Міністерство освіти і науки України
Департамент науки і освіти Харківської облдержадміністрації
Харківське територіальне відділення МАН України

Відділення інформаційних технологій
Секція: кібербезпека

ПІДВИЩЕННЯ РІВНЯ КІБЕРГІГІЄНИ МОЛОДІ ЗАСОБАМИ ІНТЕРАКТИВНОЇ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Роботу виконав:
Рощупкін Максим Анатолійович,
учень 11 класу Комунального закладу
«Харківський ліцей № 4
Харківської міської ради»

Науковий керівник:
Бутко Юрій Анатолійович,
вчитель інформатики Комунального
закладу «Харківський ліцей № 4
Харківської міської ради»

Харків – 2024

ПІДВИЩЕННЯ РІВНЯ КІБЕРГІГІЄНИ МОЛОДІ ЗАСОБАМИ ІНТЕРАКТИВНОЇ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Рощупкін Максим Анатолійович, Харківське територіальне відділення Малої академії наук України**,** Комунальний заклад «Харківський ліцей № 4 Харківської міської ради Харківської області, 11 клас, м. Харків;

Бутко Юрій Анатолійович, вчитель інформатики Комунального закладу «Харківський ліцей № 4 Харківської міської ради»

У сучасному світі, де інформаційні технології стають всеосяжними, кіберпростір витісняє реальний світ, призводячи до нових форм злочинності. Кіберзлочини, вчинені за допомогою комп'ютерів та інтернету, становлять загрозу як національному, так і світовому рівням. Вивченню цієї проблеми приділяється увага як вітчизняних, так і зарубіжних науковців.

Незважаючи на це, користувачі недостатньо обізнані з сучасними видами кіберзлочинів, що призводить до великої кількості випадків кіберзлочинності. Дослідження має на меті розробити чат-бот, використовуючи інтерактивну соціальну інженерію, для підвищення рівня кібергігієни користувачів, зокрема дітей та підлітків, які є особливо вразливими до кіберзагроз.

Автор зосереджується на важливості освіти в області кібергігієни, особливо серед дітей та підлітків. Дослідження пропонує розробку чат-бота як інструменту для підвищення рівня обізнаності молоді про кібербезпеку через інтерактивне навчання.

Аналізуючи теоретичні аспекти кібергігієни, робота включає огляд основних принципів кібербезпеки, розкриваючи методи й засоби захисту в інтернеті. Також наголошується на ролі інтерактивної соціальної інженерії в освітньому процесі, яка сприяє залученню уваги та збільшенню ефективності навчання через практичну взаємодію.

Розробка та деталі функціоналу чат-бота демонструють, як інтерактивні завдання та симуляції можуть виявляти та виправляти недоліки в знаннях користувачів про кібербезпеку. Чат-бот надає користувачам навчальні матеріали, вікторини та сценарії, що допомагають зрозуміти та впоратися з різними кіберзагрозами.

Висновки роботи демонструють успішність запропонованого підходу до підвищення рівня кібергігієни серед молоді, що відображає значний вплив інтерактивного навчання на зміцнення кібербезпеки.

Ключові слова: кіберзлочинність, кібербезпека, інформаційні технології, чат-бот, інтерактивна соціальна інженерія, користувачі, дослідження

ЗМІСТ

ВСТУП ……. 4
РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ …… 6
1.1. Аналіз і уточнення поняття кібергігієна …… 6
1.2. Огляд основних принципів кібербезпеки та кібергігієни …… 7
1.3. Постановка задачі проєкту ……. 10
РОЗДІЛ 2. ІНТЕРАКТИВНА СОЦІАЛЬНА ІНЖЕНЕРІЯ …… 12
2.1. Теоретичні аспекти застосування інтерактивної соціальної інженерії ……. 12
2.2. Аналіз інструментів та методів інтерактивної соціальної інженерії ……. 13
2.3. Вибір методу рішення …… 14
РОЗДІЛ 3. ДЕТАЛІ РОЗРОБКИ ІНТЕРАКТИВНОЇ СИСТЕМИ ТЕСТУВАННЯ …… 16
3.1. Реалізація функціоналу чат-боту …… 16
3.2. Інтерфейс користувача …… 21
ВИСНОВКИ …… 26
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ІНФОРМАЦІЇ ……..…… 27

ВСТУП

Актуальність теми. У сучасному світі використання інформаційних технологій стає всеосяжним. Віртуальний простір поступово витісняє реальний, включаючи зростання злочинності в нових її формах та проявах. Поняття "кіберпростору", яке було вперше запропоноване письменником Вільямом Гібсоном у його романі "Neuromancer", описує віртуальний світ, де переміщуються електронні дані з усіх комп'ютерів світу.

Практично кожен чув про кіберзлочини, можливо, навіть самостійно стикався з ними. Кіберзлочинність включає в себе різноманітні види злочинів, які вчиняються за допомогою комп'ютерів та мережі Інтернет. Об'єктами атак є особисті дані, банківські рахунки, паролі та інша конфіденційна інформація, яка належить як фізичним особам, так і підприємствам і громадським структурам. Кіберзлочинність є загрозою не лише на національному рівні, але і на світовому.

Вивченню проблеми кібербезпеки приділяли увагу вітчизняні та зарубіжні науковці і практики: М. Грайворонський, А. Качинський, І. Лисенко, І. Шевченко, W. Gibson, S. Staff, F. Wamala та ін.

Теоретичним підґрунтям підвищення рівня кібергігієни користувачів є праці науковців та теоретиків (З. Свердлик, Є. Аушев, О. Бакалінська, О. Скибун та ін.).

Проте користувачі недостатньо підготовлені до нових видів та методів кіберзлочинців, слабо орієнтуються у сучасних прийомах і принципах сучасної кібербезпеки. І тому відсутність достатніх знань та досвіду обумовлюють велику кількість кіберзлочинів у сучасний час.

Отже, проблема низького рівня кібергігієни сучасного користувача, а особливо, користувачів дошкільного та шкільного віку й зумовило вибір теми нашого дослідження.

Мета дослідження: на основі теоретичного та емпіричного вивчення стану досліджуваної проблеми розробити чат-бот для підвищення рівня кібергігієни користувачів.

Наукова новизна: запропоновано та реалізовано чат-бот, який використовує методи інтерактивної соціальної інженерії, спрямований на виявлення слабких місць у питаннях кібергігієни користувачів, що дозволило підвищити їх рівень обізнаності щодо кібербезпеки.

Завдання:

1. Розкрити особливості підвищення рівня кібергігієни користувачів.
2. Обґрунтувати важливість підвищення рівня кібергігієни під час користування Інтернетом у сучасному світі.
3. Здійснити аналіз проблеми низького рівня кібергігієни сучасного користувача.
4. Розробити чат-бот з покращення рівня кібергігієни методами і засобами інтерактивної соціальної інженерії.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Аналіз і уточнення поняття кібергігієна

Кібергігієна, відома також як цифрова гігієна, - це підхід, який допомагає захищати ваше фізичне і психічне здоров'я при користуванні інтернетом і цифровими пристроями. Вона охоплює питання забезпечення фізичної безпеки при тривалому користуванні комп'ютерами і смартфонами, уникнення психологічних стресів, пов'язаних з інтернетом, і враховує засоби захисту в інтернеті та цифрові навички. Основною метою є забезпечити безпечне та відповідальне користування інтернетом, а також зберегти баланс між цифровим і реальним життям. Важливо навчати людей цифровій грамотності та постійно оновлювати підходи до кібергігієни у відповідь на нові технології та виклики.

Кількість інтернет-шахрайства, фактів втручання в особистий інформаційний простір, поширення неправдивих відомостей тощо нині набуває рис епідемії. Тож таке поняття як кібергігієна є звичайною та актуальною темою сьогодення. основні Виклики сучасного технічного прогресу вимагають знання загроз в цифровому просторі, розуміння, яка інформація є головною метою хакерів та засвоєння основних рекомендації щодо захисту власних даних, а також безпечного користування гаджетами та інформаційними ресурсами [2].

З плином часу та зростаючою залежністю від технологій, кібергігієна стала дуже актуальною темою. Особливо молодь та діти, які проводять багато часу в інтернеті, піддаються ризику та потребують освіти з цього питання.

Сучасна Глобальна мережа містить у собі цілу низку серйозних загроз, включаючи загрози зараження вірусами, крадіжку паролю та персональних даних, зламу інтернет гаманця та ін. Краща стратегія захисту – знати заздалегідь, звідки саме чекати загрози та який алгоритм дій виконати для уникнення зустрічі з нею. [2]

Кібергігієна є предметом досліджень та розвитку, оскільки суспільство намагається зрозуміти, як краще забезпечити безпеку та добробут користувачів в цифровому світі.

Виділяють декілька напрямків поняття кібергігієна, а саме [10]:

- **Фізична кібергігієна**: Цей аспект включає в себе питання фізичного здоров'я, пов'язані з довгими годинами перед екранами комп'ютерів або смартфонів. До таких проблем можна віднести синдром тунельного каналу, біль у спині, погіршення зору та інші фізичні симптоми.
- **Психологічна кібергігієна**: Цей аспект стосується впливу цифрового світу на психічне здоров'я. Соціальні мережі, онлайн-ігри та інші аспекти інтернету можуть призводити до стресу, тривожності, депресії та інших психологічних проблем.

Кібергігієна також включає в себе використання заходів безпеки в інтернеті, включаючи захист особистих даних, паролів та заходів проти шахраїв та кіберзлочинців. Освіта в галузі цифрової грамотності грає важливу роль у підвищенні рівня кібергігієни. Користувачі повинні бути обізнані в техніках визнання дезінформації та захисту від шахраїв. Важливо зберігати баланс між часом, проведеним в інтернеті, та часом в реальному житті. Це може допомогти уникнути залежності від технологій.

Важливо навчати молодь, а також дорослих, засобам підвищення рівня кібергігієни, а також відповідальному і безпечному користуванню цифровими пристроями.

Кібергігієна постійно еволюціонує і вимагає постійного оновлення з урахуванням нових технологій та викликів.

1.2. Огляд основних принципів кібербезпеки та кібергігієни

Основні принципи кібербезпеки визначають фундаментальні підходи та правила для забезпечення безпеки в цифровому середовищі.

- **Принцип найменших привілегій (Principle of Least Privilege, PoLP)**: Заснований на ідеї того, що користувачі та процеси повинні мати лише ті права та доступ, які необхідні для виконання їх завдань. Це обмежує можливість зламу системи через вразливість в правах доступу.
- **Принцип обмеження поведінки (Principle of Least Functionality, PoLF)**: Цей принцип передбачає обмеження функцій та можливостей системи на мінімум, щоб зменшити потенційні атаки та ризики.
- **Принцип захисту в глибину (Defense in Depth)**: Цей принцип передбачає встановлення кількох рівнів захисту, щоб навіть якщо один рівень компрометовано, інші рівні залишаються недоторканими.
- **Принцип контролю доступу (Access Control Principle)**: Забезпечення контролю доступу до ресурсів та інформації на основі правил та політик, що визначають, хто має доступ до чого.
- **Принцип безпеки по замовчуванню (Security by Default)**: Системи та програми повинні бути налаштовані з врахуванням максимальної безпеки за замовчуванням, а користувачі повинні самостійно активувати необхідні налаштування.
- **Принцип моніторингу та аудиту (Monitoring and Auditing)**: Ведення журналу подій, моніторинг активності та аудит допомагають вчасно виявляти порушення безпеки та ідентифікувати атаки.
- **Принцип безпеки паролів (Password Security Principle)**: Встановлення сильних паролів, двофакторної аутентифікації та регулярна зміна паролів для запобігання несанкціонованому доступу.
- **Принцип навчання користувачів (User Education Principle)**: Навчання користувачів правилам та прийомам безпеки в інтернеті для зменшення соціальної інженерії та інших атак.
- **Принцип захисту даних (Data Protection Principle)**: Захист конфіденційності та цілісності даних за допомогою шифрування, резервного копіювання та інших заходів.

- **Принцип вчасних оновлень (Timely Patching Principle)**: Вчасне встановлення патчів і оновлень для програм та операційних систем для закриття вразливостей.
- **Принцип відповідальності (Accountability Principle)**: Визначення та відстеження відповідальних осіб за безпеку та захист системи.

Основні принципи кібергігієни спрямовані на збереження фізичного та психологічного здоров'я користувачів в цифровому середовищі, зменшення ризику виникнення проблем та атак в інтернеті. Розглянемо основні з них:

- **Баланс між часом в інтернеті та реальним життям**: Важливо зберігати рівновагу між часом, проведеним в інтернеті, і часом, відведеним на інші аспекти життя, такі як робота, сім'я та відпочинок. Поглинання цифровим світом може призвести до соціальної ізоляції та інших проблем.
- **Цифрова пауза (Digital Detox)**: Регулярні перерви від інтернету можуть допомогти відновити фізичне та психічне здоров'я. Вони дозволяють відпочити від екранів та знизити стрес.
- **Безпека паролів і акаунтів**: Використовуйте міцні паролі та двофакторну аутентифікацію для захисту особистої інформації та онлайн-акаунтів.
- **Захист від кібербулінгу і онлайн-насильства**: Важливо вчасно виявляти та реагувати на кібербулінг, домагання та інші форми насильства в інтернеті.
- **Посилена цифрова грамотність (Digital Literacy)**: Навчання навичкам критичного мислення та розпізнавання дезінформації та фейків в інтернеті.
- **Керування особистою інформацією**: Будьте обережні з обміном особистою інформацією в мережі та встановлюйте налаштування приватності для своїх профілів.

- **Захист від шахраїв і фішингу**: Будьте уважні до підозрілих повідомлень та e-mail листів, а також навчайтеся розпізнавати спроби обману в інтернеті.
- **Освіта та навчання**: Навчайтеся безпеці в інтернеті та поширюйте знання про кібергігієну серед інших.
- **Керування часом інтернет-користування**: Встановлюйте години інтернет-користування та дотримуйтесь їх, щоб не допустити надмірного часу перед екранами.
- **Підтримка та допомога**: Не соромтеся звертатися до фахівців, друзів або батьків, якщо виникли проблеми з цифровою залежністю або інші проблеми в інтернеті.

1.3. Постанова задачі проєкту

Проект передбачає створення інтерактивного чат-боту з метою підвищення рівня кібергігієни серед користувачів, зокрема, спрямований на запобігання кіберзлочинності, забезпечення безпеки в інтернеті та покращення цифрової безпеки. Для досягнення цілей проекту передбачено наступні завдання: перш за все, розробка інтуїтивного та зрозумілого користувацького інтерфейсу чат-боту, який би дозволив легко оволодіти матеріалом користувачам з різним рівнем обізнаності в галузі кібербезпеки.

Однак, наряду з інтерфейсом, значну увагу буде приділено створенню навчальних матеріалів та модулів, що міститимуть інформацію про важливі аспекти кібергігієни. Це включатиме в себе теми, такі як безпека паролів, розпізнавання шахраїв та фішингу, уникнення соціальної інженерії, а також захист від кіберзлочинців. Для ефективного навчання буде враховано інтерактивність та цікавість матеріалів.

Після розробки чат-боту, планується його тестування з використанням груп-користувачів або інших методів для оцінки його ефективності та

корисності. Проект також включає в себе пункт щодо постійного вдосконалення чат-боту на основі зібраної статистики та фідбеку від користувачів.

Загальною метою є забезпечення зменшення ризику інцидентів в інтернеті, покращення обізнаності користувачів у сфері кібергігієни та підвищення безпеки в цифровому середовищі. Проект також передбачає підтримку та надання допомоги користувачам щодо кібергігієни та безпеки в інтернеті.

РОЗДІЛ 2
ІНТЕРАКТИВНА СОЦІАЛЬНА ІНЖЕНЕРІЯ

2.1. Теоретичні аспекти застосування інтерактивної соціальної інженерії

Інтерактивна соціальна інженерія - це методологія, яка вивчає та використовує психологічні та соціальні аспекти взаємодії між людьми з метою впливу на їхні дії, рішення та поведінку в цифровому та реальному світі.

Ця методологія базується на розумінні людської психології та соціальних взаємодій і використовує психологічні прийоми та техніки для створення сценаріїв, які спонукають людей до певних дій. Інтерактивна соціальна інженерія включає в себе фішинг (шахрайські атаки), обман, маніпуляцію та інші психологічні та соціальні методи, що використовуються для досягнення цілей.

Теоретичні аспекти застосування інтерактивної соціальної інженерії включають вивчення психології жертв та розробку маніпулятивних технік. Вони також важливі для розуміння того, як інтерактивна соціальна інженерія використовується в атаках на інформаційну безпеку та як їх можна захищати.

Також важливо розглядати теоретичні аспекти інтерактивної соціальної інженерії в контексті інформаційних війн і дезінформації, оскільки ця методологія може бути використана для маніпуляції інформацією та впливу на громадську думку.

З розвитком інтернету та цифрових технологій етичні та правові аспекти використання інтерактивної соціальної інженерії стають дедалі важливішими, і теоретичний аналіз допомагає розуміти питання, пов'язані із приватністю, правами та етикою у цьому контексті.

2.2. Аналіз інструментів та методів інтерактивної соціальної інженерії

Аналіз інструментів та методів інтерактивної соціальної інженерії включає в себе дослідження та розгляд технік та засобів, що використовуються для маніпуляції або впливу на людей з метою отримання інформації або навіть незаконних дій.

Розглянемо основні інструменти та методи, які використовуються в інтерактивній соціальній інженерії:

- **Фішинг**: Фішинг - це техніка, при якій атакуючий видає себе за довірену особу або організацію та намагається обманути жертву, щоб отримати конфіденційну інформацію, таку як паролі або особисті дані. Існують різні види фішингу, включаючи фішинг електронною поштою, фішинг на веб-сайтах та фішинг через соціальні мережі.
- **Обман та маніпуляція**: Ця техніка включає в себе створення образу або ситуації, які маніпулюють емоціями чи розумом жертви. Наприклад, може використовуватися обманливий заголовок новини, щоб викликати певну реакцію чи розповідь історії, яка викликає співчуття або обурення.
- **Соціальна інженерія через голосове спілкування**: Шахрай може видавати себе за представника важливої організації або служби підтримки та намагатися отримати інформацію через голосове спілкування, використовуючи психологічні та соціальні техніки.
- **Імперсонація та підробка**: Шахрай може імітувати або підробити веб-сайти, логотипи, листи чи повідомлення, щоб виглядати достовірно. Це може включати в себе підробку листів від офіційних джерел або створення фальшивих веб-сайтів.
- **Соціальна інженерія в соціальних мережах**: Шахраї можуть використовувати соціальні мережі для створення фальшивих профілів або стеження за користувачами, щоб отримати особисту інформацію та використовувати її для маніпуляції.

- **Фізична соціальна інженерія**: Включає в себе фізичний доступ до приміщень або комп'ютерів, наприклад, шляхом обману або імперсонації.

Аналіз цих інструментів та методів допомагає розуміти, як шахраї використовують соціальні та психологічні техніки для досягнення своїх цілей. Для захисту від інтерактивної соціальної інженерії важливо бути уважним та обережним, а також розуміти, як розпізнавати потенційні загрози та реагувати на них.

2.3. Вибір методу рішення

Обираючи інтерактивну соціальну інженерію як метод для написання чат-боту з покращення рівня кібергігієни, існують кілька ключових причин. Інтерактивна соціальна інженерія використовує психологічні та соціальні методи для створення сценаріїв, які привертають увагу та викликають реакцію у людей, що допомагає зробити навчання цікавим та запам'ятовуючим. Ця методологія забезпечує активну взаємодію з користувачем та навчання практичним навичкам з кібергігієни, ставлячи їх у реальний контекст та допомагаючи користувачам зрозуміти, як захищати себе від потенційних загроз.

Також важливо врахувати, що інтерактивний чат-бот може легко адаптуватися до нових видів кіберзлочинності і методів атаки, постійно оновлюючись, додаючи нові сценарії та навчальні матеріали. Використання інтерактивної соціальної інженерії також допомагає користувачам розрізняти легітимні запити від підозрілих ситуацій та навчає їх реагувати розумно, що захищає від соціальних інженерів та фішингових атак. Нарешті, цей метод навчання можна використовувати для різних аудиторій, включаючи дітей, дорослих та старших груп населення, адаптуючи навчання до різних потреб та рівнів обізнаності.

Обираючи інтерактивну соціальну інженерію для написання чат-боту з покращення рівня кібергігієни, можна створити цікавий, практичний та

ефективний метод навчання, який допоможе користувачам краще розуміти і захищати себе в цифровому світі.

РОЗДІЛ 3
ДЕТАЛІ РОЗРОБКИ ІНТЕРАКТИВНОЇ СИСТЕМИ ТЕСТУВАННЯ

3.1. Реалізація функціоналу чат-боту

Чат-бот з покращення рівня кібергігієни, який використовує інтерактивну соціальну інженерію, має різноманітний функціонал, спрямований виявити слабкі місця у питаннях кібербезпеки користувача та підвищити рівень їх обізнаності щодо кібербезпеки.

Розглянемо ключові функції, які включає в себе чат-бот.

Чат-бот створює різні сценарії фішингових атак, які надсилає користувачам. Симульовані фішингові атаки є безпечними та нешкідливими. Чат-бот відстежує реакції користувачів на симульовані атаки. Коли користувач натрапляє на симуляцію фішингової атаки, чат-бот надає навчальні підказки, які допоможуть в подальшому розпізнавати спроби фішингових атак (рис. 3.1).

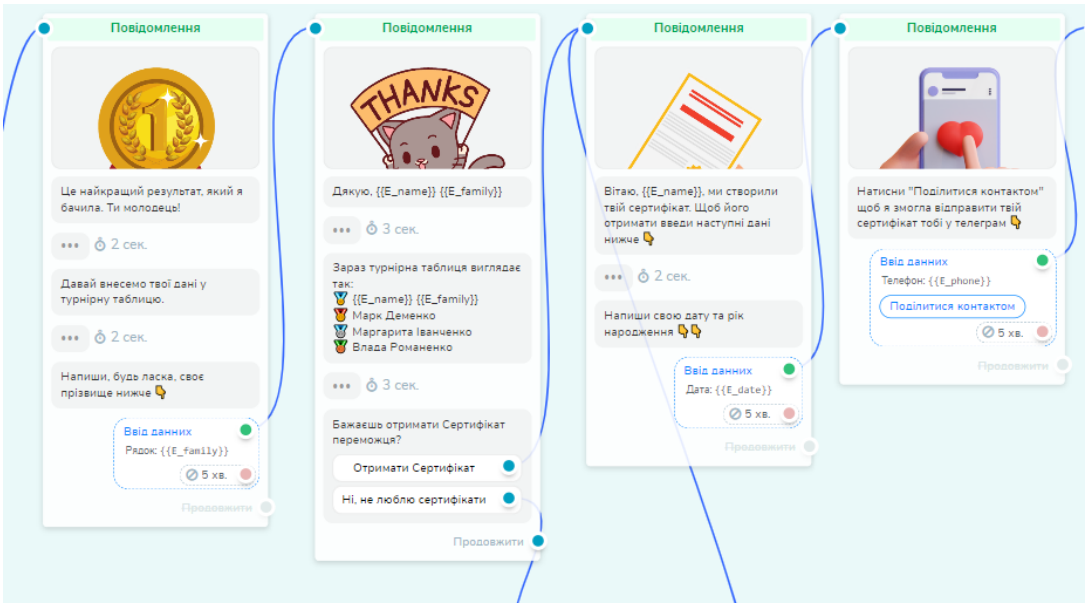

Рис. 3.1. Схема симуляції фішингових атак (рис. автора)

Інтерактивні ігри та вправи, які використовує чат-бот є різноманітними та захоплюючими. Вони призначені для закріплення у користувачів практичних навичок у сфері кібербезпеки та допомагають їм активно взаємодіяти зі інструментами чат-боту. Користувачам пропонується вікторина та різноманітні завдання, де вони відповідають на питання, пов'язані з кібербезпекою та виконують завдання зі створення віртуальної картки (рис. 3.2).

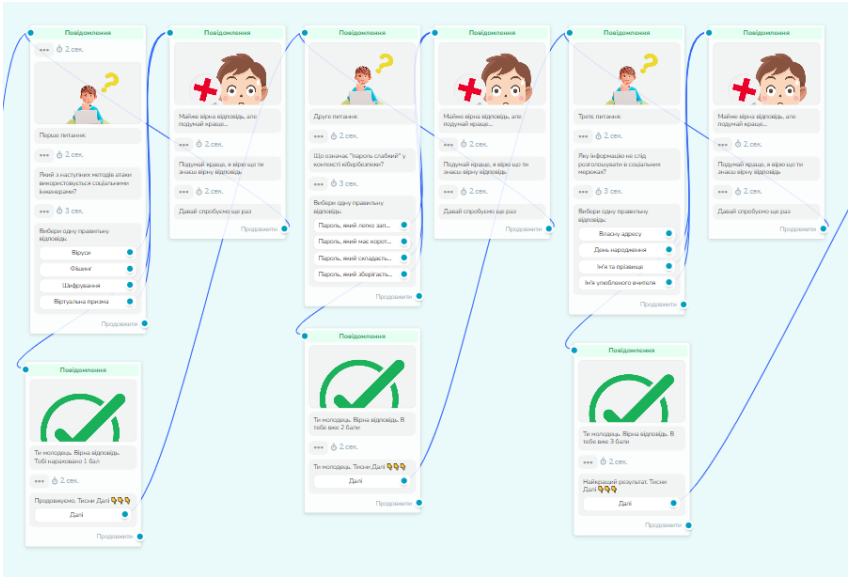

Рис. 3.2. Схема вікторини (рисунок автора)

Користувачі випробовують себе у симуляціях, де вони повинні захищати свою інформацію від злочинців. Це допомагає їм навчитися реагувати на загрози (рис. 3.3).

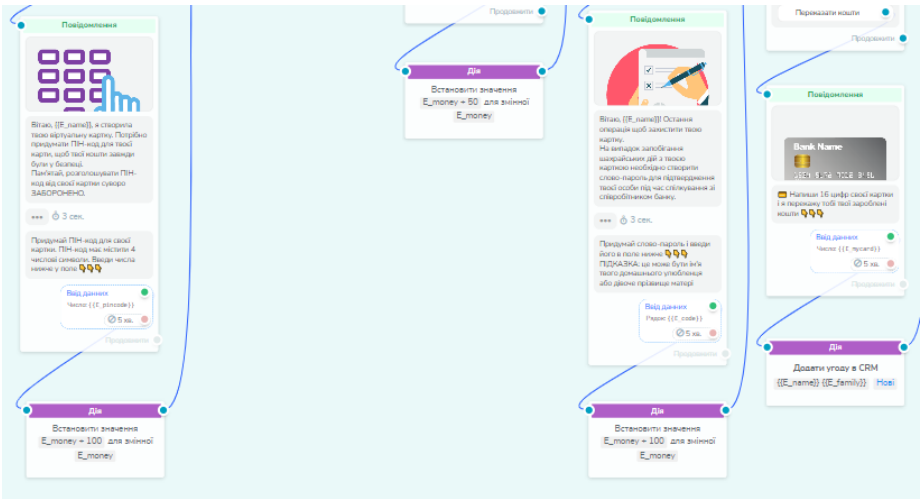

Рис. 3.3. Схема маніпуляції з конфіденційною інформацією користувача (рисунок автора)

Користувачі отримують негайний відгук за свій вибір та дії, що допомагає їм зрозуміти наслідки та вчитися зі своїх помилок (рис. 3.4).

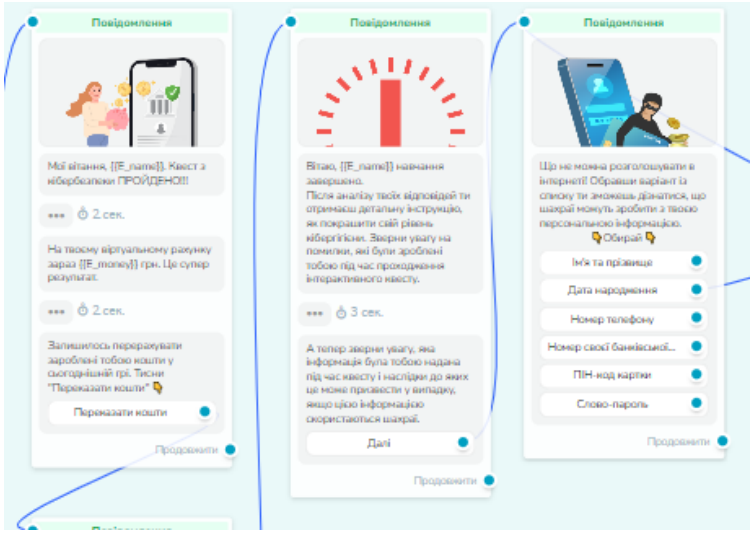

Рис. 3.4. Інструкція щодо виявлених загроз даних (рисунок автора)

Чат-бот створює ситуації, де користувачам потрібно вирішити, як вчинити в конкретній ситуації. Це допомагає вдосконалювати навички прийняття рішень в галузі кібербезпеки (рис. 3.5).

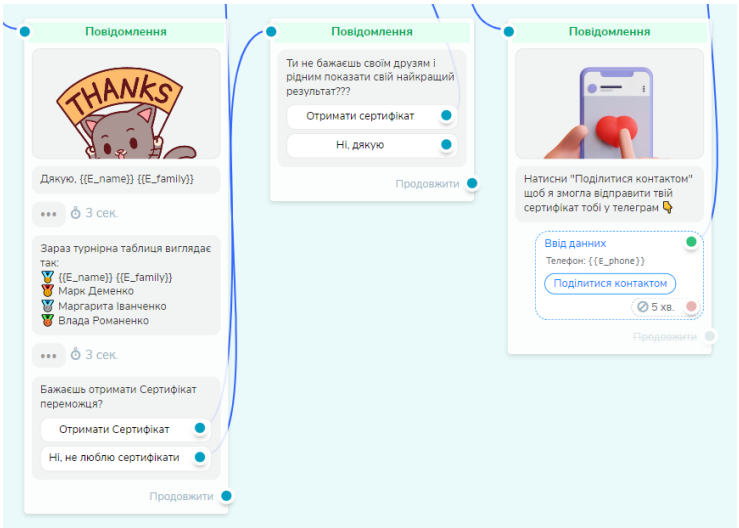

Рис. 3.5. Схема отримання телефонного номеру користувача (рисунок автора)

Чат-бот починає з простих завдань та поступово підвищує рівень складності, забезпечуючи належне навчання (рис. 3.6).

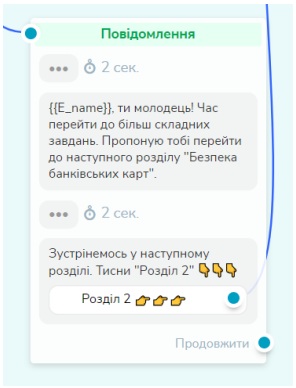

Рис.3.6. Підвищення рівня складності завдання (рисунок автора)

Симуляція обману та маніпуляції в чат-боті спрямовані на виявлення вміння користувачів розрізняти та захищатися від різних видів соціальної інженерії та маніпуляцій (рис. 3.7).

Рис. 3.7. Схема алгоритму заохочення користувача (рисунок автора)

Чат-бот надає користувачам можливість спробувати різні методи маніпуляцій, які можуть бути використані для отримання інформації чи дій від потенційної жертви. Це включає в себе психологічні прийоми, такі як виклик емоцій, створення азарту або використання авторитету (рис. 3.8).

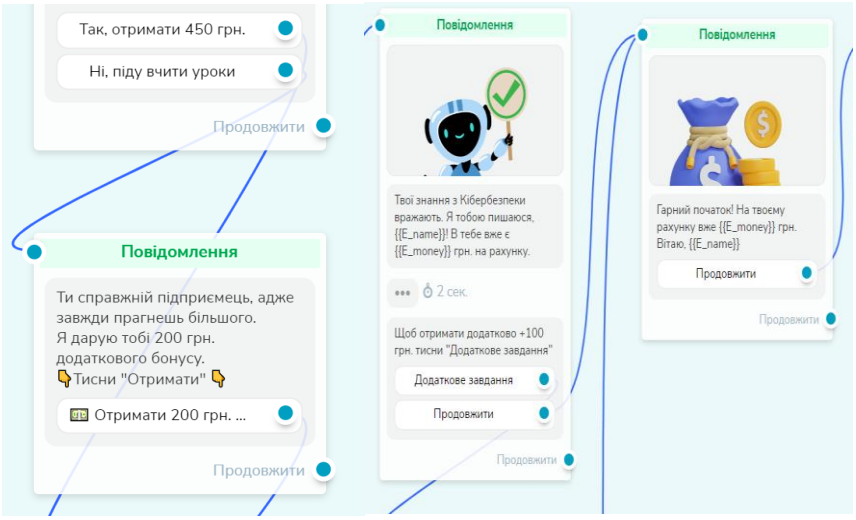

Рис. 3.8. Алгоритм підтримки азарту у користувача (рисунок автора)

Чат-бот збирає статистику щодо реакцій та відповідей користувачів на симульовані ситуації маніпуляцій та обману. Ця інформація використовується для створення звітів та оцінки рівня знань користувачів у питаннях своєї кібергігієни (рис. 3.9).

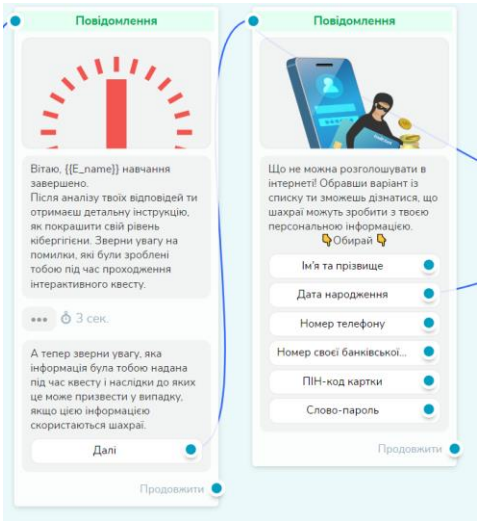

Рис. 3.9. Алгоритм створення зворотного зв’язку (рисунок автора)

3.2. Інтерфейс користувача

Інтерфейс користувача чат-боту відіграє важливу роль у забезпеченні зручності та ефективності тестування користувачів. Інтерфейс повинен бути інтуїтивно зрозумілим та забезпечувати доступ до різноманітних матеріалів й інтерактивних завдань.

Чат-бот зустрічає користувача приємним вітанням та пропонує обрати свого віртуального помічника. Вибір віртуального помічника різної статі відображає різні психологічні аспекти та індивідуальні уподобання, вибір статі віртуального помічника не обов'язково є унікальним для кожної дитини, але може бути дуже індивідуальним. Деякі діти можуть керуватися статевими стереотипами і обирати віртуального помічника, який відповідає традиційним уявленням про стать. Наприклад, хлопчики можуть більше симпатизувати віртуальним помічникам чоловічої статі, а дівчатка - жіночої.

Діти можуть розвивати емоційний зв'язок з віртуальним помічником, незалежно від статі, і вибирати помічника, з яким вони відчувають сильніше емоційне співпереживання (рис. 3.10).

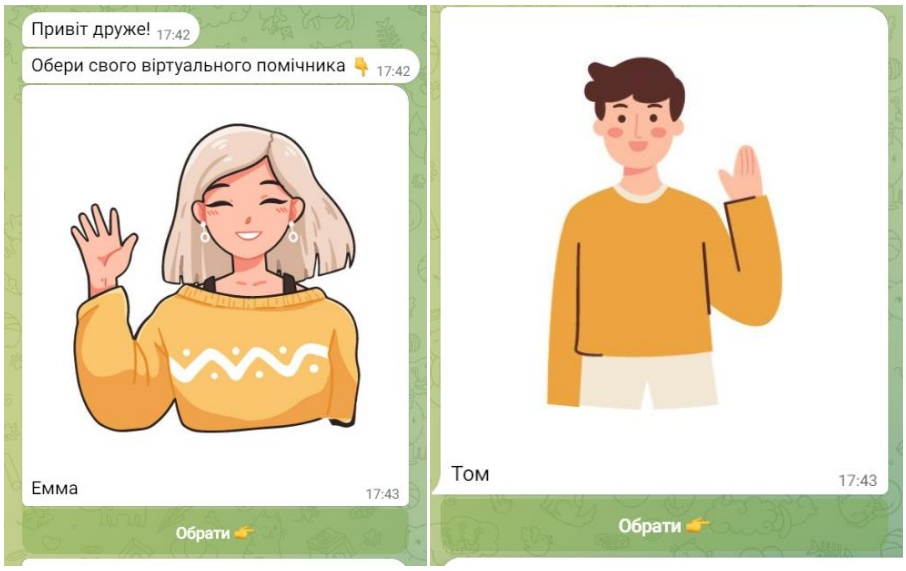

Рис. 3.10. Вибір статі віртуального помічника (рисунок автора)

Чат-бот надає користувачам інтерактивні завдання та питання, які вимагають відповідей. Завдання включають в себе вікторини, симуляції, рольові ігри та інші форми маніпуляцій (Рис. 3.11).

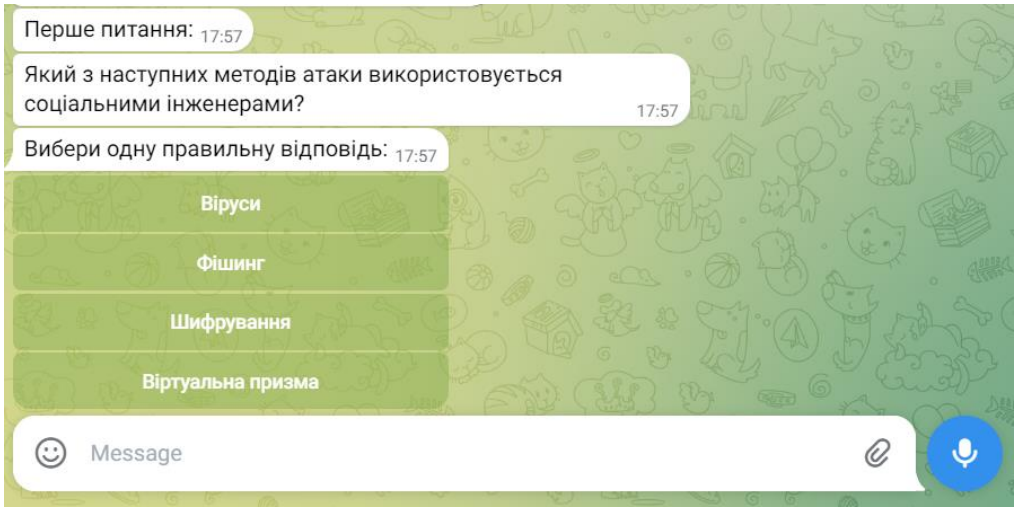

Рис. 3.11. Один з варіантів подання завдання вікторини (рисунок автора)

Чат-бот аналізує результати відповідей користувача та надає повідомлення про прогрес та рекомендації для подальших дій (Рис. 3.12).

Рис. 3.12. Один з варіантів заохочення продовжувати гру (рисунок автора)

Чат-бот надає симуляції реальних соціальних інженерних атак, щоб користувачі могли відчути загрозу та зрозуміти алгоритм розпізнання таких атак (рис. 3.13).

Рис. 3.13. Схема маніпуляції отримання номеру користувача (рисунок автора)

Чат-бот включає систему нагород та досягнень, які мотивують користувачів до активної взаємодії та розвитку (рис. 3.14).

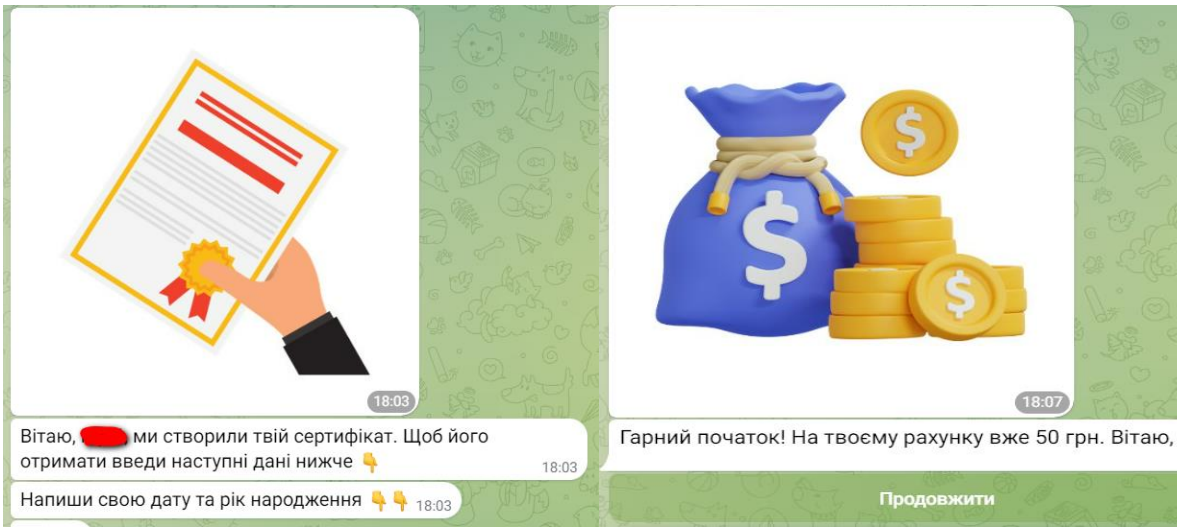

Рис. 3.14. Приклади нагород та заохочень (рисунок автора)

Інтерфейс повинен бути доступним для користувачів з різними рівнями технічної підготовки та відповідати їхнім потребам.

Чат-бот допомагає користувачам виявляти та розвивати навички захисту в інтернеті у зручному та інтерактивному форматі.

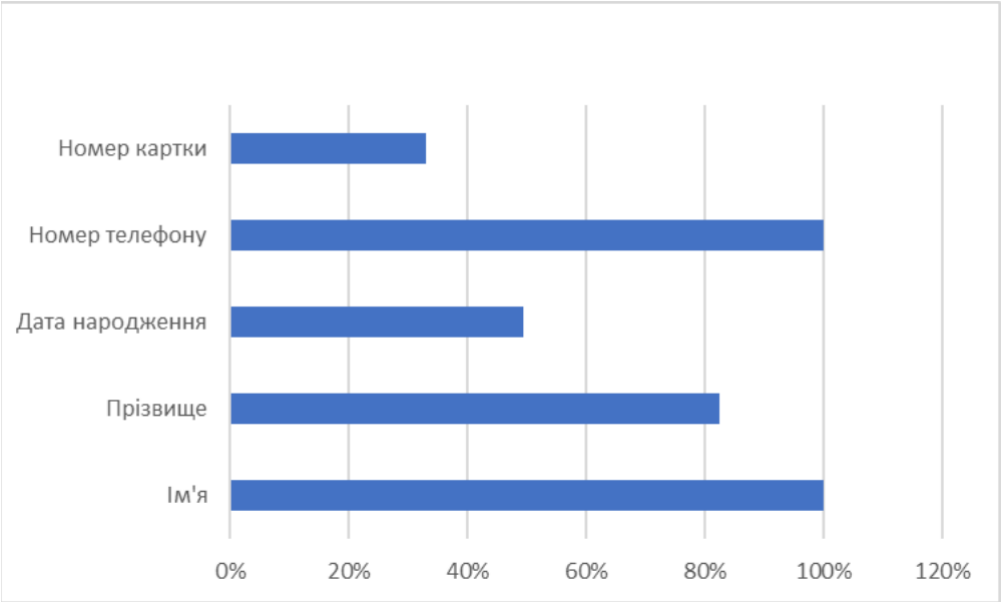

Рис. 3.15. Звіт щодо оцінки рівня знань користувачів у питаннях кібергігієни (рисунок автора)

Робота з чат-ботом серед користувачів показала, що інтерактивний підхід з використанням методів соціальної інженерії ефективно сприяє розвитку навичок розпізнавання та захисту від потенційних загроз у кіберпросторі. Ключові функції чат-бота, включаючи симуляції фішингових атак, інтерактивні ігри та вправи, а також модулювання різних сценаріїв, дозволяють користувачам на практиці випробувати свої знання та удосконалювати їх.

Завдяки аналізу реакцій користувачів на симульовані ситуації, чат-бот надає індивідуальні зворотні зв'язки та рекомендації, що допомагає підвищити рівень кібергігієни. Інтерфейс користувача розроблено таким чином, щоб бути інтуїтивно зрозумілим та зручним для користувачів різного віку та з різним рівнем технічної підготовки.

Кіберзагрози постійно еволюціонують, тому важливо систематично оновлювати свої знання у цій галузі. Використання навчальних ресурсів, таких як чат-боти, онлайн-курси, вебінари, може допомогти у цьому.

Інсталяція надійного антивірусного програмного забезпечення, файрволів, а також використання двофакторної аутентифікації для захисту акаунтів є критично важливою частиною забезпечення кібербезпеки.

Підвищення рівня обізнаності щодо кібергігієни вимагає комплексного підходу, що включає як самостійне навчання та регулярні практичні заняття, так і активну участь у спільноті фахівців та ентузіастів кібербезпеки. Розроблений чат-бот є важливим інструментом у цьому процесі, пропонуючи користувачам інтерактивний та ефективний спосіб навчання.

Переглянути робочу версію чат-бота і пройти тестування можна за посиланням у телеграм: https://t.me/lyceum4kh_bot

ВИСНОВКИ

У науковому дослідженні вивчено процес підвищення рівня кібергігієни молоді засобами інтерактивної соціальної інженерії.

Для досягнення поставленої мети, нами був вивчений матеріал з обраної теми, виконаний аналіз предметної області, на підставі якого розроблено чат-бот з покращення рівня кібергігієни з використанням прийомів інтерактивної соціально інженерії.

Перший розділ присвячений вивченню та аналізу поняття кібергігієна. Розкрито основні принципи кібергігієни та кібербезпеки.

У другому розділі розглянуто теоретичні аспекти застосування інтерактивної соціальної інженерії та проаналізовано інструменти і методи інтерактивної соціальної інженерії.

У третьому розділі розкрито деталі розробки інтерактивної системи тестування, у вигляді чат-боту телеграм. Розкрито якими методами і прийомами інтерактивної соціальної інженерії реалізовано функціонал чат-боту. Розглянуто основні елементи інтерфейсу користувача чат-боту та елементи взаємодії та маніпуляцій.

Таким чином, поставлена мета на початку роботи була досягнута, завдання реалізовані. Розроблений чат-бот з покращення рівня кібергігієни, з використанням методів інтерактивної соціальної інженерії дозволив виявити пробіли у знаннях та підвищити рівень кібергігієни користувачів, які приймали участь у тестуванні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в України// Підприємництво, господарство і право. – 2019. – № 9. – с.100 - 108
2. Кібергігієна. Кібербезпека. Безпека держави: Матеріали наукових семінарів. [Наукове електронне видання]. — Режим доступу: https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf
3. Кібергігієна. Кібербезпека. Безпека держави: матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ : Київ. нац. торг.-екон. ун-т, 2020. – 101 с.
4. Кібергігієна: для чого вона потрібна та які є методи боротьби із шахрайськими та пропагандистськими каналами [Електронний ресурс] – Режим доступу до ресурсу: https://bomok.com.ua/novyny/kibergigiyena-dlya-chodgo-vona-potribna-ta-yaki-ye-metody-borotby-iz-shahrajskymy-ta-propagandyskymy-kanalamy/
5. Кібергігієна: що це таке? [Електронний ресурс] – Режим доступу до ресурсу: http://uzinform.com.ua/news/2020/06/30/174433.html
6. Навчальний курс із основ кібергігієни “Базові правила безпеки в цифровому середовищі” [Електронний ресурс] – Режим доступу до ресурсу: https://cybereducation.org/mc/index.php/usr/login/login
7. Свердлик З. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. Український журнал з бібліотекознавства та інформаційних наук. – 2022. – №10. – с.175–188.
8. Gibson W. Neuromancer [Текст] / W. Gibson.— London: HarperCollins, 1994
9. Kevin D. Mitnick & William L. Simon The art of deception, 2011, 577 p.
10. Social Engineering: The Science of Human Hacking, 2018, 322 p.