УДК 004

І.Кіблик, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ТА АУДИТУ ДІЙ ПРИ РОБОТІ З МЕРЕЖЕВОЮ БАЗОЮ ДАНИХ

У статті розроблено програмне забезпечення, яке призначено для системи контролю доступу та аудиту дій при роботі з мережевою базою даних. Метою розробки є дослідження та принципи побудови системи контролю доступу та аудиту дій при роботі з мережевою базою даних. Об'єктом дослідження є процес контролю доступу та аудиту дій при роботі з мережевою базою даних. Предметом дослідження є методи контролю доступу та аудиту дій при роботі з мережевою базою даних. Методи дослідження базуються на методах побудови баз даних та захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи контролю доступу та аудиту дій при роботі з мережевою базою даних. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

система контролю доступу, аудит дій, мережева база даних

Постановка проблеми. Контроль доступу до бази даних, або контроль доступу до БД – це метод, що дозволяє доступ до конфіденційної інформації компанії лише групам користувачів, яким дозволено доступ до таких даних, та обмежує доступ неавторизованим особам для запобігання витокам даних у системах баз даних. Контроль доступу до бази даних у СУБД включає два основні компоненти: автентифікацію та авторизацію.

Автентифікація – це спосіб підтвердження особи особи під час доступу до вашої бази даних. Важливо пам'ятати, що автентифікації користувача недостатньо для забезпечення безпеки даних. Авторизація, яка встановлює, чи є рівень доступу користувача або контроль доступу до даних відповідним, є додатковим рівнем захисту. Зрештою, без автентифікації та авторизації немає безпеки даних.

Кожна компанія сьогодні, у якої є співробітники, що взаємодіють з даними, а отже, кожна організація, повинна встановити контроль доступу до даних.

Після того, як ми розглянули питання «Що таке контроль доступу?», важливо зазначити, що ці засоби контролю впроваджуються для захисту ресурсів від несанкціонованого, незаконного доступу та забезпечення того, щоб суб'єкти могли отримувати доступ до об'єктів лише за допомогою безпечних, попередньо затверджених процедур.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи контролю доступу та аудиту дій при роботі з мережевою базою даних.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи контролю доступу та аудиту дій при роботі з мережевою базою даних. Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем контролю доступу та аудиту дій при роботі з мережевою базою даних.

– Дослідження системи контролю доступу та аудиту дій при роботі з мережевою базою даних.

– Програмна реалізація системи контролю доступу та аудиту дій при роботі з мережевою базою даних.

Об'єктом дослідження є процес контролю доступу та аудиту дій при роботі з мережевою базою даних.

Предметом дослідження є методи контролю доступу та аудиту дій при роботі з мережевою базою даних.

Методи дослідження базуються на методах побудови баз даних та захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Найвідоміші приклади контролю доступу до бази даних включають:

– Дискреційний контроль доступу (DAC). Власник даних надає доступ до моделей DAC. DAC – це метод призначення прав доступу на основі правил, визначених користувачем.

– Обов'язковий контроль доступу (MAC). У MAC людям дозволено доступ на основі дозволу на доступ до інформації, розробленого з використанням недискреційної парадигми. MAC позначає політику, яка призначає дозволи доступу на основі правил центрального органу влади.

– Контроль доступу на основі ролей (RBAC). RBAC використовує фундаментальні принципи безпеки, такі як «мінімальні привілеї» та «розділення привілеїв», щоб надавати доступ залежно від ролі користувача. Як результат, той, хто хоче отримати доступ до інформації, може отримати доступ лише до даних, необхідних для виконання його функції.

– Контроль доступу на основі атрибутів (ABAC). Кожен ресурс і користувач в ABAC отримує набір атрибутів. Цей динамічний підхід визначає доступ до ресурсів на основі порівняння характеристик користувача, таких як час доби, місцезнаходження та місцезнаходження.

Як працюють системи контролю доступу до баз даних

Системи контролю доступу до баз даних працюють з трьох сторін: користувача, адміністратора та інфраструктури:

– Користувач: Коли співробітник бажає увійти до зони обмеженого доступу, він повинен надати свої облікові дані. Запит на розблокування подається на зчитувач карток, який надсилає інформацію до блоку контролю доступу, що згодом авторизує користувача та відкриває двері.

– Адміністратор: Система контролю доступу має панель керування або портал на адміністративній стороні. Адміністратори офісу, IT-менеджери та керівники служби безпеки можуть використовувати портал керування, щоб вказати, хто має доступ до приміщення та за яких умов.

– Системна інфраструктура: Інфраструктура системи контролю доступу включає електричні замки, зчитувачі карт, стан дверей для моніторингу руху та пристрої запитів на вихід, всі з яких повідомляють на панель керування та сервер.

Ось деякі з найкращих практик використання системи контролю доступу до бази даних:

– Зосередьтеся на доступі до конфіденційних даних. Однією з реалій управління великою компанією є збір величезних обсягів конфіденційних даних, які потім зберігаються та обробляються в базах даних. Як наслідок, бази даних є поширеною мішенню для кібератак. Як наслідок, критично важливо зосередитися на безпеці даних. Почніть із запиту до вашого IT-відділу про створення базового плану поточних рівнів доступу та політик. Завдяки цьому ви зможете виявити недоліки у ваших існуючих процесах та викрити будь-яких серйозних порушників, таких як той, хто керує бізнесом зі свого робочого місця.

– Шифрування даних. Дані під час передачі або дані в русі активно переміщуються з однієї області в іншу, наприклад, через Інтернет або приватну мережу. З іншого боку, дані в стані спокою – це інформація, яка не переміщується активно з одного пристрою на інший або

з однієї мережі в іншу, наприклад, інформація, що зберігається на жорсткому диску, ноутбуці, флеш-накопичувачі, або архівована чи збережена іншим способом. Сучасні підприємства повинні захищати конфіденційні дані як під час передачі, так і в стані спокою, оскільки кіберзлочинці розробляють нові способи компрометації систем та крадіжки даних. Шифрування є популярним інструментом для захисту даних під час передачі та в стані спокою, і воно відіграє важливу роль у захисті даних.

– Освіта для всіх зацікавлених сторін даних. Це може здатися несподіванкою, але співробітники організації несуть найбільші ризики для її кібербезпеки. Хоча співробітники компанії є найбільшими носіями ризиків, вони також мають найбільшу користь для кібербезпеки організації. Завдяки постійній освіті та комплексній програмі навчання з безпеки, співробітники можуть забезпечити додаткову безпеку, виступаючи в ролі ще одного рівня захисту.

– Застосовуйте доктрину найменших привілеїв. Гарною відправною точкою для встановлення контролю доступу є використання Доктрини найменших привілеїв, яка по суті базується на принципі, що людина не повинна мати доступу до чогось, якщо їй не потрібно з цим працювати.

– Аудит та моніторинг. Аудит та моніторинг – це гарні заходи для забезпечення безпеки контролю доступу до бази даних. Оскільки співробітники більш схильні перевіряти обмеження доступу, коли ніхто не спостерігає, компанії можуть нагадувати своїм співробітникам, що їхня діяльність з доступу до даних контролюється.

Можливі ризики й приклади реальних інцидентів

До баз даних постійно прикута пильна увага зловмисників, як внутрішніх, так і зовнішніх. Щодня в українських компаніях відбувається безліч інцидентів порушення політик безпеки.

Приклад атаки зсередини

Адміністратор безпеки у фінансовій організації, використовуючи свої права, здійснював переміщення коштів між рахунками. Операція виконувалася в самій базі даних, при цьому журнал реєстрації дій відключався, або вироблялося його чищення.

Приклад атаки ззовні

Дані при їхній передачі між підрозділами компанії не захищалися за допомогою криптографії, залишаючи можливість їхнього прослуховування й зняття копії з мережного встаткування.

Безпечне конфігурування

Створення автоматизованого середовища забезпечення безпечної роботи з базами даних повинне містити в собі: виявлення баз даних, сканування по профілях безпеки, фіксація конфігурацій і т.п.

Навіть у випадку якщо база даних пройшла процедуру настроювання параметрів безпеки, це не виключає постійного контролю її стану, через те, що користувачі своїми діями можуть знижувати захищеність, неусвідомлено відкриваючи можливості для проникнення зловмисника й експлуатації уразливостей.

Технічні засоби забезпечення безпеки баз даних

Забезпечення безпеки Web-додатків

Через те що Web-додатки є невід'ємною частиною практично будь-якої бази даних, заходи, спрямовані на їхній захист, дозволяють за порівняно короткий строк, без впливу на сам процес роботи з базами даних, підвищити їхня захищеність від проникнень із зовнішнього середовища.

Можливості дозволяють реалізувати практично будь-яку конфігурацію, у тому числі й для високонавантажених систем.

Фізичний поділ компонентів БД, контроль доступу на мережному рівні

Поділ компонентів баз даних на мережному рівні повинне вироблятися за допомогою міжмережевих екранів, що забезпечують контроль доступу з перевіркою стану сесії й бажано з перевіркою користувачів по їх обліковим даним (інтеграція з LDAP, Active Directory та ін.).

Крім реалізації функцій поділу, бажано щоб міжмережевий екран мав функціонала виявлення й запобігання вторгнень.

Наявність наочних засобів адміністрування й візуалізації подій у міжмережевих екранах, є безсумнівним плюсом через прямий вплив на операційні витрати, пов'язані з розслідуванням інцидентів. Як можливі варіанти для рішення даного завдання є продукти компанії Check Point Software Technologies, PaloAlto Networks, Cisco Systems, Інфотекс, Код Безпеки й т.п.

Контроль доступу й аудит дій користувачів і адміністраторів

Реалізація функцій по контролі доступу, поділу прав, і виконанню аудита всіх дій, може бути виконана убудованими засобами БД. Однак, слід зазначити, що включення функцій по убудованому аудиті, як того вимагають завдання по забезпеченню безпеки (тобто не тільки базовий набір команд), приводить до зростання навантаження на апаратні ресурси від 10 до 30% залежно від бази даних, що у свою чергу тягне неефективну розтрату дорогих апаратних ресурсів. Реалізація функцій аудита убудованими засобами БД, у кожному разі залишає можливість адміністраторові відключити цього аудита.

У зв'язку із цим найбільш раціональним шляхом є винесення завдань по аудиті на зовнішню систему, що забезпечує запис всіх дій, виконуваних у БД користувачами й адміністраторами.

У загальному виді, рішення зможе складатися з декількох компонентів різних функцій, що забезпечують реалізацію, зокрема:

Сервер керування – для керування й збору даних із всіх компонентів рішення;

Шлюз – який реалізує функції розмежування доступу й аудита для мережних обігів;

Агент – який реалізує функції розмежування доступу й аудита для операцій, виконуваних безпосередньо із БД (даний спосіб роботи повинен бути максимально обмежений).

Звичайний міжмережевий екран не дозволяє працювати з даними на рівні sql – запитів, розбираючи їх і вишиковуючи для них профіль захисту.

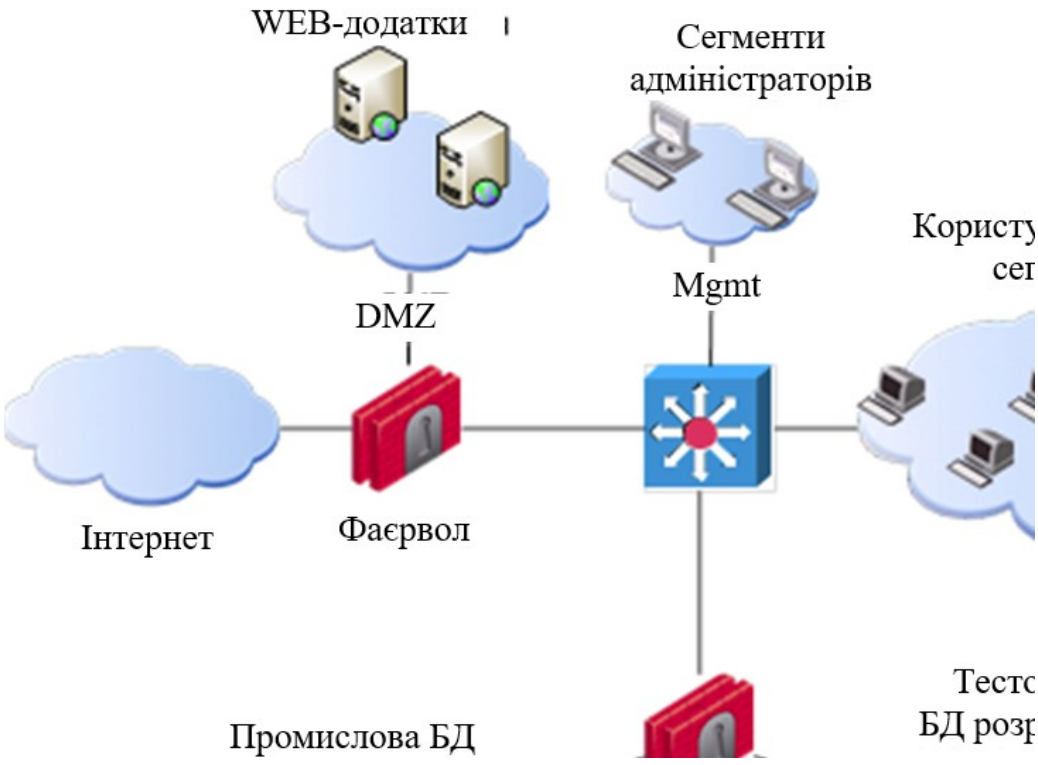

Рисунок 1 – Структурна схема системи

Поділ компонентів

Поділ бази даних на середовища розробки, тестування й промислове середовище, є обов'язковою вимогою й невід'ємною частиною всіх рекомендацій з безпеки. Однак це, у свою чергу народжує проблеми своєчасного одержання відновлень, даних із промислового середовища в тестову й розробки, швидкого відновлення й обслуговування декількох копій середовища розробки й тестування (через те, що ті самі відновлення можуть перевірятися як одночасно різними співробітниками й розроблювачами, так і для різних станів однієї й тої ж бази даних). Таким чином, швидке перенесення даних з одного середовища в іншу, відновлення копій баз даних і їхнє адміністрування починає істотно впливати на операційні витрати.

Вирішити дані проблеми можна за допомогою розробленої програми, що також дозволяє паралельно вирішити завдання маскування даних у середовищі тестування й розробки.

Розроблена програма дозволяє віртуалізувати базу даних, швидко й ефективно працювати з копіями баз даних і інформацією в ній (відновлюючи/відкочуючи/видаляючи дані й стан бази даних на бажаний момент часу), а також забезпечити зміна даних стерпних із промислової бази даних у середовища розробки й тестування виконавши тим самим їх маскування.

Немаловажним завданням є перевірка встановлюваних на базу даних і її компоненти відновлень ПЗ. Необхідність постійного відновлення баз даних і її компонент із однієї сторони може бути викликана вимогами бізнесу (по додаванню нового функціонала), а з іншої сторони вимогами безпеки (усунення виявлених уразливостей). Вирішити дане завдання в тому числі можливо шляхом відпрацьовування змін на віртуальних копіях бази даних.

Аналіз захищеності

Постійний контроль за змінами, що відбуваються з базами даних і їхніх компонентів, аналіз їхньої захищеності й схильності уразливостям повинен бути виділений в окремий процес, здійснюваний адміністраторами компанії, адміністраторами баз даних і розроблювачами. Для виявлення й аналізу уразливостей у базах даних варто використовувати сканери безпеки, при цьому їхнє застосування повинне виконуватися в строго погоджені технологічні “вікна” с дотриманням вимог по попередньому резервуванню поточних конфігурацій у базі даних. Сканування за допомогою технічного інструментарію повинне виконуватися по заздалегідь підготовлених профілях сканування актуальним для виконуваного завдання. Результати сканування повинні розбиратися й інтерпретуватися відповідними фахівцями, щоб з однієї сторони максимально точно настроїти профіль сканування, а з інший чітко позначити виявлені недоліки в конфігураціях баз даних, уразливості й відсутні відновлення.

Результатом проведеної роботи повинне з'явитися підтримка незмінності настроювань безпеки в базах даних і її компонентів, виявлення відхилень від затверджених профілів безпеки й своєчасне усунення що виявляються уразливостей шляхом відновлення відповідних компонентів.

Виявлення відхилень у поводженні користувачів/адміністраторів

Рішення, що аналізують профіль поводження користувачів і адміністраторів, дозволяють у тому числі ефективно боротися із шахрайськими діями зловмисників навіть у тому випадку, якщо в них за якимись причинами виявилися легітимні облікові записи. Як подібні рішення можуть застосовуватися системи UBA (User Behavioral Analysis), принцип роботи яких будуватися на підставі складання профілю поводження для кожного контрольованого суб'єкта при його операціях з об'єктами доступу. При цьому варто враховувати факти спрацьовування подібних систем у випадках появи додаткових повноважень у суб'єктів доступу, зміни їхніх прав і додавання нових об'єктів з якими здійснюється робота. Через вищесказаний найбільш доцільним є застосування систем UBA у

зв'язуванні з іншими системами, що фіксують правомірність зміни прав суб'єктів доступу, створення нових об'єктів доступу й т.п.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів контролю доступу та аудиту дій при роботі з мережевою базою даних. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем контролю доступу та аудиту дій при роботі з мережевою базою даних.

– Досліджена система контролю доступу та аудиту дій при роботі з мережевою базою даних.

– На основі отриманих результатів досліджень створена програмна реалізація системи контролю доступу та аудиту дій при роботі з мережевою базою даних.

Розроблені алгоритми дозволяють успішно вирішувати завдання контролю доступу та аудиту дій при роботі з мережевою базою даних. 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. 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.
2. 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.
3. 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.
4. 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.
5. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
6. 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
7. 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.
8. 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.
9. 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.
10. 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.
11. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». ІІ 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.
12. 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.
13. 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.

14. 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.
15. 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,
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
22. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
23. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.
24. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58.
25. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
26. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
27. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
28. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131.
29. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
30. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84.
31. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.