru)

Abstract. This article presents a thorough examination of how the Internet has altered the landscape of fraud, with particular focus on increasingly sophisticated digital schemes. It examines how the internet serves both criminals and cybersecurity efforts alike. Beginning with an exploration of fraud's historical roots from its early manifestations in pre-digital to digital times and continuing into modernity, this article details its development alongside technological progress. Utilizing various research methodologies (historical and statistical analysis), such as tracking its progression across time as well as any countermeasures implemented during that period.

Significant findings of this research highlight the rise of internet-enabled fraud forms such as phishing, identity theft and cyber extortion; emphasizing their global and anonymous nature. Furthermore, research indicates the need for multidisciplinary approaches that combine technological, legislative and educational strategies in combatting internet fraud. This highlights machine learning technologies like artificial intelligence in detecting fraud along with greater public awareness campaigns to build cyber literacy literacy levels among society at large.

Keywords: internet, fraud evolution, cybercrime, phishing attacks, cybersecurity measures and digital technologies.

Received 15.03.2024. Revised 17.03.2024. Accepted 25.03.2024. Available online 29.03.2024

Introduction

With global digitalization accelerating at unprecedented speed, Internet has become an indispensable resource to most people's daily lives, offering access to an infinite source of knowledge and forms of communication. Yet as these limitless opportunities expand so too has fraud expanded; its prevalence now warrants careful study and assessment.

Relevance of this study lies within its rising tide of fraudulent schemes on the Internet that are becoming ever more complex and difficult to recognize, due to Internet technologies' influence over methods and forms of fraudster activity. Therefore, there has been an urgent need to reexamine our approaches against cybercrime as well as examine ways by which fraudsters adapt to changing operating environments.

This study seeks to analyze the Internet's role in the history of fraudulent activities from an historical standpoint, exploring how its evolution has altered fraud techniques as well as identify main trends and directions of Internet-related fraud.

To meet this objective, this work lays out three tasks to pursue this aim. These are: (1) an investigation of historical fraud cases prior and after widespread Internet use (2) studying how digital technologies have altered fraudster methods (3) uncovering new forms of Internet-induced fraud.

Research in this area utilizes an integrative approach, including analysis of scientific literature, legal framework, statistical data and real cases of Internet fraud. As digital technologies have proliferated into everyday life and created opportunities for criminal enterprises, gaining an in-depth knowledge about its mechanisms and consequences is vitally important and timely.

Research methodology

To thoroughly explore the development and influence of fraud with Internet, as well as cybercrime methods today, various methodological approaches were employed to gain a thorough understanding of our subject of study and identify key trends.

Historical examination has been employed as a means to understand how fraud has evolved since pre-Internet times to the modern era, using historical analysis as a lens through which to view fraud schemes' development as technological innovations affect them. Through this method it became possible to pinpoint key phases in fraudulent schemes' evolution as well as determine their transformation when technology innovations emerged.

Content analysis was applied to process and organize information obtained from scientific articles, news reports, law enforcement reports and other pertinent sources in order to assess the scale of Internet fraud and identify its most frequent types. This approach enabled assessment of its scale as well as identification of its most prevalent manifestations.

Comparative analyses focused on fraud methods prior and after Internet's wide adoption in order to detect new threats that differed from more traditional forms. This allowed investigators to compare fraud techniques before and after widespread Internet usage and identify any differences or similarities with traditional forms.

Statistics were employed to examine quantitative data related to Internet fraud incidence and impact. This approach enabled us to observe its growth dynamics while pinpointing specific cybercrimes as trends of growth.

This study took an integrative, cross-disciplinary approach, combining elements from criminology, information technology and social sciences for maximum insight and an in-depth evaluation of cyber fraud issues. Data obtained as part of this investigation may serve as the foundation of effective methods to combat and prevent such crimes online.

Discussion and results

Fraud as a social phenomenon has deep historical roots that reflect shifts in relationships, technology and business practices. Tracing its development requires analysing an assortment of sources spanning ancient chronicles to modern academic works on cybercrime and information security.

Fraud first made its first appearance in Roman law. With subsequent reception into Kazakh law and legal systems from nearby and distant countries forming one of our global legal systems - Roman-Germanic law - fraud became understood as criminal liability when one appropriates another person's property [1, p. 143].

This thesis can be demonstrated through an examination of definitions provided by legislators: fraud under Germany's Criminal Code (§ 263) can be defined as any act committed intentionally with intent to deceive for personal gain or third-party gain resulting in greater property damages by deception and maintaining false assumptions regarding an injured party's injuries or misconception. Criminals engage in fraud when they present false facts as truth or distort actual facts to obtain advantage [2, p. 277]; according to France, "fraud is defined as any practice which intentionally leads to someone acting against themselves or against themselves through deceptive methods such as false names or status, abuse of power or deception to transfer funds, securities, material assets or any other property to people, provide services or enter transactions which create obligations or release them"(Art. 313-1 of France's Criminal Code) [3]; Republic of Latvia laws require "acquiring someone's property through deception"(Article 177 of Latvia's Criminal Code) [4] etc.

Fraud in history can take many forms. From simple deception and counterfeiting in antiquity to complex financial schemes enabled by modern banking systems in modernity. Postal communication and telegraphy brought new opportunities for fraudsters in the 19th century; postal scammers could operate anonymously over long distances [5]. At that time many modern fraud schemes such as pyramid schemes or financial scams began taking shape.

Of particular note is the period during the second half of the 20th century when computer technology led to significant shifts in fraud methods. Banking, insurance and trade were increasingly conducted digitally over this timeframe; therefore requiring new approaches for protecting fraud. Computer viruses and Trojans, specifically targeting financial information without authorization were the precursors to modern cyber fraud [6].

At the turn of the 20th and 21st centuries, Internet revolutionized our society in many ways. However, its rapid growth led to fraudsters exploiting it for illicit schemes through E-commerce, online banking, social networks and other Internet services such as Ebay or Craigslist; including new channels of fraud such as phishing scams. Skimming attacks became common place; while cyber extortion schemes and identity fraud also presented serious threats against Internet users [7, p. 342].

Literature review illustrates that, regardless of changing tools and techniques, fraud remains fundamentally the same: deception or breach of trust to acquire illegal gain. Current cybersecurity and law enforcement research efforts focus on devising effective measures against digital-era fraud as well as studying past cases that illustrate this evolution of fraudulent schemes.

Internet penetration into all aspects of society has drastically transformed fraudsters' landscape, opening new opportunities and challenges for criminals. Due to digital technologies' development and increased users on the web, fraudsters have found it an ideal environment for various scams to take place.

Phishing is one of the most prevalent online fraud schemes, in which criminals attempt to gain access to confidential user data (login credentials, passwords or bank card details) by creating fake websites or emails which appear as official requests from well-known companies or banks [8, p. 53].

Skimming in the digital era has seen an explosive expansion due to fraudsters installing malicious software onto payment terminals over the Internet that enables them to collect bank card details during online payments [9].

Cyber extortion became possible with the rise of cryptocurrency, involving blocking access to personal or company resources with demands for ransom payment to restore them - sometimes using encryption programs (ransomware) [10].

Identity fraud has taken on new dimensions with the ability to create fake social media and other online profiles to conduct illegal activities on behalf of someone else, including identity theft.

"Romantic" fraud refers to online dating scams designed to exploit victims by taking advantage of trust established through dating services to obtain funds for "urgent needs". Criminals create fake profiles in order to lure in potential victims before persuading them to send money for urgent needs [11].

Due to Internet development, globalized scammers can operate with anonymity while remaining unseen by law enforcement authorities. Not only has digitalization made accessing victims easier for fraudsters but it has also made tracking them down more challenging due to having to coordinate actions across borders and navigate legal hurdles.

Internet has played an essential role in the rise of fraud, providing criminals with new technologies to implement their plans and causing cybercrimes to multiply rapidly. Society and government agencies must therefore develop and implement new methods of protecting themselves against and preventing such cybercrimes.

Analyzing specific cases and statistical data of online fraud enables us to accurately gauge both its scale and trends as well as any countermeasures taken against it, while measuring effectiveness of our countermeasures. The research is based on reports from law enforcement agencies, research organizations, cybersecurity researchers and cybersecurity companies; key areas identified for development and fight against cyber fraud identified through this study [12]. According to analysis conducted from January through August 2022 in Kazakhstan alone 11.7 thousand cases of Internet fraud were detected totaling 7 billion tenge in damage; most were recorded from Nur-Sultan, Almaty or Karaganda regions

Reports indicate a sharp rise in online scams in recent years. Phishing attacks and identity theft continue to incur losses of billions annually globally. According to the study, from May

2022 through April 2023 the total number of phishing attacks reached 1,850,392, an increase of 727,813 over the same period in 2021 [13]. Google blocks approximately 100 million spam emails each day [14]. Social engineering to spread malware and extort victims is also on the rise, according to statistics; social engineering attacks increased 147% between 2020 and 2021 [15]. LinkedIn (52%), DHL (14%), Google (7%), Microsoft (6%), and FedEx (6%) were among the top five brands most often copied during Q1 2022 [16].

Responding to the growing threat of online fraud, governments, international organizations, and the private sector are taking various steps to strengthen cybersecurity. These include:

– developing and enacting legislative acts with stricter penalties for cybercrimes;

– Raising user awareness about online fraud risks and ways to mitigate them;

– Implementation of advanced identification and authentication technologies that protect access to personal and financial data;

– Cooperation among nations for sharing information and taking coordinated measures against international cyber fraud.

Case studies of fraudsters' strategies revealed common tactics used by them, including impersonating financial and trading organizations, engaging in social engineering to gain trust from victims, and employing advanced technologies to conceal their actions. Yet successful instances of fraud prevention were identified through rapid exchanges between banks and law enforcement agencies as well as modern techniques for monitoring and analyzing transactions [17].

Current developments in information technology and the Internet offer unprecedented opportunities to both individuals and businesses alike, but also pose serious cyber threats - with fraud being one of the key culprits. Effectiveness of existing mechanisms against fraud has become an urgent matter and must be thoroughly assessed in order to combat cyber fraud successfully.

Analysis of modern practices in fighting fraud online reveals the key elements for fighting it are software for detecting and preventing fraudulent activity, educational campaigns among network users, as well as strengthening legislative frameworks and international cooperation in cybersecurity matters.

Technical security measures such as antivirus programs and intrusion detection systems play a critical role in combatting fraudulent activity. Due to the complexity and variation of modern fraudulent schemes, however, continuous updating and improvement must take place for these technologies to stay effective. One area in particular that needs further exploration is machine learning/artificial intelligence systems capable of adapting quickly to new threats while effectively neutralizing them.

Educational activities aim to raise the level of cyber literacy among users. Informing them regularly on different types of fraud, protection methods and threats can significantly reduce successful attacks against them. Working closely with Internet service providers on additional security measures such as two-factor authentication or early warning systems for fraud may also prove effective in mitigating attacks successfully.

Legislative frameworks and international cooperation play an essential role in combatting global fraud. By tightening penalties for cybercrimes, developing common standards in cybersecurity, and sharing information among nations, international cooperation enables governments to more efficiently combat fraudsters operating from various jurisdictions.

Based on our analysis, it is evident that an integrated approach to combating fraud on the Internet is required, comprising technical, educational and legislative measures. Of all proposals to strengthen user protection measures, three areas stand out:

1. Implementation of cutting-edge artificial intelligence technologies to detect and block fraudulent transactions in real time;

2. Extending cyber hygiene training programs to various user groups including children, adults and seniors:

3. Strengthen international cooperation by sharing cyber threat intelligence and coordinating efforts against fraudulent activity;

4. Increase ISP responsibility for taking measures that protect users from fraud.

Effective protection from fraud in the digital era requires collaboration among state, business and society.

Conclusion

Research into the Internet's role in fraud's development has uncovered dramatic shifts in both its methods and scale of cybercrime since digital technologies' advent. With globalization and digitization taking hold, fraud has taken on new forms, becoming more sophisticated and widespread requiring society and state authorities to adopt novel approaches for prevention and countermeasure.

One of the key findings was that Internet use has drastically expanded opportunities for fraudsters, making it easier to reach potential victims while making the fraud process less obvious and difficult to detect. At the same time, however, advancements in information technology have provided new tools to fight this form of criminality - machine learning algorithms that analyze cyberattack attempts as well as artificial intelligence-powered strategies that detect them can now assist law enforcement officials with stopping fraudsters in their tracks.

As digital fraud becomes an increasing threat, developing and preventing it requires an integrated approach, including strengthening international cooperation, developing common cybersecurity standards, sharing threat information with stakeholders, raising public awareness about cyber security threats and increasing their cyber literacy level. Particular focus should be given to protecting vulnerable categories of users such as children and the elderly who may become targets of scammers online.

Fighting online fraud requires active user participation. Being aware of existing threats and knowing basic cyber hygiene can significantly lower the risk of falling prey to scammers; for this reason, educational programs, targeted awareness campaigns, and easy-to-understand self-protection tools must all play an integral part of an effective cybersecurity strategy.

Internet's impact in the development of fraud is dubious: on one hand it has provided criminals with greater opportunities, while providing valuable tools against them. Cyber fraud's future depends on society's adaptability in adapting to new challenges; developing and implementing innovative technologies and security strategies; as well as remaining vigilant and informed within digital space.

The contribution of authors.

Apsimet Nurdaulet Mukhamediyaruly – abstract, keywords, introduction.
Smanova Akmaral Bakhtiyarovna – methodology, results and discussion.
Utegenova Gulzat Amandykovna – conclusion, list of references, transliteration, information about the authors.

References

1. Фефлов И.В. Происхождение и развитие российского и зарубежного законодательства о мошенничестве // Территория науки. – 2014. – №4. – С. 141-152.

2. Федорков А.В. Институт мошенничества в ФРГ // Пробелы в российском законодательстве. – 2008. – №1. – С. 277-278.

3. Уголовный Кодекс Франции. https://yurist-online.org/laws/foreign/criminalcode_fr/_doc-5-.pdf?ysclid=ltouur4072447286295

4. Уголовный Закон Латвии. Закон, принятый Сеймом 17 июня 1998 года и обнародованный Президентом государства 8 июля 1998 года (С изменениями, внесенными по состоянию на 20 июня 2019 года) https://lawyer-khroulev.com/wp-content/uploads/2019/09/ugolovnij-zakon-latvii.pdf

5. История создания и распространения телеграфа. https://diletant.media/articles/25556820/.

6. Дубровин Н.А., Бычков Д.В., Гордеев К.С., Жидков А.А. Компьютерные вирусы // Современные научные исследования и инновации. 2017. № 11. https://web.snauka.ru/issues/2017/11/84861

7. Фатахова, Д.Р. Мошенничество в сети Интернет / Д.Р. Фатахова. — Текст : непосредственный // Молодой ученый. — 2020. — № 49 (339). — С. 341-344.

8. Казыханов Артём Азаматович, Байрушин Фёдор Тимофеевич Фишинг, как проблема для специалистов отдела ИБ // Символ науки. 2016. №10-2. С. 53-54.

9. Считать и украсть: как работает скимминг банковских карт. https://trends.rbc.ru/trends/industry/612d019d9a79470c54677745?from=copy.

10. Что такое кибервымогательство? https://www.keepersecurity.com/blog/ru/2024/01/15/what-is-cyber-extortion/.

11. Онлайн-знакомства: куда сообщить о мошенничестве? https://datingscammer.info/ru/blog/onlajn-znakomstva-kuda-soobshhit-o-moshennichestve-19094.html%.

12. Кибермошенничество в Казахстане: факты, тенденции и анализ. https://er10.kz/read/analitika/kibermoshennichestvo-v-kazahstane-fakty-tendencii-i-analiz/

13. Число фишинговых атак утроилось за последние три года. https://bing.com/search?q=%d1%84%d0%b8%d1%88%d0%b8%d0%bd%d0%b3%d0%be%d0%b2%d1%8b%d0%b5+%d0%b0%d1%82%d0%b0%d0%ba%d0%b8+%d1%81%d1%82%d0%b0%d1%82%d0%b8%d1%81%d1%82%d0%b8%d0%ba%d0%b0.

14. 250+ Статистика Фишинга: Виды, Стоимость И Многое Другое. https://marketsplash.com/ru/statistika-fishingha/.

15. Что такое социальная инженерия: история, методы, примеры. https://www.reg.ru/blog/chto-takoe-sotsialnaya-inzheneriya/.

16. Что такое социальная инженерия и почему вы должны знать о ней. https://blog.ishosting.com/ru/what-is-social-engineering/

17. Минфин подготовил законопроект об обмене данными об аферах с картами между ЦБ и МВД. https://www.forbes.ru/finansy/467741-minfin-podgotovil-zakonoproekt-ob-obmene-dannymi-ob-aferah-s-kartami-mezdu-cb-i-mvd.

Н.М. Әпсімет*1, А.Б. Сманова[1], Г.А. Утегенова[2]

[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қаласы, Қазақстан

[2]Қорқыт Ата атындағы Қызылорда университеті, Қызылорда қаласы, Қазақстан

Интернеттің алаяқтық эволюциясындағы рөлі: тарихи аспект

Андатпа. Мақалада интернеттің алаяқтық ландшафтын қалай өзгерткеніне мұқият талдау жасалып, барған сайын жетілдірілген цифрлық схемаларға ерекше назар аударылады. Сол сияқты интернеттің қылмыскерлерге де, киберқауіпсіздікке де қалай қызмет ететіні қарастырылады. Еңбекте алаяқтықтың тарихи тамырларын зерттеуден оның цифрлық дәуірге дейінгі алғашқы көріністерінен бастап, цифрлық технологияларға және қазіргі заманға дейін жалғасуы, оның технологиялық прогреспен қатар дамуы егжей-тегжейлі сипатталған. Зерттеудің әртүрлі әдістемелерін (тарихи және статистикалық талдау) пайдалану, мысалы, оның уақыт бойынша дамуын бақылау, сондай-ақ осы кезеңде қабылданған кез келген қарсы шараларды жүргізу барысы талданған.

Зерттеудің маңызды тұжырымдары фишинг, жеке басын ұрлау және киберқуат сияқты интернетті пайдаланатын алаяқтық форумдардың көбеюін көрсетеді; олардың жаһандық және анонимді сипатына баса назар аударылады. Сонымен қатар, зерттеу интернет-алаяқтықпен күресуде технологиялық, заңнамалық және білім беру страт-егияларын біріктіретін пәнаралық тәсілдердің қажеттілігін көрсетеді. Бұл алаяқтықты анықтауда жасанды интеллект сияқты машиналық оқыту технологияларын және жалпы қоғамдағы кибер сауаттылық деңгейін арттыру үшін халықты ақпараттандыру бойынша жүргізілетін науқандық шараларды жүйелейді.

Түйін сөздер: интернет, алаяқтық эволюциясы, киберқылмыс, фишингтік шабуылдар, киберқауіпсіздік шаралары және цифрлық технологиялар.

Н.М. Апсимет*[1], А.Б. Сманова[1], Г.А. Утегенова[2]

[1]Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан

[2] Кызылординский университет имени Коркыт Ата, г. Кызылорда, Казахстан

Роль интернета в эволюции мошенничества: исторический аспект

Аннотация. В этой статье представлен тщательный анализ того, как интернет изменил ландшафт мошенничества с особым акцентом на все более изощренные цифровые схемы. В

ней рассматривается, как интернет служит как преступникам, так и усилиям по обеспечению кибербезопасности. Начиная с исследования исторических корней мошенничества, с его ранних проявлений в доцифровые времена и заканчивая цифровыми технологиями в современности, в этой статье подробно описывается его развитие наряду с технологическим прогрессом. Использование различных методологий исследования (исторический и статистический анализ), таких, как отслеживание его развития во времени, а также любых контрмер, принятых в течение этого периода.

Важные выводы этого исследования подчеркивают рост числа мошеннических форумов с использованием интернета, таких, как фишинг, кража личных данных и кибервымогательство; подчеркивается их глобальный и анонимный характер. Кроме того, исследование указывает на необходимость междисциплинарных подходов, сочетающих технологические, законодательные и образовательные стратегии в борьбе с интернет-мошенничеством. Это выдвигает на первый план технологии машинного обучения, такие, как искусственный интеллект, в выявлении мошенничества наряду с более широкими кампаниями по информированию общественности для повышения уровня киберграмотности в обществе в целом.

Ключевые слова: интернет, эволюция мошенничества, киберпреступность, фишинговые атаки, меры кибербезопасности и цифровые технологии.

1. Feflov I.V. Proishozhdenie i razvitie rossijskogo i zarubezhnogo zakonodatel'stva o moshennichestve // Territorija nauki. – 2014. – №4. – S. 141-152. [in Russian]

2. Fedorkov A. V. Institut moshennichestva v FRG // Probely v rossijskom zakonodatel'stve. – 2008. – №1. – S. 277-278. [in Russian]

3. Ugolovnyj Kodeks Francii. https://yurist-online.org/laws/foreign/criminalcode_fr/_doc-5-.pdf?ysclid=ltouur4072447286295

4. Ugolovnyj Zakon Latvii. Zakon, prinjatyj Sejmom 17 ijunja 1998 goda i obnarodovannyj Prezidentom gosudarstva 8 ijulja 1998 goda (S izmenenijami, vnesennymi po sostojaniju na 20 ijunja 2019 goda) https://lawyer-khroulev.com/wp-content/uploads/2019/09/ugolovnij-zakon-latvii.pdf

5. Istorija sozdanija i rasprostranenija telegrafa. https://diletant.media/articles/25556820/. [in Russian]

6. Dubrovin N.A., Bychkov D.V., Gordeev K.S., Zhidkov A.A. Komp'juternye virusy // Sovremennye nauchnye issledovanija i innovacii. 2017. № 11. https://web.snauka.ru/issues/2017/11/84861 [in Russian]

7. Fatahova, D.R. Moshennichestvo v seti Internet / D.R. Fatahova. – Tekst : neposredstvennyj // Molodoj uchenyj. – 2020. – № 49 (339). – S. 341-344. [in Russian]

8. Kazyhanov Artjom Azamatovich, Bajrushin Fjodor Timofeevich Fishing, kak problema dlja specialistov otdela IB // Simvol nauki. 2016. №10-2. C. 53-54. [in Russian]

9. Schitat' i ukrast': kak rabotaet skimming bankovskih kart. https://trends.rbc.ru/trends/industry/612d019d9a79470c54677745?from=copy. [in Russian]

10. Chto takoe kibervymogatel'stvo? https://www.keepersecurity.com/blog/ru/2024/ 01/15/what-is-cyber-extortion/. [in Russian]

11. Onlajn-znakomstva: kuda soobshhit' o moshennichestve? https://datingscammer.info/ru/blog/onlajn-znakomstva-kuda-soobshhit-o-moshennichestve-19094.html%. [in Russian]

12. Kibermoshennichestvo v Kazahstane: fakty, tendencii i analiz. https://er10.kz/read/analitika/kibermoshennichestvo-v-kazahstane-fakty-tendencii-i-analiz/ [in Russian]

13. Chislo fishingovyh atak utroilos' za poslednie tri goda. https://bing.com/search?q=%d1%84%d0%b8%d1%88%d0%b8%d0%bd%d0%b3%d0%be%d0%b2%d1%8b%d0%b5+%d0%b0%d1%82%d0%b0%d0%ba%d0%b8+%d1%81%d1%82%d0%b0%d1%82%d0%b8%d1%81%d1%82%d0%b8%d0%ba%d0%b0. [in Russian]

14. 250+ Statistika Fishinga: Vidy, Stoimost' I Mnogoe Drugoe. https://marketsplash.com/ru/statistika-fishingha/. [in Russian]

15. Chto takoe social'naja inzhenerija: istorija, metody, primery. https://www.reg.ru/blog/chto-takoe-sotsialnaya-inzheneriya/. [in Russian]

16. Chto takoe social'naja inzhenerija i pochemu vy dolzhny znat' o nej. https://blog.ishosting.com/ru/what-is-social-engineering/ [in Russian]

17. Minfin podgotovil zakonoproekt ob obmene dannymi ob aferah s kartami mezhdu CB i MVD. https://www.forbes.ru/finansy/467741-minfin-podgotovil-zakonoproekt-ob-obmene-dannymi-ob-aferah-s-kartami-mezdu-cb-i-mvd. [in Russian]

Information about authors:

Apsimet Nurdaulet Mukhamediyaruly – the author for correspondence, 1st year doctoral student, faculty of law of Al-Farabi Kazakh National University, 050000, Almaty, Kazakhstan. Apsimet.nurdaulet@gmail.com, +77073506590

Smanova Akmaral Bakhtiyarovna – candidate of law, senior lecturer of the department of theory and history of state and law, constitutional and administrative law, faculty of law of Al-Farabi Kazakh National University, 050000, Almaty, Kazakhstan. akmaral.smanova@kaznu.edu.kz, +77026833709

Utegenova Gulzat Amandykovna – Master of «Jurisprudence», Lecturer of the Departament of «Jurisprudence» of the Korkyt Ata Kyzylorda University, 120000, Kyzylorda, Kazakhstan. gulzat-utegenova@mail.ru

Апсимет Нурдаулет Мухамедиярулы – автор для корреспонденции, докторант, Казахский национальный университет имени аль-Фараби, 050000, Алматы, Казахстан. Apsimet.nurdaulet@gmail.com, +77073506590.

Сманова Акмарал Бахтияровна – к.ю.н., старший преподаватель, Казахский национальный университет имени аль-Фараби, 050000, Алматы, Казахстан. akmaral.smanova@kaznu.edu.kz, +77026833709

Утегенова Гульзат Амандыковна – магистр юриспруденции, Кызылординский университет имени Коркыт Ата, 120000, Кызылорда, Казахстан. gulzat-utegenova@mail.ru

Әпсімет Нұрдәулет Мұхамедиярұлы – хат-хабар үшін автор, әл-Фараби атындағы Қазақ ұлттық университеті Заң факультетінің 1-ші курс докторанты, 050000, Алматы қ., Қазақстан. Apsimet.nurdaulet@gmail.com, +77073506590

Сманова Акмарал Бахтияровна – з.ғ.к., әл-Фараби атындағы Қазақ ұлттық университеті Заң факультетінің мемлекет және құқық теориясы мен тарихы, конституциялық және әкімшілік құқық кафедрасының аға оқытушысы, 050000, Алматы қ., Қазақстан. akmaral.smanova@kaznu.edu.kz, +77026833709

Утегенова Гульзат Амандыковна – Заңтану магистрі, Қорқыт Ата атындағы Қызылорда университетінің «Құқықтану» кафедрасының оқытушысы, 120000, Қызылорда, Қазақстан. gulzat-utegenova@mail.ru