

ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛЬ-ФАРАБИ
AL-FARABI KAZAKH NATIONAL UNIVERSITY

# «ЖАһАНДАНУ ЖАҒДАЙЫНДАҒЫ ҚЫЛМЫСТЫҚ САЯСАТТЫҢ ДАМУ ТЕНДЕНЦИЯЛАРЫ»

**атты Халықаралық ғылыми-тәжірибелік конференцияның (XIII жыл сайынғы Баймурзин оқулары)**

## МАТЕРИАЛДАР ЖИНАҒЫ

**30 қараша 2023**

## СБОРНИК МАТЕРИАЛОВ

**Международной научно-практической конференции**

# «ТЕНДЕНЦИИ РАЗВИТИЯ УГОЛОВНОЙ ПОЛИТИКИ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ»

**(XIII Ежегодные Баймурзинские чтения)**

**30 ноября 2023**

## COLLECTION OF MATERIALS

**of the International scientific-practical conference**

# «TRENDS IN THE DEVELOPMENT OF CRIMINAL POLICY IN THE CONTEXT OF GLOBALIZATION»

**(XIII Annual Baymurzins readings)**

**November 30th 2023**

**Алматы/Almaty 2023**

**ӘЛ – ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ**
**КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛЬ-ФАРАБИ**
**AL-FARABI KAZAKH NATIONAL UNIVERSITY**

«ЖАҺАНДАНУ ЖАҒДАЙЫНДАҒЫ ҚЫЛМЫСТЫҚ
САЯСАТТЫҢ ДАМУ ТЕНДЕНЦИЯЛАРЫ»
**атты Халықаралық ғылыми – тәжірибелік конференцияның**
(XIII жыл сайынғы Баймурзин оқулары)

# МАТЕРИАЛДАР ЖИНАҒЫ
**30 қараша 2023**

# СБОРНИК МАТЕРИАЛОВ
**Международной научно-практической конференции**

«ТЕНДЕНЦИИ РАЗВИТИЯ УГОЛОВНОЙ ПОЛИТИКИ
В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ»
(XIII Ежегодные Баймурзинские чтения)
**30 ноября 2023**

# COLLECTION OF MATERIALS
**of the International scientific-practical conference**

«TRENDS IN THE DEVELOPMENT OF CRIMINAL POLICY
IN THE CONTEXT OF GLOBALIZATION»
(XIII Annual Baymurzins readings)
**November 30th 2023**

Алматы/Almaty 2023

**ӘОЖ 343.3/.7**
**КБЖ 67.408**
**Ж35**



**Жаһандану жағдайында қылмыстық саясатты жетілдіру тенденциялары** (XIII жыл сайынғы Баймурзин оқулары)**:** халықаралық ғылыми-тәжірибелік конференция материалдары (30 қараша 2023 ж.)/ Жауапты ред. Р.Е. Джансараева. – Алматы, 2023. – 286 б.

**Тенденции развития уголовной политики в условиях глобализации** (XIII ежегодные Баймурзинские чтения): материалы международной научно-практической конференции (30 ноября 2023 г.)/ отв. ред. Р.Е. Джансараева. – Алматы, 2023. – 286 с.

**Trends in the development of criminal policy in the context of globalization** (XIII Annual Baymurzins readings): materials of the international scientific and practical conference (November 30, 2023)/ ed. by R.E.Dzhansarayeva. – Almaty, 2023. – 286 p.

**ISBN 978-601-04-6542-8**

*Жинаққа әл-Фараби атындағы ҚазҰУ-нің заң факультетінің қылмыстық құқық, қылмыстық іс жүргізу және криминалистика кафедарасы, Қылмыстылыққа қарсы тұру мәселелерін зерттеу Орталығымен бірігіп өткізген: «Жаһандану жағдайында қылмыстық саясатты жетілдіру тенденциялары» атты халықаралық ғылыми – тәжірибелік конференция материалдары енді.*

*Конференция материалдары жинағы 2023-2025 жылдарға арналған ғылыми және (немесе) ғылыми-техникалық бағдарламалар бойынша ЖТН BR 27882414 «Зорлық-зомбылық құрбандарын қолдау және оңалту бағдарламасы: ресурстық модульдік орталықтар желісін іс жүзінде енгізу» жобасы бойынша бағдарламалық-нысаналы қаржыландыру шеңберінде дайындалды.*

*В сборник вошли материалы международной научно-практической конференции «Тенденции развития уголовной политики в условиях глобализации (XIV ежегодные Баймурзинские чтения)», проведенной юридическим факультетом КазНУ им.Аль-Фараби совместно с центром изучения проблем уголовного права, уголовно – процессуального и криминалистического поведения.*

*Сборник материалов конференции подготовлен в рамках программно-целевого финансирования по проекту ИРН BR 27882414 «Программа поддержки и реабилитации детей-жертв насилия: практическое внедрение сети ресурсных модульных центров».*

*The collection includes materials of the international scientific and practical conference "Trends in the development of criminal policy in the context of globalization (XIV Annual Baymurzins readings)", organized by the cafe of Criminal Law, Criminal Procedure and criminalistics of the Faculty of law of Al-Farabi Kazakh National University together with the Center for research on countering crime.*

*The collection of conference materials was prepared within the framework of program-targeted financing under the project IRN BR 27882414 «Program for support and rehabilitation of child victims of violence: practical implementation of a network of resource modular centers».*

ISBN 978-601-04-6542-8

**ӘОЖ 343.3/.7**
**КБЖ 67.408**

**МАЗМҰНЫ/СОДЕРЖАНИЕ/CONTENTS**

**Әпсімет Н.М.**
әл-Фараби атындағы ҚазҰУ, заң факультеті
Қылмыстық құқық, қылмыстық іс жүргізу
және криминалистика кафедрасы
1 курс докторанты
Алматы қ., Қазақстан Республикасы

**Алимкулов Е.Т.**
әл-Фараби атындағы ҚазҰУ, заң факультеті
Қылмыстық құқық, қылмыстық іс жүргізу
және криминалистика кафедрасы
з.ғ.к., доцент

# КИБЕРҚАУІПТЕР ЖӘНЕ ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУ: ОНЛАЙН АЛАЯҚТЫҚТЫҢ ЗАМАНАУИ ӘДІСТЕРІН ТАЛДАУ

Мақалада Қазақстандағы алаяқтық мәселесін, оның интернеттегі көріністеріне анализ жасалады. Автор дәстүрлі қаржылық алаяқтық, корпоративтік алаяқтық және интернет-алаяқтық сияқты алаяқтықтың әртүрлі нысандарын зерттеп, олардың әділ сауда мен әлеуметтік сенімге төнетін қаупін көрсетеді. Қазақстандағы қылмыстардың динамикасына ерекше назар аударылады, онда алаяқтық қылмыстар санының, оның ішінде интернетте артуы байқалады.

Фишинг, вишинг, «Нигериялық хаттар», фарминг, сондай-ақ интернет-дүкендер мен жеке хабарландыру сайттарындағы алдау сияқты интернет-алаяқтық түрлері қарастырылады. Алаяқтардың адамдарды алдау және жеке деректерге ену үшін қолданатын әдістері, соның ішінде психологиялық әдістер мен ақпараттық технологияларды қолдану сипатталған. Автор алаяқтардың интеллект деңгейі жоғары және мамандандырылған білімі бар екенін, бұл оларды күрделі алаяқтық схемаларын жасауға қабілетті ететінін атап көрсетеді.

Мақала сонымен қатар антивирустық бағдарламалық жасақтаманы хабардар ету мен қолданудың маңыздылығын, сондай-ақ электрондық пошта жәшіктерін үнемі жаңартып отыру және қорғау қажеттілігін көрсете отырып, алаяқтықтың осы түрлерінің алдын алу және қарсы тұру мәселелерін қарастырады.

**Кілт сөздер:** алаяқтық, онлайн алаяқтық, жеке мәліметтер, фишинг, вишинг, «Нигерия хаттары», фарминг.

Статья освещает проблему мошенничества в Казахстане, акцентируя внимание на его проявлениях в интернете. Автор рассматривает различные формы мошенничества, такие как традиционный финансовый обман, корпоративное мошенничество, и интернет-мошенничество, подчеркивая

их угрозу для справедливой торговли и социального доверия. Особое внимание уделяется динамике преступлений в Казахстане, где наблюдается увеличение количества мошеннических преступлений, в том числе в интернете.

Рассматриваются такие виды интернет-мошенничества как фишинг, вишинг, «Нигерийские письма», фарминг, а также обман на интернет-магазинах и сайтах частных объявлений. Описываются методы, которые мошенники используют для обмана людей и проникновения в личные данные, включая психологические методы и использование информационных технологий. Автор подчеркивает, что мошенники часто обладают высоким уровнем интеллекта и специализированными знаниями, что делает их способными разрабатывать сложные схемы мошенничества.

Статья также затрагивает вопросы предотвращения и противодействия этим видам мошенничества, подчеркивая важность осведомленности и применения антивирусного программного обеспечения, а также необходимость регулярного обновления и защиты электронных почтовых ящиков.

**Ключевые слова:** мошенничество, интернет-мошенничество, личные данные, фишинг, вишинг, «Нигерийские письма», фарминг.

The article highlights the problem of fraud in Kazakhstan, focusing on its manifestations on the Internet. The author examines various forms of fraud, such as traditional financial fraud, corporate fraud, and Internet fraud, emphasizing their threat to fair trade and social trust. Particular attention is paid to the dynamics of crimes in Kazakhstan, where there is an increase in the number of fraudulent crimes, including on the Internet.

Such types of Internet fraud as phishing, vishing, «Nigerian letters», farming, as well as fraud on online stores and private ad sites are considered. It describes the methods that fraudsters use to deceive people and penetrate personal data, including psychological methods and the use of information technology. The author emphasizes that fraudsters often have a high level of intelligence and specialized knowledge, which makes them capable of developing complex fraud schemes.

The article also addresses the issues of preventing and countering these types of fraud, emphasizing the importance of awareness and the use of antivirus software, as well as the need for regular updating and protection of electronic mailboxes..

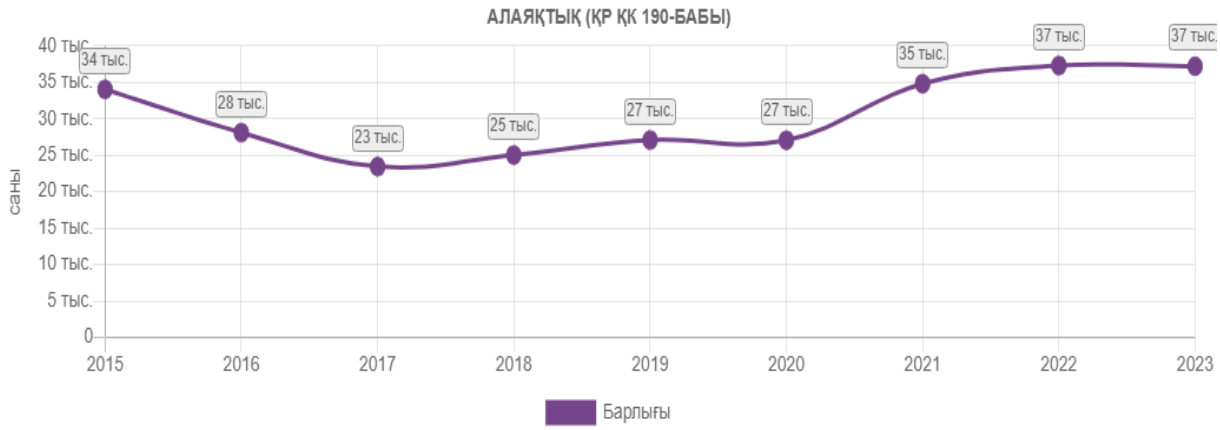
**Key words:** fraud, internet fraud, personal data, phishing, vishing, «Nigerian letters», farming.

Экономикалық белсенділік пен жеке қарым-қатынастар барған сайын күрделеніп, өзара байланысты болып жатқан әлемде алаяқтық әділ сауда мен әлеуметтік сенімге үлкен кедергі болуда. Бұл өзгермелі жағдайларға

бейімделген алдаудың ежелгі өнері дәстүрлі қаржылық алдаудан бастап күрделі ұжымдық алдау схемаларына дейін көптеген нысандарда көрініс табуы мүмкін.

Алаяқтық – Қазақстан Республикасы Қылмыстық кодексінің 190-бабында көзделген қылмыстық жауаптылық көзделген, алдау немесе сенімге қиянат жасау арқылы бөтеннің мүлкін ұрлау немесе бөтеннің мүлкіне құқықтарды иемдену түрі [1]. Алаяқтықтың түрлері мен формалары әртүрлі болуы мүмкін. Интернет тек ақпарат алатын орын ғана емес, сонымен қатар заңсыз баю мақсатында жеке және заңды тұлғалардың жеке деректеріне заңсыз ену құралына айналды. Ақпараттық технологиялардың дамуымен және олардың қолданылу аясының кеңеюімен алаяқтықтың жаңа түрлері пайда болды, оның ішінде онлайн алаяқтар деп аталатындар да пайда болды. Қылмыстық кодекстің 190-бабы екінші бөлігінің төртінші тармағында интернет-алаяқтық үшін қылмыстық жауапкершілік көзделгенімен, олардың саны жыл сайын артып келеді.

Соңғы бірнеше жылда қылмыстардың, атап айтқанда алаяқтықтың динамикасын талдау осы жағдайлардың көбеюін көрсетеді [2]. Атап айтқанда, статистикалық мәліметтерге сүйенсек, алаяқтық қылмыстар саны 2020 жылы 27 мың, 2021 жылы 35 мың, 2022 жылы 37 мың жағдайды құраса, 2023 жылы қазан айына дейінгі ақпаратқа сәйкес 37 мың болып қалуда. Соның ішінде, онлайн алаяқтық саласы да өзекті болып қала береді және ағымдағы жылдың басынан бері 20 мыңнан астам оқиға тіркелген.




ҚР Қылмыстық кодексінің 190-бабы Алаяқтық қылмыстарының тіркелген динамикасы

Технологияның дамуымен және әлеуметтік медиа, мобильді төлем жүйелері және бұлтты технологиялар сияқты интернет байланысының жаңа түрлерінің пайда болуымен алаяқтар үшін мүмкіндіктер ауқымы да кеңейе түседі. Бұл қылмыстың осы түрін анықтау және онымен күресу әдістерін ұдайы талдап, бейімдеуді қажет етеді. Онлайн-алаяқтық экономикаға зиян келтіріп қана қоймайды, сонымен қатар оның табысының кілті болып табылатын цифрлық технологияға деген сенімге нұқсан келтіреді. Қазақстан да көптеген басқа елдер сияқты онлайн алаяқтық мәселесімен

бетпе-бет келіп отыр, бұл оның алдын алу және жолын кесу бойынша тиімді шараларды әзірлеуді талап етеді.

Онлайн алаяқтық адамды немесе адамдар тобын алдау, сондай-ақ қылмыстық әрекетке ынталандыру және осы әрекеттерді жасаудың жаңа, әлі зерттелмеген әдістерін қолдану мақсатында ақпараттық технологияларды пайдалана отырып жасалған қылмыстардың жиынтығымен сипатталады.

Онлайн алаяқтық контекстінде шабуылдаушылар жеке тұлғаларды да, компьютерлік жүйелерді де нысанаға алуы мүмкін. Электрондық жүйелер жағдайында пайдаланушыларды фишингтік веб-ресурстарға бағыттауға бағытталған жасырын бағдарламалық құралдар, сондай-ақ сақталған парольдерді және зиянды кодтың басқа түрлерін тіркеуге арналған пернетақталық шпиондық бағдарламалар қолданылады.

Криминология және алаяқтықты зерттеу контекстінде С.И. Ожеговтың «Орыс тілінің түсіндірме сөздігіне» [3] сәйкес қылмыс жасаудың «әдісі» жұмысты орындау немесе белгілі бір мақсатты жүзеге асыру кезінде қолданылатын әрекеттер немесе әрекеттер жүйесі ретінде анықталатынын ескеру қажет. Бұл, әсіресе, қылмыс жасау әдісі ақпараттық және телекоммуникациялық технологияларды қолданумен байланысты ерекшеліктерге ие болатын онлайн алаяқтықты талдау кезінде маңызды.

Интернеттегі алаяқтар, әдетте, жоғары интеллект пен психологияны білетін адамдар болып табылады, бұл оларға тиімді байланыс орнатуға және құрбандарды жеңуге мүмкіндік береді. Олар көбінесе экономика және ақпараттық технологиялар бойынша мамандандырылған білімге ие, бұл оларды күрделі алаяқтық схемаларын жасауға және оларды интернетте қолдануға қабілетті етеді. Осылайша, онлайн алаяқтық әдістерінің ерекшеліктерін және алаяқтардың сипаттамаларын түсіну мұндай қылмыстардың алдын алу шараларын әзірлеудің негізгі элементі болып табылады.

Сонымен, қазіргі кезеңде онлайн алаяқтықтың қандай түрлері бар екенін талдайық:

«*Фишинг*» (ағылш. phishing) қазіргі кезеңде интернет желісіндегі алаяқтықтың жетекші әдісі болып табылады. Алаяқтықтың бұл түрі құпия сөздерді бұзуға және несие картасының төлем ақпараты, банк шоттары және қаржылық ақпарат сияқты құпия ақпаратты ұрлауға бағытталған [4, 57 б.]. Алаяқтар белгілі ұйымдар атынан жаппай электрондық хаттар жіберу, фишингтік сайттар мен түпнұсқа сайттарға ұқсайтын, бірақ URL мекенжайы басқа жалған беттер жасау сияқты түрлі айла-амалдарды пайдаланады.

Фишингтің негізгі элементі – құпия сөзді немесе басқа қорғалған ақпаратты ұрлау мақсатында белгілі веб-сайттың көшірмесін жасау. Фишингтік беттің пайда болуы түпнұсқаның өте сенімді көшірмесі болып табылады және пайдаланушылар мекенжай жолағына назар аудармайтындықтан бұл алдауға жиі түседі.

Фишингке қарсы тұру үшін күдікті сілтемелерді, әсіресе бейтаныс адамдар жіберген сілтемелерді ашпау және браузерлерде көп факторлы авторизация жүйесін және фишингке қарсы қорғанысты пайдалану ұсынылады. Сонымен қатар, күнделікті қолданатын Chrome, Safari, Firefox сияқты веб-парақшаларда пайдаланушыларға күдікті сайттар туралы ескертетін және олардан кетуді ұсынатын антифишинг мүмкіндіктері бар.

Фишинг түрлерінің ішінде интернет желілерін пайдаланушылардан банктік шотқа қатысты мәселелерді шешу үшін көрсетілген нөмірге қоңырау шалу сұралатын дауыстық фишинг, сондай-ақ құпия ақпаратты алу үшін қысқа мәтіндік хабарламаларды пайдаланатын SMS фишингі бар. Екі әдіс те қолданушының жеке деректерін алуға және шоттарындағы қаржыға қол жеткізуге бағытталған.

«*Вишинг*» (ағылшынша vishing, voice + phishing) — телефон байланысы арқылы әлеуметтік инженерияны қолдануға негізделген алаяқтық әдісі. Бұл процесс банк қызметкерлері немесе әлеуетті сатып алушылар сияқты сенімді тұлғалар ретінде әрекет ете отырып, төлем карталарының иелерінен құпия ақпаратты алуға ұмтылатын шабуылдаушылар әрекеттерін қамтиды [5]. Олар жәбірленушілерді түрлі сылтаулармен банктік шоттарымен немесе төлем карталарымен операциялар жүргізуге көндіруі мүмкін.

Бұл әдіс төлем жүйесінің клиенттері жүйе әкімшілігінен немесе қауіпсіздік қызметінен болжамды электрондық пошта хабарларын алатын фишингке ұқсас. Бұл хабарлар әдетте кіру тіркелгі деректерін, құпия сөздерді және басқа құпия ақпаратты сұрайды. Фишингтің маңызды ерекшелігі – деректерді ұрлау үшін жалған веб-сайттарды пайдалану, олар көбінесе жойылып, жасаушыларды қадағалауды қиындатады.

Вишинг, фишингтен айырмашылығы, көбінесе белгілі бір нөмірге телефон арқылы қоңырау шалу туралы өтінішті қамтиды, жәбірленушіге дауыстық немесе тональды енгізу арқылы жеке мәліметтерін беру ұсынылады. Мұндай вишинг оқиғалары алғаш рет 2006 жылы тіркелген. Алаяқтықтың бұл түрінен қорғау фишингтің алдын алу үшін қолданылатын білім мен сақтықты қажет етеді.

«*Нигерия хаттары*» (ағылш. Advance-fee scam , сөзбе-сөз «алдын ала төленген алаяқтық») – спам-хабарламаларды жаппай жіберуге негізделген алаяқтықтың ең көп таралған түрлерінің бірі. «Advance-fee scam» деп те аталатын алаяқтықтың бұл түрі өз атауын интернет пайда болғанға дейін Нигерияда мұндай хаттар кәдімгі пошта арқылы таратылған кезде де танымал болғанынан алады. Содан бері мұндай хаттар таратылып, 1980 жылдардың ортасында басталды, сонымен қатар Нигериядан ғана емес, басқа Африка елдерінен, сондай-ақ Лондон, Амстердам, Мадрид, Дубай сияқты ірі нигериялық диаспорасы бар қалалардан тарай бастады.

Алаяқтар әдетте электрондық пошта алушыларына миллиондаған немесе көп миллиард долларлық транзакциялар бойынша көмек сұрап, транзакцияға үлкен қызығушылықты уәде етеді. «Бизнес серіктесінің»

келісімімен ол біртіндеп әр түрлі сылтаулармен, мысалы, баждарды төлеу, шенеуніктерге пара беру, құжаттарды рәсімдеу және мәмілелер жасау қажеттілігімен азғырылады. Алаяқтар көбіне ақшаны төлеу үшін үйімді кепілге қойдым немесе жеке мүлкін саттым деп психологиялық қысым жасайды.

Сонымен қатар, спам-хабарламалардың алуан түрлілігі шетелде тұру және билеттер үшін алдын-ала төлемді талап ететін жұмыс ұсыныстарын, қайтыс болған туыстарының адвокаттарынан мұраға жәрдемдесу туралы хабарламаларды, табыс салығын төлеуді талап ететін лотерея ұтыстары туралы хабарламаларды, тіпті жоқ шіркеулерге қайырымдылық жасауға шақыруды қамтиды. Алаяқтар өздерінің жалған ұсыныстарын тарату үшін әлеуметтік медианы, танысу сайттарын және электрондық хабарландыру тақталарын белсенді пайдаланады.

Алаяқтықтың бұл әдісі көптеген жылдар бойы болғанына қарамастан, оның жаппай және әдістердің үнемі жаңаруы жаңа құрбандардың пайда болуына әкелуде. № 419 коды бар Нигериялық хаттар интернеттегі алаяқтықтың ең көрнекті және тұрақты түрлерінің бірі болып қала береді [6, 119 б.].

*Фарминг* (ағылш. «Фарминг» – ағылш. «phishing» және «farming» - егіншілік, мал шаруашылығы сөздерінің туындысы) – бұл желідегі пайдаланушыларды жалған IP мекенжайларына жасырын қайта бағыттауды қамтитын манипуляциялық процесс. Қарапайым фишингтен айырмашылығы, алаяқтар логин мен құпия сөздерді алу үшін жалған веб-сайттарға құрбандарды тарту үшін әлеуметтік желілер, онлайн-банкинг және веб-пошта қызметтерінің пайдаланушыларына электрондық хаттар жібереді, фарминг күрделі әдістерді пайдаланады.

Заманауи интернет қызметтерімен белсенді әрекеттесетін пайдаланушылар фишингтік шабуылдарға жиі тап болады және күдікті хабарларға сақтық танытады. Классикалық фишинг схемасында тиімділіктің шешуші факторы пайдаланушының сенімділігі болып табылады. Фишингтік шабуылдар туралы хабардарлықтың артуына байланысты банктер мен әлеуметтік медиа қоғамды әлеуметтік инженерияға негізделген әртүрлі алаяқтық схемалар туралы белсенді түрде хабардар етеді, бұл сәтті фишингтік шабуылдардың азаюына ықпал етеді. Бұған жауап ретінде алаяқтар зиянды бағдарламалық жасақтаманы пайдаланушылардың компьютерлеріне таратуды көздейтін фарминг механизмін жасады [7]. Мұндай бағдарламалық жасақтаманы іске қосқаннан кейін белгілі бір сайттарға жасалған сұраныстар жалған ресурстарға бағытталады, бұл шабуылдардың жоғары жасырындығын қамтамасыз етіп, пайдаланушының белсенділігіне қойылатын талаптарды азайтады. Қазіргі уақытта фарминг шабуылдарынан абсолютті қорғаныс әдістері жоқ, дегенмен лицензияланған антивирустық бағдарламалық жасақтаманы пайдалану және оны үнемі жаңартып отыру, электрондық

пошта жәшігін қорғау және белгісіз немесе күмәнді көздерден электрондық пошта тіркемелерін ашудан және жүктеуден аулақ болу сияқты алдын алу шараларын қолдану ұсынылады.

Интернет-дүкендер мен жеке хабарландырулар сайттары көбінесе алаяқтардың аренасына айналады. Алдаудың ең көп тараған тәсілі – бұл үлкен жеңілдікпен немесе жүз пайыздық алдын-ала төлемді талап ететін тауарды сату. Төмен бағаға алданған сатып алушылар көбінесе төлем жасалғаннан кейін тауар жеткізілмейтініне немесе, жолы болған жағдайда, бос пакетті алатынын байқайды.

Көптеген алаяқтық схемаларының арасында адам интернет-дүкенде өнімді сатып алатын, бірақ алған заты ешқашан келмейтін жағдайлар жиі кездеседі. Басқа сценарийде жәбірленуші билетті брондайды, тек вокзалда орынды басқа жолаушы алғанын біледі. Бұл бір күндік дүкендер көбінесе қысқа науқандарда тауарларды айтарлықтай төмендетілген бағамен ұсынады, ал сатып алушылар үнемдеуді қалап, тапсырысты төлеуге асығады.

Сонымен қатар, жеке жарнама сайттарындағы алдау тағы бір жиі кездесетін мәселе. Қалаған затын төлеген сатып алушылар оны алмай, шығынға ұшырайды. Мұндай қауіптен сақтану қиынырақ, өйткені сайттардағы жаңа қолданушылардың көпшілігі адал пайдаланушылар. Мұндай жағдайларда ең жақсы шешім жеке кездесу болуы мүмкін.

Мұндай жағдайлардың алдын алу үшін тауарларды (әсіресе қымбат) кем дегенде бір жылдық жұмыс тарихы бар сенімді интернет-дүкендерден сатып алу және тартымды ұсыныстарға тап болған кезде асығыс шешім қабылдаудан аулақ болу ұсынылады.

Ақпараттық қауіпсіздік контекстінде зиянды бағдарламалар, соның ішінде вирустар, интернет құрттары және трояндық аттар цифрлық жүйелерге айтарлықтай қауіп төндіреді. Іске қосылғаннан кейін белсендірілетін және таралатын вирустар жиі бос компьютер жадын толтырады және өңдейді, Windows операциялық жүйесін бұзып, құпия пайдаланушы деректеріне рұқсатсыз кіруді қамтамасыз етеді.

Электрондық пошта, әлеуметтік медиа, жүктеп алулар, USB құрылғылары мен ықшам дискілер осы вирустардың таралуының негізгі арналары болып табылады. Интернет құрттарының айрықша ерекшелігі-олардың басқа бағдарламаларға енбестен таралу қабілеті, бұл олардың желілік түйіндер арқылы автономды және қарқынды таралуына мүмкіндік береді, кейде вирустық шабуылдардан асып түсетін зиян келтіреді.

Қауіптің тағы бір түрі заңды қолданбалар ретінде көрінетін трояндық аттар болып табылады. Олардың өзін-өзі репликациялау мүмкіндігі жоқ, бірақ пайдаланушы оларды қате пікірде іске қосқан кезде тиімді шабуыл құралдары бола алады. Олардың кейбіреулері жүйеде «артқы есіктер» жасай алады, бұл шабуылдаушыларға  жеке ақпаратқа қол жеткізуге мүмкіндік береді..

Кейбір трояндық бағдарламалар компьютерлік жүйеге ену үшін оның қауіпсіздік жүйелерін дербес жеңе алады. Алайда, көп жағдайда олар компьютерге басқа вируспен бірге енеді. Трояндық бағдарламаларды қосымша зиянды бағдарлама ретінде қарастыруға болады. Көбінесе пайдаланушылар трояндық бағдарламаларды интернеттен жүктеп алады.

Трояндық бағдарламалардың өмірлік циклін келесі кезеңдермен анықтауға болады:

- жүйеге ену;
- белсендіру;
- зиянды әрекеттерді орындау.

Алайда, ену және жұқтыру механизмдерін біле отырып, амалдық жүйенің бағдарламалық модульдерінің кодтарын түзетуге болады. Оның бір жолы – пайдаланушы бағдарламаларының бір-бірімен тікелей байланысуына жол бермеу; делдал – операциялық жүйені пайдалана отырып, бір-бірімен өзара әрекеттесуге мүмкіндік береді [8, 130 б.].

Шабуылшылар көбінесе бағдарламалық жасақтаманың осал тұстарын пайдаланады, аппараттық құралдарға шабуыл жасайды немесе тіпті желілерге қол жеткізу үшін басқа адамдардың логиндері мен құпия сөздерін болжау сияқты әлеуметтік инженерия әдістеріне жүгінеді. Бұл қауіптің төрт негізгі түріне әкелуі мүмкін: ақпаратты, жеке деректерді және қолма-қол ақшаны ұрлау, сондай-ақ алаяқтықтың басқа да түрлері.

Біздің зерттеуімізде қазіргі әлемде белсенді дамып келе жатқан интернет-алаяқтықтың әртүрлі формалары мен әдістерін қарастырдық. Сияқты алаяқтықтың негізгі түрлері фишинг, вишинг, Нигерия хаттары және фарминг, жеке пайдаланушылар үшін де, бүкіл ұйымдар үшін де айтарлықтай қауіп төндіреді.

Бұл қауіптерге тиімді қарсы тұру заңнаманы күшейтуді, пайдаланушылардың тәуекелдер мен алаяқтық тәжірибелері туралы хабардарлығын арттыруды және ақпараттық қауіпсіздік саласындағы озық технологияларды әзірлеу мен енгізуді қоса алғанда, кешенді тәсілді талап етеді.

Сондай-ақ, интернет-алаяқтықпен күресудің негізгі факторларының бірі ретінде киберқауіпсіздік саласындағы білім мен білімнің рөлін атап өту қажет. Оқу бағдарламалары мен ақпараттық науқандар пайдаланушыларды желідегі ықтимал қауіпті жағдайларды тануға және болдырмауға үйретуге бағытталуы керек.

Қорытындылай келе, алаяқтық технологиялары мен әдістерінің қарқынды дамуын ескере отырып, цифрлық әлемде тиімді қорғауды қамтамасыз ету үшін үнемі бақылау және жаңа қауіптерге бейімделу қажет. Онлайн алаяқтықтың алдын алу үшін жауапкершілік құқық қорғау органдарында да, интернет желісінің әрбір пайдаланушысында да болады.

**Пайдаланылған дереккөздердің тізімі:**

1. Қазақстан Республикасының Қылмыстық Кодексі 2014 жылғы 03 шілдедегі № 226-V ҚРЗ // https://adilet.zan.kz/rus/docs/K1400000226;

2. Құқықтық статистика // Тіркелген қылмыстық құқық бұзушылықтар бойынша негізгі көрсеткіштер туралы мәліметтер URL: https://qamqor.gov.kz/crimestat/indicators/criminal (жүгінген күні: 03.11.2023).

3. Ожегов С.И. Толковый словарь русского языка: около 100 000 слов, терминов и фразеологических выражений / под ред. Л.И. Скворцова. 26-е изд., испр. и доп. М.: Оникс [и др.]. – 2009. – 1359 б.;

4. Сазонов М.М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения // Виктимология.– № 2 (16). – 2018. – 55-60 бб.

5. Вадим Свидерский. Осторожно, вишинг! / Свидерский Вадим. — Текст: электронный // Forex Magnates Русская версия: [сайт]. — URL: https://ru.forexmagnates.com/ostorozhno-vishing/ (жүгінген күні: 26.10.2023).

6. В.В. Радевич. Этапы и виды манипуляции как коммуникативной стратегии в неискреннем дискурсе на материале жанра «Нигерийские письма». СибСкрипт. – 4 (4). – 119-122 бб.

7. «Фарминг»: скрытый вариант фишинга. — Текст: электронный // — URL: https://web.archive.org/web/20180829025309/http://www.symantec.com/region/ru/resources/2006/article_1_8.html (жүгінген күні: 28.10.2023).

8. Трубачёв Евгений Сергеевич. «Троянские программы: механизмы проникновения и заражения». В.Н. Татищев атындағы Еділ университетінің хабаршысы, № 18. – 2011. – 130-134 бб.

**Бақыт С.Б.**
Құқықтану және халықаралық құқық кафедрасы
1 курс докторанты
«Тұран» университеті
Алматы қ., Қазақстан Республикасы

**Жанибеков А.К.**
әл-Фараби атындағы ҚазҰУ
Қылмыстық құқық, қылмыстық іс жүргізу
және криминалистика кафедрасы
PhD докторы, қауымдастырылған профессоры
Алматы қ., Қазақстан Республикасы

# ҚЫЛМЫСТЫҚ ІС ЖҮРГІЗУ БАРЫСЫНДАҒЫ САРАПТАМАЛЫҚ ҚОРЫТЫНДЫЛАРДЫҢ ДӘЛЕЛДЕМЕ РЕТІНДЕ ЖОЛ БЕРІТІНДІГІ МЕН АНЫҚТЫҒЫ МӘСЕЛЕСІ

Бұл мақала қылмыстық сот ісін жүргізу контекстіндегі сарапшы қорытындысының жол берілетіндігі мен анықтығын бағалау мәселесіне арналған. Сарапшының қорытындысы қылмыстық істердегі маңызды дәлел