ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

как OAuth или JWT для управления сеансами. Однако недавнее исследование, проведенное командой OpenAI, показало, что GitHub Copilot иногда может генерировать небезопасные фрагменты кода из-за ограничений в его обучающих данных, которые включают общедоступный код из репозиториев GitHub, некоторые из которых могут содержать уязвимости. В отличие от этого, Cursor AI был разработан с акцентом на кибербезопасность, интегрируя инструменты безопасности и предоставляя рекомендации по кодированию, соответствующие принципам безопасного программирования. Ярким примером является его роль в оказании помощи разработчикам в создании безопасных RESTful API, рекомендуя такие меры безопасности, как проверка вводимых данных, шифрование и безопасная обработка токенов. Одним из примеров, когда Cursor AI оказался особенно полезен, была разработка нового мобильного банковского приложения, где разработчики столкнулись с трудностями при обеспечении безопасности транзакций и персональных данных. Благодаря рекомендациям Cursor AI они смогли внедрить надежные протоколы шифрования и предотвратить такие распространенные уязвимости, как внедрение SQL-инъекций. Кроме того, интеграция Cursor AI с такими инструментами безопасности, как Aikido, демонстрирует, как ИИ может проактивно обнаруживать уязвимости в режиме реального времени. Например, Aikido и Cursor AI использовались совместно для сканирования кодовой базы платформы электронной коммерции на предмет уязвимостей в системе безопасности. Сочетание подсказок по коду, основанных на искусственном интеллекте, и обнаружения угроз в режиме реального времени помогло выявить несколько критических уязвимостей, включая небезопасные методы хранения данных, которые затем были исправлены до того, как приложение было выпущено для широкой публики. Эти тематические исследования имеют решающее значение, поскольку они демонстрируют практическое применение инструментов искусственного интеллекта для повышения кибербезопасности, особенно в реальных сценариях, и подчеркивают уникальную направленность Cursor AI на обеспечение безопасности, как показано в таблице 1. В таблице сравниваются функции Cursor AI, ориентированные на безопасность, с другими инструментами искусственного интеллекта, что еще раз иллюстрирует его преимущества при разработке безопасного программного обеспечения.

Список использованных источников

1. Stallings, W. (2017). *Data and Computer Communications*. Pearson Education.
2. OpenAI. "AI-assisted coding: Enhancing software security and efficiency." *AI Research Journal*, 2023.
3. OWASP Foundation. "Secure coding practices: A guide for developers." *Cybersecurity Standards Report*, 2022.
4. Smith, J., & Lee, W. (2021). "Machine learning in cybersecurity: Applications and risks." *Cyber Defense Journal*.
5. Raza, S., Wallgren, L., & Voigt, T. (2013). "SVELTE: Real-time intrusion detection in the Internet of Things." *Ad Hoc Networks*, 11(8), 2661-2674.

СТЕГАНОГРАФИЯ В КИБЕРБЕЗОПАСНОСТИ КАЗАХСТАНА

А.М. Султанов

salikovalpamys@gmail.com

Бакалавр Евразийский национальный университет им. Л.Н. Гумилева, Астана

Научный руководитель – Онгарбаева Айнагуль Игиликовна

Аннотация

В данной статье рассматриваются современные аспекты применения стеганографии в сфере кибербезопасности Казахстана. Особое внимание уделено основным методам скрытия информации в цифровых объектах, таким как изображения, аудиофайлы, видеозаписи и сетевые протоколы. Проанализированы потенциальные преимущества стеганографии для защиты данных, а также угрозы, связанные с её использованием киберпреступниками. В статье рассматриваются существующие вызовы, стоящие перед Казахстаном в области кибербезопасности. Также сатья рассматривает развитие технологий обнаружения стеганографических угроз и сотрудничество с международными организациями.

Ключевые слова: стеганография, кибербезопасность, Казахстан, защита данных, скрытая информация, цифровая безопасность.

Введение: В эпоху цифровых технологий и развития киберугроз защита информации становится ключевой задачей для любого государства. Казахстан, активно развивающий цифровую экономику и электронное правительство, сталкивается с новыми вызовами в области кибербезопасности. Одним из перспективных инструментов защиты данных является стеганография — метод скрытия информации внутри цифровых объектов. Однако наряду с преимуществами стеганография также используется злоумышленниками для сокрытия вредоносного кода и передачи конфиденциальных данных. В данной статье рассматриваются современные вызовы и возможные решения в области применения стеганографии в кибербезопасности Казахстана.

Стеганография — это метод сокрытия данных в цифровых объектах, таких как изображения, аудиофайлы, видео или сетевые протоколы. В отличие от криптографии, которая скрывает сам смысл сообщения, стеганография скрывает сам факт его существования. Это делает её полезным инструментом как для защиты информации, так и для её несанкционированного использования. Стеганографические методы классифицируются по нескольким основным признакам, таким как тип носителя информации, способ внедрения скрытых данных и уровень сложности обнаружения. По типу носителя информации:

1. Изображения – один из самых популярных носителей для стеганографии. Данные встраиваются в пиксели изображения путем изменения младших битов цветовых компонентов (LSB-метод), изменения частотных характеристик (DCT-метод) или применения пространственных преобразований.

2. Аудиофайлы – используются для сокрытия данных путем незначительного изменения амплитуды звуковых волн или манипуляций с фазами частотных компонентов. Методы включают LSB-стеганографию, фазовое кодирование и скрытие данных в шуме.

3. Видео – скрытие информации происходит аналогично методам стеганографии в изображениях, но с учетом временного измерения, позволяя изменять пиксели в разных кадрах.

4. Текст – стеганография может реализовываться путем изменения пробелов, использования синонимов, перестановки букв или внедрения специальных символов, невидимых для пользователя.

Сетевые протоколы – скрытая передача данных может осуществляться путем изменения заголовков пакетов, использования специфических временных задержек или модификации управляющих сигналов.

По методу внедрения:

1. Замена битов (LSB-метод) – наиболее распространенный способ, при котором изменяются младшие значащие биты пикселей изображения или аудиоданных, что делает изменения практически незаметными.

$$P' = P - (P \bmod 2^n) + m$$

P — исходное значение пикселя,

P' — измененное значение пикселя,

n — количество изменяемых бит,

M — скрываемая информация (вставляемые биты).

2. Спектральное скрытие – данные маскируются в частотных областях с применением дискретного косинусного преобразования (DCT) или дискретного вейвлет-преобразования (DWT).

$$A_k = \sum_n x\,(n)\phi(2k-n)$$

A — приближенные сигналы

D — детализированные сигналы

3. Геометрическое преобразование – метод заключается в незначительном изменении формы носителя, например, деформации изображений или варьировании временных параметров в аудиофайлах.

$$\begin{bmatrix} x^1 \\ y^1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} t & y \\ t & x \end{bmatrix}$$

x, y— исходные координаты,

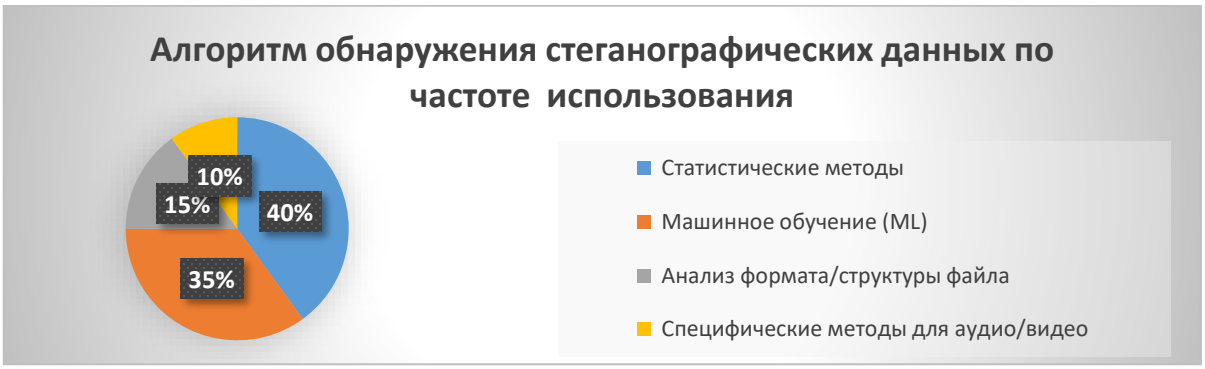
x', y' — новые координаты,

a, b, c, d — параметры трансформации,

tx, ty — смещения.

В сфере кибербезопасности Казахстана стеганография может применяться для:

- Защиты государственных и корпоративных данных;
- Создания цифровых водяных знаков для защиты авторских прав;
- Обеспечения безопасной передачи конфиденциальных данных;
- Обнаружения скрытых угроз и вредоносного кода.



Несмотря на перспективность, стеганография также представляет определенные риски для кибербезопасности Казахстана:

1 .Использование стеганографии в кибератаках. Злоумышленники могут использовать стеганографию для сокрытия вредоносных программ в изображениях, аудиофайлах и видео. Это затрудняет обнаружение угроз традиционными антивирусными программами. В 2023 году исследователи в области кибербезопасности обнаружили, что вредоносное ПО может передаваться через обычные медиафайлы, скрывая команды внутри их структуры. В Казахстане в 2022 году была зафиксирована атака на крупную финансовую компанию, когда злоумышленники использовали стеганографию для передачи команд ботнету через изображения, размещённые на легитимных сайтах.

2. Недостаток инструментов для обнаружения стеганографических угроз. В Казахстане недостаточно развито программное обеспечение для выявления стеганографически скрытых данных. Традиционные системы мониторинга сетевого трафика и

антивирусные программы часто не способны идентифицировать скрытые сообщения. Казахстанские банки, такие как Halyk Bank и Kaspi Bank, внедряют системы анализа киберугроз, однако обнаружение стеганографических методов остаётся сложной задачей.

3. Использование стеганографии в финансовых преступлениях. Злоумышленники могут применять стеганографию для обхода систем финансового мониторинга, передавая скрытые команды в цифровых транзакциях или фальсифицируя документы. В 2023 году Агентство финансового мониторинга Казахстана зафиксировало случай, когда преступники скрывали команды для отмывания денег в зашифрованных изображениях, передаваемых через социальные сети.

В Казахстане есть компании и организации, которые активно работают в области кибербезопасности и внедряют новые технологии для защиты данных:

1. TSARKA — один из ведущих центров по расследованию кибератак, активно занимается анализом новых угроз, в том числе связанных со стеганографией.

2. KZ-CERT — национальный центр киберзащиты, который мониторит угрозы и разрабатывает стратегии борьбы с кибератаками.

3. Kaspi Bank — внедрил технологии искусственного интеллекта для анализа транзакций и предотвращения мошенничества.

4. Halyk Bank — использует системы анализа больших данных для выявления подозрительных финансовых операций. Эти организации играют ключевую роль в обеспечении кибербезопасности Казахстана и могут стать первыми, кто внедрит системы обнаружения стеганографических угроз.

Международный опыт и сотрудничество. Многие страны уже внедрили технологии обнаружения стеганографии для борьбы с киберугрозами. В США, Великобритании и Германии активно развиваются системы машинного обучения, позволяющие анализировать цифровые файлы на предмет скрытых данных. В частности, Национальное агентство безопасности США (NSA) и Центр правительственной связи Великобритании (GCHQ) разрабатывают инструменты для выявления стеганографических атак. Согласно исследованию Европейского агентства по кибербезопасности (ENISA), в 2023 году более 60% кибератак в ЕС использовали методы скрытия данных, включая стеганографию, что вызвало необходимость внедрения новых инструментов мониторинга трафика.

Казахстан активно сотрудничает с международными организациями, такими как INTERPOL и Международный союз электросвязи (ITU), для обмена опытом и разработки стандартов в области борьбы со стеганографией. Казахстан интегрирует свои кибербезопасные структуры, такие как KZ-CERT, в глобальные инициативы по защите цифрового пространства.

На данный момент Казахстан реализует ряд мер, направленных на усиление защиты от киберугроз, включая противодействие стеганографии. Одним из ключевых документов в этой сфере стала Концепция кибербезопасности «Киберщит Казахстана», утвержденная в 2017 году. Она направлена на создание комплексной системы защиты цифрового пространства страны и предотвращение угроз, связанных с кибератаками. В декабре 2023 года был принят закон, вносящий изменения в нормативные акты, регулирующие вопросы информационной безопасности. В нем особое внимание уделяется защите персональных данных и регулированию деятельности в сфере цифрового майнинга. Также в рамках этого закона были инициированы программы по сотрудничеству с экспертами в области кибербезопасности для выявления и устранения уязвимостей в информационных системах.

На международном форуме Digital Almaty 2025 обсуждалось применение технологий искусственного интеллекта в сфере защиты информации. Как отметил глава Комитета по информационной безопасности Министерства цифрового развития, в Казахстане активно внедряется платформа Bug Bounty, а также интегрируются более 220 государственных информационных систем с платформой защиты данных. Эти технологии позволяют

оперативно выявлять уязвимости и предотвращать угрозы, включая методы сокрытия информации с использованием стеганографии. В мае 2024 года было утверждено постановление правительства, определяющее новые требования по обеспечению информационной безопасности. Среди них – использование систем для предотвращения утечек данных (DLP), а также внедрение фильтрации сетевого трафика с применением межсетевых экранов. Эти инструменты повышают уровень защиты от скрытых методов передачи информации.

Таким образом, Казахстан активно совершенствует кибербезопасность, принимая законодательные инициативы, внедряя современные технологии и взаимодействуя с международными организациями.

Стеганография — это мощный инструмент, который может использоваться как для защиты данных, так и в целях кибератак. Для Казахстана важно не только применять стеганографию в области информационной безопасности, но и разрабатывать методы её выявления и предотвращения вредоносного использования. Развитие технологий обнаружения, законодательное регулирование и повышение осведомленности специалистов помогут Казахстану эффективно противостоять киберугрозам, связанным со стеганографией. Внедрение новых технологий и активное сотрудничество государственных и частных компаний в сфере кибербезопасности позволит укрепить цифровую защиту страны и минимизировать риски, связанные с использованием стеганографии в преступных целях.

Список использованных источников:

1. Кибербезопасность. Учебник для вузов. – Санкт-Петербург: Издательство ЛАНЬ, 2024. – 680 с.
2. Стеганографические методы защиты информации. – Москва: Издательство Картаслов, 2018. – 250 с.
3. Основы информационной безопасности и стеганографии: учебник и практическое руководство. – Казань: Издательство Казанского федерального университета, 2022. – 295 с.
4. Digital Watermarking and Steganography: Fundamentals and Techniques. – Boca Raton: CRC Press, 2017. – 292 p.

WI-FI ЖЕЛІСІНДЕ ШАҚЫРЫЛМАҒАН ҚОНАҚТАРДЫ АВТОМАТТЫ ТҮРДЕ АНЫҚТАУ ЖҮЙЕСІ

Танатаров Ернар, Іргебай Санжар, Султанов Алпамыс
ttt.ernar@gmail.com, irgebaikliptonit@gmail.com, salikovalpamys@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті, Ақпараттық қаупсіздік кафедра студенттері Танатаров Ернар, Іргебай Санжар, Султанов Алпамыс топ 39,39/1
Астана, Қазақстан
Ғылыми жетекшісі – Казиева Н.М.

Аңдатпа: Бұл мақалада Wi-Fi желісіндегі рұқсатсыз қосылған құрылғыларды автоматты түрде анықтау жүйесі қарастырылады. Жүйе желідегі құрылғыларды бақылап, белгісіз MAC-адрестерді сенімді құрылғылар тізімімен салыстырады. Егер рұқсат етілмеген құрылғы анықталса, әкімшіге Telegram API арқылы жедел хабарлама жіберіледі. Python және Scapy құралдарының көмегімен жүзеге асырылған бұл жүйе ARP және DHCP сұраныстарын пайдаланып, желідегі құрылғылардың белсенділігін талдайды. Сонымен қатар, Kali Linux негізінде қауіпсіздік тесттері жүргізіліп, желінің қорғаныс деңгейі бағаланады. Ұсынылған шешім ұйымдар мен жеке тұлғалар үшін Wi-Fi инфрақұрылымының қауіпсіздігін нығайтуға