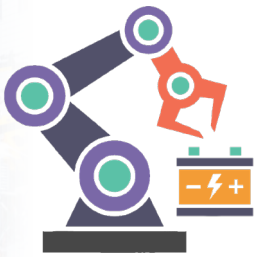
Автоматика. Энергетика. ИКТ



DOI 10.52209/1609-1825_2025_3_385 УДК 343.721:621.395.9

Оценка угроз мошенничества в мобильных телекоммуникационных сетях

***КУЛАКАЕВА Айгуль Ергалиевна,** PhD, ассоциированный профессор, a.kulakayeva@iitu.edu.kz,
КАБИБОЛАЕВА Дария Бауржанқызы, студент, 30116@iitu.edu.kz,
АО «Международный университет информационных технологий», ул. Манаса, 34/1, Алматы, Казахстан,
*автор-корреспондент.

Аннотация. *Проведена оценка угроз и анализ мошенничества в мобильных телекоммуникационных сетях с учетом региональной специфики Республики Казахстан. Основой исследования послужили данные онлайн-опроса, в ходе которого выявлено, что 26,5% опрошенных уже столкнулись с мошенническими схемами, включая фишинг через SMS (smishing), клонирование SIM-карт и уведомления от поддельных источников. Несмотря на то, что многие респонденты заявили о своей осведомленности о методах защиты, значительная их часть на практике не применяет базовые меры безопасности. Такой разрыв между самооценкой и реальным поведением указывает на необходимость усиления специализированных информационных мероприятий. В статье также анализируются последствия мошенничества, включая финансовые потери и психологический стресс, что подтверждает важность внедрения более эффективных мер защиты для предотвращения таких инцидентов. Новизна работы состоит в комплексном учете локальной инфраструктуры мобильной связи в Республике Казахстан, поведенческих факторов и глобальных тенденций, что позволяет сформулировать конкретные рекомендации по снижению рисков для операторов, государственных структур и конечных пользователей, учитывая особенности казахстанского рынка мобильной связи.*

Ключевые слова: *мошенничество, фишинг, уязвимость, финансовые потери, информационная безопасность, методы защиты.*

Введение

Развитие мобильных телекоммуникаций в Республике Казахстан в последние годы отличается высокими темпами цифровизации и увеличением числа абонентов операторов. Параллельно с этим наблюдается усиление мошеннической активности, особенно в аспектах, связанных с рассылкой фишинговых SMS, звонками от несуществующих источников и схемами клонирования SIM-карт. Так, по официальным данным, в 2023 году в Республике Казахстан зарегистрировано 44 тысячи инцидентов мошенничества с финансовыми потерями на сумму 140 миллиардов тенге [1].

В исследовании [2] рассматриваются основные факторы, влияющие на распространение мошенничества через информационно-телекоммуникационные технологии. Анализ основан на статистике и мнениях экспертов и включает социально-экономические, виктимологические, нравственные, технические и управленческие аспекты. В 2019 году зафиксировано более 119 000 преступлений в данной сфере. Результаты исследования подчеркивают важность глубокого анализа и разработки целенаправленных стратегий противодействия мошенничеству.

Также применение краудсорсинга и методов искусственного интеллекта, включая глубокое обучение, позволило создать систему, способную точно предсказывать мошенничество. Алгоритм Few-shot обучения показал высокую точность, превосходя традиционные методы, такие как LSTM и CNN. Разработанное приложение для WeChat предоставляет пользователям персонализированные уведомления о рисках мошенничества, повышая уровень защиты [3].

Изучив более 200 млн сообщений с 11 публичных SMS-шлюзов, исследователи обнаружили 67991 фишинговое сообщение, указывающее на широкомасштабное распространение этого вида мошенничества. Работа выявила 35128 фишингов в разных странах, включая США и европейские государства. Анализ показал, что мошенники активно используют облачные сервисы и временные URL для маскировки атак, большинство из которых длится около 13 дней. На основе этих данных предложены стратегии борьбы с фишингом, направленные на мониторинг и анализ поведения фишинговых операций [4]. Так, с использованием комбинированной модели регрессии и LSTM можно эффективно прогнозировать количество преступлений в сфере телекоммуникационного мошенничества. Модель обеспечила точность прогноза на уровне 86,80%, опережая ARIMA и другие гибридные модели. Такая высокая точность делает данную модель ценным инструментом для борьбы с телекоммуникационным мошенничеством [5].

В работе [6] анализируются цифровые следы мошенничества через мобильные устройства: данные о вызовах, текстовых сообщениях, информации с SIM-карт и устройств, а также банковские данные. Авторы подчеркивают, что эти следы играют ключевую роль в раскрытии преступлений и формировании следственных гипотез, рекомендуя привлечение экспертов для детального анализа, что существенно улучшает расследование мошенничеств с использованием мобильных технологий.

Кроме того, исследование [7] показало, что пожилые люди более подвержены телекоммуникационному мошенничеству. Установлено, что факторы, такие как образование и доход, влияют на способность распознавать мошеннические схемы, а особенно уязвимы лица с консервативными стратегиями (например, полное недоверие ко всем сообщениям). Результаты подчеркивают необходимость обучения пожилых людей методам защиты, чтобы повысить их устойчивость к мошенническим атакам, особенно когда злоумышленники выдают себя за официальных лиц.

Первоначально доминировали кражи наличных, однако к 2021 году основными стали хищения с банковских карт, при этом лишь 43% пострадавших обращаются в полицию. Преступники все активнее используют IT для совершения преступлений через интернет-магазины и облачные сервисы, что затрудняет расследование и приводит к росту числа преступлений – от 294 409 случаев в 2019 году до 517 722 в 2021 году и 35,3 тысячи за первое полугодие 2022 года, подчеркивая критическую необходимость адаптации методов борьбы с этим явлением [8].

В работе [9] рассматривается применение машинного обучения для выявления мошеннических звонков с помощью анализа эмоционального состояния голоса. Модель на основе CNN классифицирует эмоции с точностью 98%, используя аудиоданные из датасетов TESS и SAVEE, содержащих 6160 файлов, размеченных по семи типам эмоций. Преобразование аудио в числовой формат осуществляется с использованием MFCC, что ускоряет обработку данных. По сравнению с логистической регрессией и RandomForest, CNN демонстрирует наивысшую эффективность, обеспечивая возможность распознавания и предотвращения мошеннических звонков в режиме реального времени.

В работе [10] рассматриваются методы фишинга, включая почтовый и целевой фи-

шинг, vishing, smishing, атаки на социальные сети, клонирование писем и pharming. В 2021 году фишинговые атаки выросли на 18%, при этом в 99% случаев целью были деньги и личные данные, особенно в социальных сетях и финансовых организациях. Также появился сервис Phishing-as-a-Service, упрощающий организацию атак. Рекомендуемые меры противодействия включают использование защитного ПО, обучение сотрудников распознаванию угроз и двухэтапную проверку URL и содержимого веб-страниц.

Была исследована мошенническая схема Wangiri, при которой короткие звонки приводят к дорогостоящим перезвонам на премиум-номера. Для их выявления использована трехслойная нейронная сеть. Анализ 1000 звонков (300 мошеннических) показал, что MLP достигает точности 90,6% на тренировочной выборке и 85% на тестовой, что эффективно помогает операторам выявлять мошенничество и защищать клиентов [11].

Таким образом, анализ литературы показывает, что наиболее глубокие исследования телекоммуникационного мошенничества проводятся в странах с развитым рынком связи, где действуют свои законодательные нормы, высокий уровень цифровой грамотности и передовые методы идентификации абонентов. Прямое копирование этих решений в условиях Республики Казахстан не всегда оказывается эффективным, что подчеркивает необходимость проведения исследований с учетом местных особенностей, практик мобильных операторов и поведения абонентов различных возрастных групп. Настоящее исследование направлено на восполнение пробела в научной литературе, предоставляя комплексную оценку мошеннических схем (от технических до социально-психологических) применительно к казахстанской инфраструктуре. Полученные результаты имеют прямую практическую значимость, поскольку помогут заложить основу для разработки специальных мер противодействия мошенничеству для операторов связи и способствовать повышению уровня информационной грамотности казахстанских абонентов.

Методы исследования

Для реализации данного исследования был использован комплексный метод сбора данных, который объединяет количественный и качественный анализ. Основным инструментом стал онлайн-опрос на платформе Google Forms. Этот опрос был направлен на оценку уровня осведомленности пользователей Республики Казахстан о различных видах мошенничества и их отношении к мерам защиты, применяемым мобильными операторами связи. Особое внимание уделялось целевой аудитории, характерной для Республики Казахстан: опрос распространялся через мессенджер WhatsApp, что способствовало высокому охвату и активному вовлечению респондентов. Применение как закрытых, так и открытых вопросов позволило собрать как структурированные данные, так и субъективные мнения участников исследования.

В общей сложности в исследовании приняли участие 226 респондентов. Из них 47,8% (108 мужчин) – мужчины, а 52,2% (118 женщин) – женщины. Возрастное распределение также было разнообразным: 50,4% респондентов находились в возрастной группе от 18 до 30 лет, что составило самую большую долю участников. 17,7% респондентов были старше 65 лет, 14,6% – в возрасте от 31 до 50 лет, 11,5% – от 51 до 64 лет. Отдельная группа включала респондентов моложе 18 лет, доля которых составила 5,8%. Такое распределение позволило учесть мнения представителей различных возрастных групп.

В результате анализа данных было установлено, что 44,25% (100) респондентов являются пользователями оператора ТОО «Мобайл Телеком-Сервис» с торговыми марками Tele2, Altel, что делает его самым популярным среди участников опроса. На втором месте оказался оператор ТОО «КарТел» с торговыми марками Beeline, Izi и т.д. – 36,73% респондентов, а на третьем месте – АО «K'cell» – 20,35% респондентов.

Научные результаты

По результатам проведенного опроса 26,5% (примерно 60) респондентов отметили, что они становились жертвами мошенничества в телекоммуникационных сетях, в то время как 73,5% (примерно 166) участников не сталкивались с подобным опытом (рисунок 1). Эти данные свидетельствуют о том, что четверть пользователей телекоммуникационных услуг подвергались мошенническим действиям, что подчеркивает актуальность проблемы. Однако 73,5% опрошенных не имела подобного опыта, что может указывать на эффективность существующих методов защиты, либо на недостаточную осведомленность пользователей о подобных случаях.

Несмотря на то, что значительная доля респондентов не стала жертвами мошенничества, это не отменяет необходимость усиления профилактических мер. Важно учитывать, что реальное количество жертв может быть выше из-за латентности мошенничества и неосведомленности пользователей о

фактах неправомерных действий.

В соответствии с рисунком 2, в результате анализа, было выявлено, что из 225 опрошенных 56,9% (128) респондентов указали, что их осведомленность является средней. Это может указывать на определенное поверхностное знание основных видов угроз, но недостаточную глубину понимания механизмов защиты. Около 27,6% (62) респондентов утверждают, что обладают высоким уровнем осведомленности, что может свидетельствовать либо о подлинных знаниях, либо о субъективной переоценке своей компетенции.

Критически оценивая данные, можно предположить, что реальный уровень осведомленности пользователей в Казахстане ниже заявленного, поскольку мошенники применяют сложные методы, распознать которые даже опытным пользователям бывает трудно. Лишь 15,6% (35) респондентов признались в недостатке знаний, что указывает на необходимость активного обучения современным методам защиты и повышения самокритичности. Среди видов мошенничества, с которыми сталкивались респонденты, 11,8% (16) отмечают клонирование SIM-карт, 10,3% (14) – мошенничество с данными, а голосовой фишинг (vishing) упомянули 12,5% (17) респондентов, что свидетельствует о значительной угрозе данного вида атак. Особенно актуально это для Казахстана, где особенности цифровой инфраструктуры и уровень цифровой грамотности создают дополнительные риски. Полученные результаты подчеркивают необходимость внедрения более эффективных мер защиты и повышения осведомленности пользователей о различных формах мошенничества, чтобы снизить вероятность стать жертвой преступных действий на казахстанском рынке телекоммуникаций.

На рисунке 3 представлены данные о том, какие последствия испытали респонденты в результате мошеннических действий. Основными последствиями стали психологический стресс – 35,6% (48 человек) и финансовые потери – 28,1% (38 человек),

Рисунок 1 – Статистика жертв мошенничества

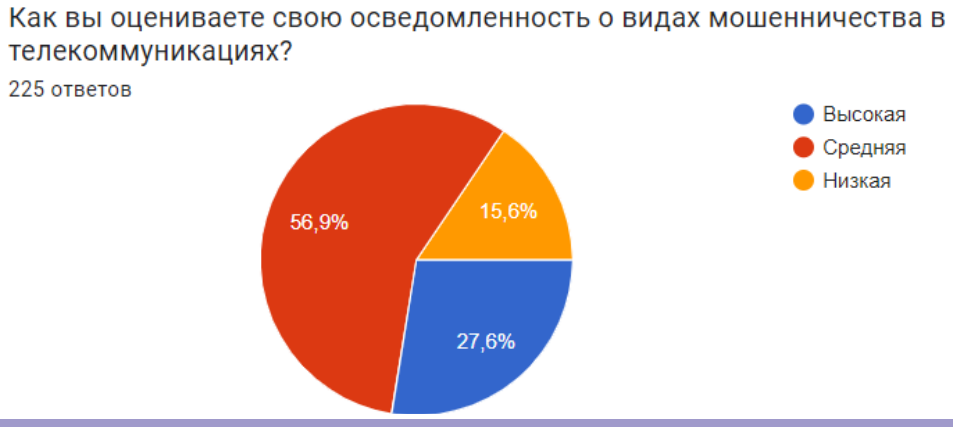


Рисунок 2 – Уровень осведомленности о видах мошенничества

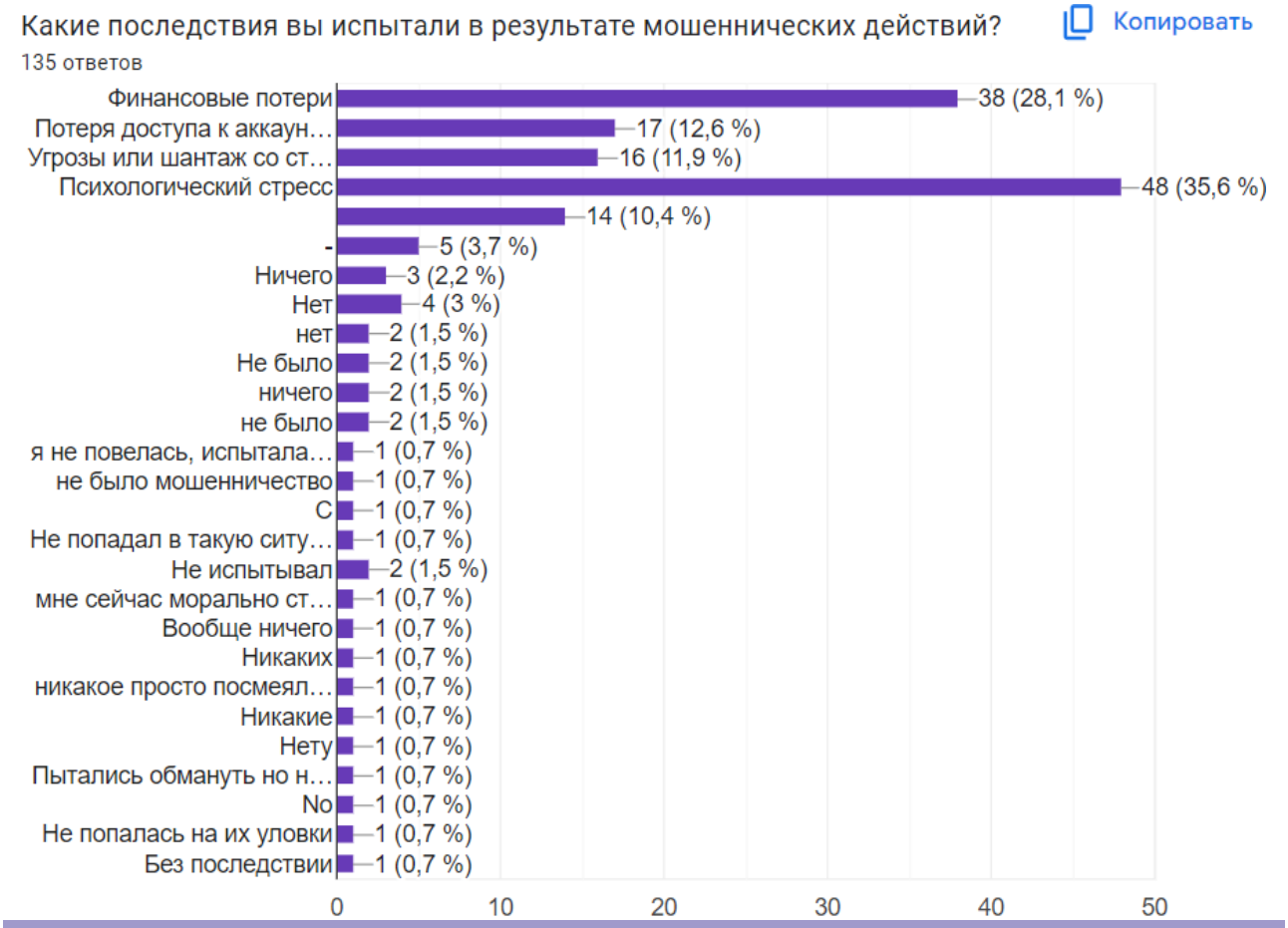


Рисунок 3 – Последствия мошеннических действий

что подчеркивает значительное влияние подобных преступлений на эмоциональное и материальное состояние жертв.

Потеря доступа к аккаунтам составила 12,6% (17 человек), а угрозы или шантаж со стороны мошенников – 11,9% (16 человек), что демонстрирует, что помимо финансовых и эмоциональных последствий пострадавшие сталкиваются с серьезными проблемами, связанными с кражей личных данных и нарушением безопасности аккаунтов. Лишь 3,7% (5 человек) респондентов не отметили негативных последствий, что свидетельствует о том, что большинство участников опроса испытали отрицательные эффекты от мошеннических действий.

На рисунке 4 представлены результаты опроса касательно осведомленности о методах защиты от мошенничества в сетях мобильного оператора.

Из 226 опрошенных 31% (70) респондентов ответили, что хорошо знакомы с методами защиты, что свидетельствует о высоком уровне осведомленности респондентов. Однако 35% (79) респондентов указали, что знают основные методы, но не применяют все из них, что подчеркивает необходимость практического использования этих знаний.

В условиях казахстанского рынка телекоммуникаций около 20,4% (46) респондентов сообщили, что слышали о методах защиты, но не применяют их, а 13,7% (31 человек) не знают вообще никаких методов, что подчеркивает необходимость повышения цифровой грамотности и внедрения практических мер безопасности.

Выводы

Проведенное исследование показало, что телекоммуникационные сети Республики Казахстан остаются уязвимыми для мошенничества, поскольку более четверти респондентов сталкивались с такими атаками. Несмотря на заявленную осведомленность, значительная часть пользователей не применяет меры защиты в повседневной жизни, что указывает на необходимость целенаправленных разъяснительных программ с учетом регионального менталитета и реальных технических навыков населения. Анализ показал, что объединение технического и социологического подходов дает наиболее

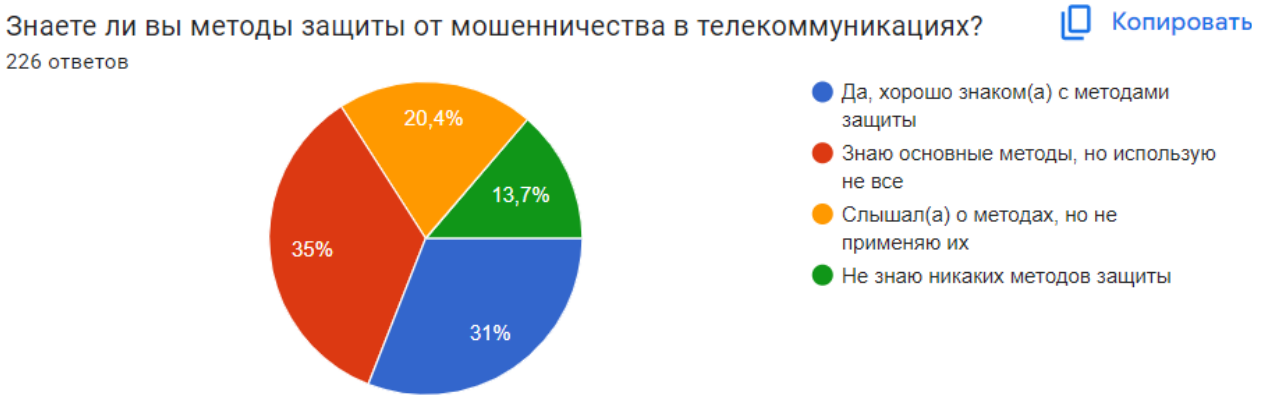


Рисунок 4 – Осведомленность о методах защиты от мошенничества

полное понимание проблемы. Помимо технических уязвимостей, значительную роль играют поведенческие факторы, такие как доверие к сообщениям «от оператора» и игнорирование базовых мер киберзащиты. Это указывает на то, что борьба с мошенничеством требует не только совершенствования сетевой инфраструктуры, но и повышения цифровой грамотности абонентов.

Перспективы дальнейших исследований включают разработку персонализированных систем предупреждения мошенничества с учетом поведенческих моделей и применение машинного обучения для анализа звонков и SMS. Особое внимание следует уделить сегментации пользователей по возрасту и цифровой грамотности, а также применению опережающих мер защиты, таких как прогнозирование аномальной активности и динамическая блокировка высокорисковых операций. Это позволит снизить финансовый ущерб и эмоциональный стресс абонентов, а также укрепить доверие к мобильным услугам в стране.

Таким образом, основные рекомендации, следующие:

- внести дополнения в законодательство, обязывающие операторов применять многофакторную аутентификацию (как минимум двух- или трехуровневую проверку личности) через eGov.kz при выдаче дубликатов SIM-карт;
- использовать единый протокол взаимодействия для оперативного обмена данными о мошеннических номерах через ЦБДАН РГП «Государственная техническая служба», обеспечивая централизованную блокировку подозрительных абонентов;
- использовать автоматический запрос к eLicense.kz при регистрации/обновлении лицензий сервис-провайдеров, чтобы исключить «фиктивные» call-центры и сервисы;
- предоставить абонентам возможность в один клик жаловаться на подозрительные номера и сообщения через eOtinish, упрощая процесс блокировки на уровне операторов и госорганов;
- применять отечественные алгоритмы машинного обучения для анализа больших объемов звонков и SMS и выявления нетипичных закономерностей, что позволит быстрее реагировать на массовые фишинговые атаки.

СПИСОК ЛИТЕРАТУРЫ

1. Официальный новостной сайт РК «Tengri news». https://tengrinews.kz/ 30.05.2024.
2. Молчанова Т.В. и др. Факторы, обусловливающие мошенничество, совершенное с использованием информационно-телекоммуникационных технологий // Вестник экономической безопасности. 2020;(2):93-8.
3. Deng W. et al. An Early Warning Model of Telecommunication Network Fraud Based on User Portrait // Computers, Materials and Continua. – 2023. – Т. 75. – №. 1. – С. 1561-1576.

4. Nahapetyan A. et al. On sms phishing tactics and infrastructure //2024 IEEE Symposium on Security and Privacy (SP). – IEEE Computer Society, 2024. – С. 169-169.
5. Gao Y. et al. Prediction of Telecommunication Network Fraud Crime Based on Regression-LSTM Model // Wireless Communications and Mobile Computing. – 2022. – Т. 2022. – №. 1. – С. 3151563.
6. Барченкова Я. В. Цифровые следы при расследовании мошенничества, совершенного при помощи средств сотовой связи // Экономика и Право, №4, 2020, С. 135-136.
7. Xiang, H., Zhou, J., & Xie, B. Understanding Older Adults' Vulnerability and Reactions to Telecommunication Fraud: The Effects of Personality and Cognition // Lecture Notes in Computer Science, 2020, pp. 351-363.
8. Тхазеплов Т.М. Перевод общества на цифровой формат и развитие в нем киберпреступности // Право и управление. – №5. – 2023. – С. 210-214.
9. Никитин П. В. и др. Распознавание эмоций по аудиосигналам как один из способов борьбы с телефонным мошенничеством // Программные системы и вычислительные методы. – 2022. – №. 3. – С. 1-13.
10. Афанасьева Н. С. и др. Классификация фишинговых атак и меры противодействия им //Инженерный вестник Дона. – 2022. – №. 5 (89). – С. 169-182.
11. Mawgoud A. A. et al. A Holistic Neural Networks Classification for Wangiri Fraud Detection in Telecommunications Regulatory Authorities //International Conference on Advanced Machine Learning Technologies and Applications. – Cham: Springer International Publishing, 2021. – С. 175-183.

Мобильді телекоммуникациялық желілердегі алаяқтық қатерлерін бағалау

***КУЛАКАЕВА Айгуль Ергалиевна,** PhD, қауымдастырылған профессор, a.kulakayeva@iitu.edu.kz,*
***КАБИБОЛАЕВА Дария Бауржанқызы,** студент, 30116@iitu.edu.kz,*
«Халықаралық ақпараттық технологиялар университеті» АҚ, Манас көшесі, 34/1, Алматы, Қазақстан,
**автор-корреспондент.*

***Аңдатпа.** Берілген мақалада онлайн-сауалнама арқылы жиналған мәліметтер негізінде мобильді телекоммуникациялық желілердегі алаяқтық қатерлерін бағалау жүргізілді. Зерттеу алаяқтар қаражат пен жеке ақпаратты ұрлау үшін пайдаланатын мобильді желілердің кейбір осалдықтарын анықтады. Алаяқтықтың ең көп таралған түрлерінің қатарына SMS (smishing) арқылы фишинг, SIM карталарын клондау және жалған көздерден хабарламалар жатады. Зерттеу 226 респонденттің жауаптарын талдады, олардың 26,5% (шамамен 60 респондент) алаяқтықтың құрбаны болған. Нәтижелер көрсеткендей, көптеген пайдаланушылар қорғаныс әдістерімен таныс болғанымен, респонденттердің едәуір бөлігі оларды іс жүзінде қолданбайды, бұл хабардарлықты арттыру қажеттілігін көрсетеді. Мақалада алаяқтықтың салдарын, соның ішінде қаржылық шығындар мен психологиялық стрессті талдау келтірілген, бұл мұндай оқиғалардың алдын алу үшін тиімді қорғаныс шараларын енгізудің маңыздылығын растайды.*

***Кілт сөздер:** алаяқтық, мобильді байланыс, фишинг, осалдық, қаржылық шығындар, ақпараттық қауіпсіздік, қорғау әдістері, аутентификация.*

Assessment of Fraud Threats in Mobile Telecommunications Networks

***KULAKAYEVA Aigul,** PhD, Associate Professor, a.kulakayeva@iitu.edu.kz,*
***KABIBOLAEVA Dariya,** Student, 30116@iitu.edu.kz,*
JSC «International Information Technology University», Manas Street, 34/1, Almaty, Kazakhstan,
**corresponding author.*

***Abstract.** An assessment of threats and an analysis of fraud in mobile telecommunications*

networks was conducted, taking into account the regional specifics of the Republic of Kazakhstan.. The study revealed some vulnerabilities of mobile networks used by fraudsters to steal funds and personal information. Among the most common types of fraud are phishing via SMS (smishing), SIM card cloning and notifications from fake sources. The study analyzed the responses of 226 respondents, among whom 26.5% (approximately 60 respondents) were victims of fraud. The results show that although many users are familiar with the protection methods, a significant proportion of respondents do not apply them in practice, which underscores the need to raise awareness. The article also provides an analysis of the consequences of fraud, including financial losses and psychological stress, which confirms the importance of implementing more effective protection measures to prevent such incidents.

Keywords: *fraud, mobile communications, phishing, vulnerability, financial losses, information security, security methods, authentication.*

REFERENCES

1. Ofitsial'nyi novostnoi sait RK «Tengri news». Available at: https://tengrinews.kz/ (accessed: 30.09.2024).
2. Molchanova T.V. et al. Faktory, obuslovlivayushchie moshennichestvo, sovershennoe s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologii [Factors that determine fraud committed using information and telecommunication technologies]. Vestnik ekonomicheskoi bezopasnosti [Bulletin of Economic Security], 2020, no. 2, pp. 93-98.
3. Deng W. et al. An Early Warning Model of Telecommunication Network Fraud Based on User Portrait // Computers, Materials and Continua. – 2023. – T. 75. – №. 1. – C. 1561-1576.
4. Nahapetyan A. et al. On SMS phishing tactics and infrastructure //2024 IEEE Symposium on Security and Privacy (SP). – IEEE Computer Society, 2024. – C. 169-169.
5. Gao Y., Yin D., Zhao X., Wang Y., Huang Y. Prediction of Telecommunication Network Fraud Crime Based on Regression-LSTM Model. Wireless Communications and Mobile Computing, 2022, 16 pages.
6. Barchenkova Ya.V. Tsifrovye sledy pri rassledovanii moshennichestva, sovershennogo pri pomoshchi sredstv sotovoi svyazi [Digital traces in the investigation of fraud committed using mobile communication]. Ekonomika i pravo [Economics and Law], 2020, no. 4, pp. 135-136.
7. Xiang H., Zhou J., Xie B. Understanding Older Adults' Vulnerability and Reactions to Telecommunication Fraud: The Effects of Personality and Cognition. Lecture Notes in Computer Science, 2020, pp. 351-363.
8. Thazheplov T.M. Perevod obshchestva na tsifrovoi format i razvitie v nem kiberprestupnosti [Transition of society to digital format and the development of cybercrime]. Pravo i upravlenie [Law and Management], 2023, no. 5, pp. 210-214.
9. Nikitin P.V., Osipov A.V., Pleshakova E.S., Korchagin S.A., Gorokhova R.I., Gataullin S.T. Raspoznavanie emotsii po audiosignalam kak odin iz sposobov bor'by s telefonnym moshennichestvom [Emotion recognition from audio signals as one of the ways to combat telephone fraud]. Programmnye sistemy i vychislitel'nye metody [Software Systems and Computational Methods], 2022, no. 3.
10. Afanas'eva N.S. et al. Klassifikatsiya phishingovykh atak i mery protivodeistviya im [Classification of phishing attacks and measures to counteract them]. Inzhenernyi vestnik Dona [Engineering Bulletin of Don], 2022, no. 5.
11. Mawgoud A.A. et al. A Holistic Neural Networks Classification for Wangiri Fraud Detection in Telecommunications Regulatory Authorities. Advances in Machine Learning and Data Analytics, 2021, pp. 175-183.