УДК 004

Б. Андрусик, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ СКРЕМБЛЮВАННЯ ЦИФРОВОГО СИГНАЛУ НА МОБІЛЬНИХ ПРИСТРОЯХ

У статті розроблено програмне забезпечення, яке призначено для системи скремблювання цифрового сигналу на мобільних пристроях. Метою розробки є дослідження та принципи побудови системи скремблювання цифрового сигналу на мобільних пристроях. Об'єктом дослідження є процес скремблювання цифрового сигналу на мобільних пристроях. Предметом дослідження є методи скремблювання цифрового сигналу на мобільних пристроях. Методи дослідження базуються на методах теорії сигналів та теорії захисту інформації в мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи скремблювання цифрового сигналу на мобільних пристроях. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

скремблювання цифрового сигналу, мобільні пристрої

Постановка проблеми. Сучасному суспільству часом доводилося зіштовхуватися із проблемою прослуховування телефонних розмов. І цим нікого не здивуєш. В еру новітніх технологій ніколи не можна бути впевненим у повній конфіденційності чого-небудь. Зловмисники, намагаючись заволодіти анонімною інформацією, найчастіше підключаються до телефонних ліній як мобільних, так і стаціонарних телефонів, приносячись абонентам як стаціонарних, так і стільникових телефонів безліч проблем.

Скремблером називають пристрій, призначений для шифрування мови, що проходить через телефон, тим самим воно забезпечує захист і анонімність переговорів.

Шифрування відбувається за допомогою розбивки звукових сигналів на, так звані, під діапазони. Далі кожна частина піддається частотної інверсії, тобто перетворенню високих частот у низькі й навпаки. Поділ спектра на під діапазони відбувається на певній частоті, що називають крапкою розбивки. Крапка розбивки може бути фіксованою (під час розмови не виконується перемикання між режимами) або приймає одне з декількох можливих значень, коли під час телефонного переговору користувачі самі перемикаються між режимами скремблювання.

Процес розшифровки відбувається в тому випадку, якщо алгоритми скремблювання стоять на обох телефонах. Програми, працюючи одночасно, синхронно шифрують розмову. Таким чином, абоненти відмінно розуміють один одного, а зловмисники чують мову, що спотворюється повністю.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні скремблювання цифрового сигналу на мобільних пристроях.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи скремблювання цифрового сигналу на мобільних пристроях.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем скремблювання цифрового сигналу на мобільних пристроях.

– Дослідження системи скремблювання цифрового сигналу на мобільних пристроях.

– Програмна реалізація системи скремблювання цифрового сигналу на мобільних пристроях.

Об'єктом дослідження є процес скремблювання цифрового сигналу на мобільних пристроях.

Предметом дослідження є методи скремблювання цифрового сигналу на мобільних пристроях.

Методи дослідження базуються на методах теорії сигналів та теорії захисту інформації в мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У 2025 році ваш смартфон – це не просто засіб зв'язку, це портативне сховище, яке містить усе ваше цифрове існування. Від цінних спогадів та фінансових даних до конфіденційних робочих документів, ваш телефон – це центр вашого життя. Але наскільки безпечне це сховище?

В епоху постійно мінливих кіберзагроз та витончених фішингових шахрайств питання про те, як захистити свій телефон, ще ніколи не було таким критичним, особливо для новачків, які орієнтуються в цьому складному цифровому середовищі. Ви можете почуватися приголомшеними технічним жаргоном або не знати, з чого почати захист свого пристрою від сторонніх очей та зловмисників.

За межами екрана блокування: вичерпне визначення

Захист вашого телефону виходить за рамки простого блокування екрана. Він охоплює комплексний набір методів і технологій, розроблених для захисту вашого пристрою, даних, що зберігаються на ньому, та вашої особистої конфіденційності від несанкціонованого доступу, шкідливого програмного забезпечення та різних кіберзагроз.

По суті, захист телефону передбачає впровадження надійних заходів для захисту вашого цифрового життя, незалежно від того, чи використовуєте ви його для особистого спілкування, банківських операцій чи конфіденційних бізнес-операцій.

Такий багаторівневий підхід гарантує, що як апаратні, так і програмні компоненти вашого пристрою стійкі до потенційних вразливостей. Це забезпечує основу довіри у світі, що дедалі більше взаємопов'язаний. Зрештою, йдеться про створення цифрової фортеці навколо вашої найперсональнішої та найважливішої інформації, забезпечуючи її цілісність та конфіденційність.

Основні переваги та особливості мобільної безпеки

Переваги розуміння того, як захистити свій телефон, численні та критично важливі в сучасному цифровому середовищі. По-перше, це забезпечує першорядний захист від витоків даних та крадіжки особистих даних. Ваш телефон часто містить конфіденційну інформацію – контакти, фотографії, фінансові програми, електронні листи та особисті документи – які, якщо їх скомпрометувати, можуть призвести до серйозних особистих та фінансових наслідків.

По-друге, надійні заходи безпеки гарантують конфіденційність ваших повідомлень та особистих файлів. Це запобігає прослуховуванню або несанкціонованому доступу до ваших приватних розмов і документів. Це особливо важливо для фахівців, які працюють з конфіденційною інформацією, та для людей, які цінують свій особистий простір.

Чому це так важливо на сучасному ринку? Мобільні пристрої стали центральним центром нашого цифрового існування. Від керування розумними будинками до проведення фінансових транзакцій та доступу до робочих ресурсів, телефони постійно піддаються впливу кіберзагроз, що постійно змінюються. Добре захищений телефон пропонує душевний спокій, знаючи, що ваш цифровий слід захищений. Він також допомагає у дотриманні нормативних вимог для бізнесу, оскільки закони про захист даних дедалі більше вимагають безпечного поводження з особистою інформацією. Інвестування часу у вивчення того, як захистити свій телефон, більше не є необов'язковим; це фундаментальна необхідність для кожного, хто орієнтується в сучасному цифровому світі, захищаючись від постійних ризиків кіберзлочинності.

Галузеві стандарти мобільної безпеки

Перевірені стратегії безпеки телефонів узгоджуються з ширшими принципами кібербезпеки, підкреслюючи багаторівневий захист. Дотримання галузевих стандартів забезпечує надійну основу для захисту вашого пристрою:

– Надійна автентифікація: Завжди використовуйте складні паролі, відбитки пальців або розпізнавання обличчя. Уникайте легко вгадуваних шаблонів, простих PIN-кодів або паролів за замовчуванням.

– Регулярні оновлення програмного забезпечення: оновлюйте свою операційну систему (ОС) та всі програми. Ці оновлення часто містять критичні виправлення безпеки, які усувають нещодавно виявлені вразливості, захищаючи ваш пристрій від експлойтів.

– Керування дозволами програм: Будьте дуже вибірковими щодо дозволів, які ви надаєте програмам. Обмежте доступ до вашого місцезнаходження, камери, мікрофона та контактів, якщо це не є абсолютно необхідним для основної функції програми.

– Зашифрований зв'язок: для конфіденційних розмов та обміну даними використовуйте програми обміну повідомленнями з наскрізним шифруванням та безпечні служби електронної пошти.

– Безпечне використання Wi-Fi: Уникайте проведення конфіденційних транзакцій або доступу до особистих облікових записів у публічних мережах Wi-Fi без віртуальної приватної мережі (VPN). Публічні мережі часто не зашифровані та вразливі до прослуховування.

До поширених помилок, яких слід уникати, належать натискання на підозрілі посилання (спроби фішингу), повторне використання паролів у кількох онлайн-сервісах та нехтування регулярним резервним копіюванням даних вашого пристрою.

Рекомендації експертів щодо покращення безпеки телефону

Експерти з кібербезпеки постійно рекомендують конкретні, передові заходи для підвищення безпеки телефону та оптимізації вашого захисту:

– Розширений двоетапний вхід (2FA): Для всіх ваших облікових записів ми наполегливо рекомендуємо використовувати сучасні, безпечніші методи двоетапного входу (2FA), такі як Okta Verify, Google Authenticator або біометричні дані. Ці методи генерують коди, залежні від часу, або використовують унікальні фізичні атрибути, що значно знижує ризик несанкціонованого доступу, навіть якщо ваш пароль скомпрометовано.

– Поступова відмова від старих методів: Важливо зазначити, що традиційні методи 2FA, такі як SMS та голосові дзвінки, є застарілими методами та можуть бути недоступними в майбутньому через їхню схильність до атак заміни SIM-картки та інших вразливостей. Пріоритет багатофакторної автентифікації на основі додатків або біометричної багатофакторної автентифікації є ключовою порадою щодо оптимізації для кращої безпеки.

– Проактивне управління безпекою: Як наголошують експерти, «управління продуктами безпеки є важливим для забезпечення безпеки вашого веб-сайту від кіберзагроз», цей принцип поширюється безпосередньо на ваш мобільний пристрій. Проактивне та безперервне управління продуктами безпеки вашого телефону є життєво важливим. Це включає регулярний перегляд налаштувань безпеки вашого телефону, увімкнення функцій віддаленого стирання даних для втрачених або викрадених пристроїв та регулярне резервне копіювання даних у безпечне, зашифроване місце. Ці поради щодо оптимізації гарантують, що ваш телефон залишатиметься фортецею від постійно зростаючих кіберзагроз.

Професійні поради щодо безпеки мобільних пристроїв

Захист вашого телефону на розширеному рівні починається з фундаментальних професійних знань та надійних методів впровадження. Критичним аспектом є використання апаратного рівня безпеки, що включає безпечні процеси завантаження та апаратне шифрування. Це гарантує, що цілісність пристрою перевіряється з моменту запуску, а всі дані, що зберігаються на ньому, шифруються в стані спокою, що робить його недоступним без належної автентифікації.

Крім того, професійна безпека поширюється на всю екосистему зв'язку. Так само, як підприємства ретельно керують безпекою серверів, наприклад, вивчаючи «Як встановити SSL-сертифікати на серверах Zimbra» для забезпечення безпечної передачі даних, розширена безпека телефону вимагає наскрізного шифрування для всіх комунікацій – дзвінків, повідомлень та передачі даних. Це гарантує, що ваша особиста інформація залишається конфіденційною від вашого пристрою до одержувача і назад, захищаючи від прослуховування та перехоплення даних. Регулярні та своєчасні оновлення безпеки мають першочергове значення, виправляючи вразливості, перш ніж їх можна буде використати.

Розширені стратегії для забезпечення майбутнього вашого телефону

Виходячи за рамки базової безпеки, передові стратегії захисту вашого телефону передбачають проактивні заходи та врахування майбутніх факторів. Впровадження моделі безпеки з нульовою довірою для мобільних пристроїв є надзвичайно важливим; це означає, що жоден користувач чи пристрій не є довіреним за своєю суттю, незалежно від їхнього місцезнаходження, і кожен запит на доступ має бути автентифікований та авторизований. Такий підхід значно зменшує поверхню для атаки.

Ще один передовий метод передбачає розгортання складних механізмів виявлення загроз. Це включає виявлення аномалій на основі штучного інтелекту, яке може виявляти незвичайні моделі поведінки, що вказують на шкідливе програмне забезпечення або вторгнення, а також моніторинг шкідливих програм у режимі реального часу. Заглядаючи в майбутнє, майбутні міркування щодо безпеки телефонів все частіше включатимуть квантово-стійку криптографію для захисту від потенційних можливостей розшифрування майбутніх квантових комп'ютерів, забезпечуючи довгострокову конфіденційність даних. Ці стратегії професійного рівня є важливими для підтримки найвищого рівня цифрового захисту від кіберзагроз, що розвиваються.

Оцінка ризиків та вразливостей безпеки мобільних пристроїв

Перш ніж запроваджувати конкретні заходи, важливо зрозуміти, як кібербезпека та мобільні пристрої впливають на діяльність компанії. Підприємства повинні виявляти потенційні загрози безпеці мобільних пристроїв та оцінювати поточні вразливості, щоб краще зрозуміти наслідки порушення безпеки та як відповідно реагувати у разі порушення.

Організації можуть розробляти індивідуальні стратегії безпеки, що відповідають унікальним викликам та потребам, шляхом проведення оцінки ризиків.

Зокрема, зростання занепокоєння щодо безпеки даних та шифрування пов'язане з кількома тенденціями:

– З розвитком програмного забезпечення для генеративного штучного інтелекту (ГШІ), зловмисники вже створили складніші форми кібератак.

– Оскільки все більше компаній переходять на віддалені та гібридні моделі роботи, злочинці націлюються на пристрої, що належать компанії, або особисті пристрої поза межами захищених корпоративних мереж.

– Зростаюча нестача фахівців з кібербезпеки також вплинула на здатність компаній захищати інформацію.

Основні стратегії безпеки мобільних пристроїв

Надійна стратегія мобільної безпеки повинна включати технічні засоби контролю, політики безпеки та програми підвищення обізнаності користувачів. Впровадження методів шифрування, забезпечення багатофакторної автентифікації та реалізація можливостей віддаленого стирання допомагають зменшити ризик втрати даних.

Найкращі рекомендації щодо безпеки мобільних пристроїв

1. Впроваджуйте політику нульової довіри

– Вимагати від користувачів встановлення унікальних надійних паролів.

– Відмовляйте співробітників від поширення паролів.

– Заохочуйте використання багатофакторної автентифікації або біометричних методів.

– Не радите натискати на посилання від незнайомих відправників та не завантажувати програмне забезпечення з незнайомих джерел.

– Уникайте обміну особистою інформацією з неперевіреними веб-сайтами або особами.

2. Шифруйте мобільні дані для запобігання витокам даних

– Шифруйте дані, що зберігаються на мобільних пристроях, зокрема шифруйте дані мобільних додатків, щоб захистити їх від несанкціонованого доступу у разі втрати або крадіжки.

– Використовуйте симетричні або асиметричні методи шифрування для підвищення безпеки.

3. Оновіть мобільну ОС та програми, щоб виправити вразливості безпеки

– Оновлюйте мобільні операційні системи та програми, щоб виправляти вразливості та запобігати атакам.

– Плануйте регулярні аудити, щоб забезпечити регулярні оновлення на всіх пристроях.

4. Посилення безпеки мобільних пристроїв за допомогою політик управління

– Впроваджуйте політики для забезпечення налаштувань безпеки, таких як захист паролем і шифрування.

– Забезпечити дотримання керівниками політики.

5. Захистіть мобільні з'єднання за допомогою безпечних віртуальних приватних мереж (VPN)

– Зменште ризики злому мобільних мереж, зобов'язавши використовувати VPN під час доступу до конфіденційної інформації або підключення до загальнодоступних мереж Wi-Fi. Загальнодоступні мережі Wi-Fi є небезпечними та часто стають мішенню злочинців.

– Мінімізуйте використання публічного Wi-Fi для віддаленої роботи.

6. Увімкніть функції віддаленого стирання та блокування для втрачених пристроїв

– Активуйте функції віддаленого стирання та блокування на пристроях, що належать компанії.

– Дозвольте IT-командам дистанційно видаляти дані та запобігати несанкціонованому доступу у разі крадіжки або втрати пристрою.

7. Моніторинг активності мобільних пристроїв для виявлення кіберзагроз

– Регулярно контролюйте та перевіряйте активність пристроїв, щоб виявляти підозрілу поведінку або несанкціонований доступ.

– Усувайте вразливості за допомогою проактивних заходів, таких як оцінка вразливостей та тестування на проникнення.

8. Контролюйте використання мобільних додатків для зменшення ризиків безпеки

– Контролюйте встановлення та використання програм.

9. Створіть резервні копії мобільних даних, щоб запобігти їх втраті через шкідливе програмне забезпечення або збій пристрою

– Заохочуйте регулярне резервне копіювання даних, щоб запобігти втраті у разі пошкодження або збою пристрою.

– Автоматизуйте резервне копіювання за допомогою хмарних платформ для безперебійного захисту даних.

10. Захист мобільних пристроїв за допомогою програмного забезпечення MDM/EMM

– Використовуйте програмне забезпечення для керування мобільними пристроями або корпоративного управління мобільністю для віддаленого керування пристроями та їх захисту.

– Отримуйте аналітику бізнес-операцій та забезпечуйте дотримання політик на всіх пристроях.

11. Навчіть співробітників передовим практикам безпеки мобільних пристроїв та кіберзагрозам

– Забезпечувати постійне навчання щодо найкращих практик безпеки мобільних пристроїв та важливості захисту даних.

– Запропонуйте довідковий контекст щодо нових правил та проілюструйте реальними прикладами кіберзлочинності.

– Заохочуйте участь співробітників та зміну їхньої поведінки за допомогою ефективних ініціатив у сфері лідерства та навчання.

Захист інтересів співробітників: як навчання знижує ризики мобільної безпеки

Окрім технічних заходів безпеки, організації повинні зосередитися на навчанні співробітників передовим практикам кібербезпеки.

Сприяючи розвитку культури обізнаності та відповідальності, компанії можуть надати співробітникам можливість відігравати активну роль у захисті своїх мобільних пристроїв і даних. Регулярні аудити можуть допомогти виявити проблеми відповідності та забезпечити дотримання заходів безпеки.

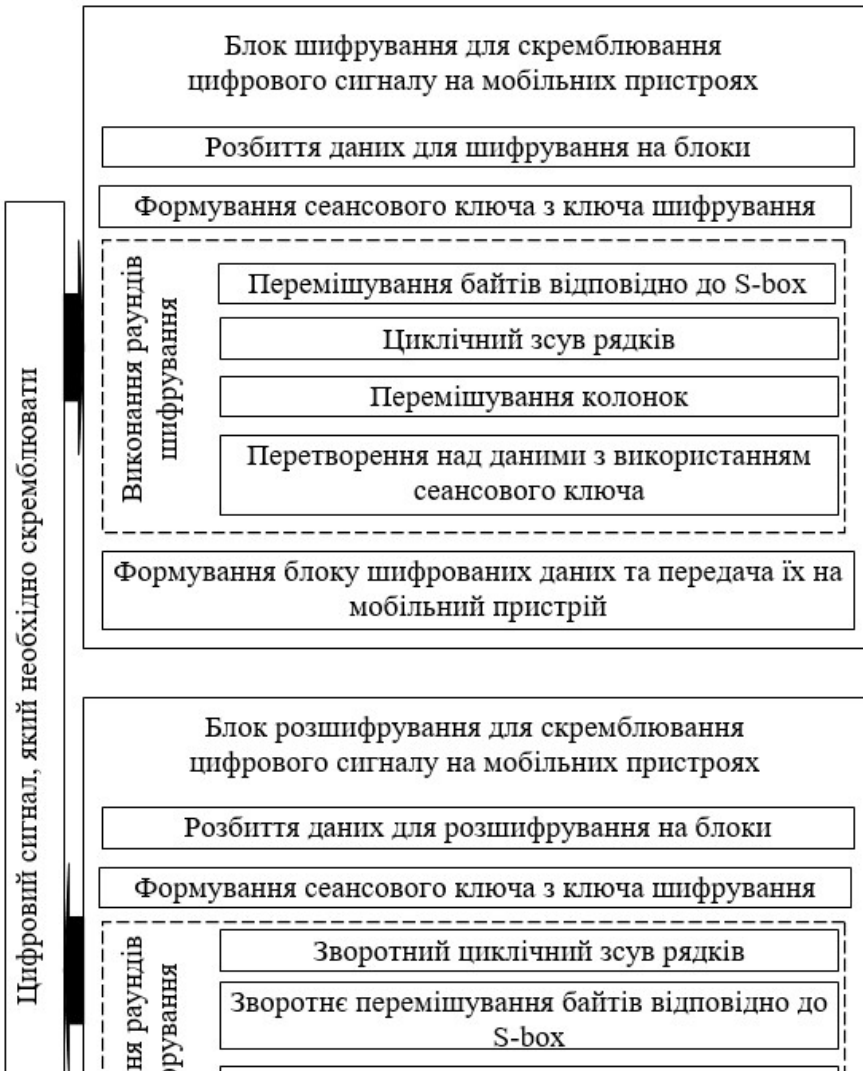

Рисунок 1 – Структурна схема системи

У даній роботі, для системи скремблювання цифрового сигналу на мобільних пристроях використовується алгоритм AES.

Структурна схема наведена на рисунку 1. З неї ми бачимо, що розроблена система складається з наступних структурних блоків.

– Дані, які передаються між мобільними пристроями.

– Блок шифрування за допомогою алгоритму AES для скремблювання цифрового сигналу на мобільних пристроях.

– Блок розшифрування за допомогою алгоритму AES для скремблювання цифрового сигналу на мобільних пристроях.

– Мобільний пристрій, на який надходять зашифровані сигнали.

Основним блок системи є блок шифрування AES.

Випереджайте кіберзагрози за допомогою безпеки мобільних пристроїв

Зі зміною ландшафту загроз, актуальні заходи безпеки є надзвичайно важливими. Це включає регулярний перегляд та оновлення політик безпеки, інформування про нові загрози та відповідну адаптацію стратегій безпеки.

ІТ-менеджерам слід підписатися на розсилку новин про безпеку мобільних пристроїв та заохочувати всіх співробітників ділитися будь-якими відповідними новинами щодо пристроїв або програмних послуг, які вони використовують.

Проактивні заходи для безпеки мобільних пристроїв

Ефективна безпека мобільних пристроїв вимагає постійного моніторингу та швидкого реагування на інциденти безпеки. Аналіз після інциденту має вирішальне значення для навчання та вдосконалення в майбутньому.

Програмне забезпечення для управління корпоративною мобільністю надає важливі дані бізнес-аналітики для підтримки надійної стратегії безпеки пристроїв. Крім того, організаціям слід дотримуватися наведених вище найкращих практик безпеки мобільних пристроїв для захисту конфіденційних даних, зменшення ризиків та захисту від потенційних загроз.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів скремблювання цифрового сигналу на мобільних пристроях. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем скремблювання цифрового сигналу на мобільних пристроях.

– Досліджена система скремблювання цифрового сигналу на мобільних пристроях.

– На основі отриманих результатів досліджень створена програмна реалізація системи скремблювання цифрового сигналу на мобільних пристроях. Розроблені алгоритми дозволяють успішно вирішувати завдання скремблювання цифрового сигналу на мобільних пристроях. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». Cybersecurity Defensive Walls in Edge Computing, 2025. pp. 21-61.
2. Chulinda L., Smirnov O., Shapenko L., Ustynova I., Bohatiuk I., Kelyp S. «The role of innovation in ensuring the safety of international civil aviation». Ceur Workshop Proceedings, 2025, 4024, pp. 530–542.
3. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А, Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.
4. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». Кібербезпека: освіта, наука, техніка. 2025. Том 1 № 29. С.704–716, 2025
5. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
6. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
7. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT

networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
8. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
9. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
10. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
11. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
12. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
13. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
14. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
15. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
16. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
17. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
18. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56
19. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
20. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
21. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
22. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
23. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи hозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
24. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
25. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
26. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 2(72), С. 170-178.
27. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data

Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
28. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
29. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
30. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
31. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
32. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.