УДК 004

Р.Слабінога, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО МОНІТОРИНГУ ТА ЗАПОБІГАННЯ АКТИВНОСТІ ДОДАТКІВ

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуального моніторингу та запобігання активності додатків. Метою розробки є дослідження та принципи побудови системи інтелектуального моніторингу та запобігання активності додатків. Об’єктом дослідження є процес інтелектуального моніторингу та запобігання активності додатків. Предметом дослідження є методи інтелектуального моніторингу та запобігання активності додатків. Методи дослідження базуються на методах інтелектуального моніторингу, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуального моніторингу та запобігання активності додатків. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальний моніторинг, запобігання активності, додатки

Постановка проблеми. Малоймовірно, що ваш комп'ютер буде заражений вірусом, але в той же час існує небезпека зараження іншими типами шкідливих програм і онлайн-погроз. Трояни-вимагачі зашифровують важливі файли й чекають оплати викупу, перш ніж розблокувати доступ до них. Банківські трояни втручаються в онлайн транзакції й намагаються украсти кошти. Зараження ботнетом зробить ваш комп'ютер ланкою в ланцюзі пристроїв, використовуваних для організації DDoS-атак. З цих і багатьох інших причин, ви повинні захистити свій комп'ютер за допомогою антивірусу.

Багато які із представлених антивірусів є безкоштовними тільки для некомерційного використання. Якщо ви хочете захистити комп'ютери в організації, то прийдеться придбати платну версію. У цьому випадку варто розглянути перехід на повноцінний комплексний антивірус. Зрештою, від цього залежить безпека вашого бізнесу. Якщо захистити потрібно великі підприємства, то на допомогу приходять SaaS-рішення, які дозволяють централізовано виконувати моніторинг і управляти захистом всіх комп'ютерів у компанії.

Ваш антивірус повинен надійно видаляти шкідливі програми, що вкоренилися в системі, але його основне завдання – запобігання нових заражень троянами-шифрувальниками, ботнетами, троянами й іншими видами погроз. Всі представлені в даному рейтингу антивіруси пропонують захист реального часу проти шкідливих атак. Багато продуктів пропонують надійний веб-захист, що блокує доступ до джерел шкідливих об'єктів і запобігає уведення конфіденційних даних на шахрайських сайтах.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи інтелектуального моніторингу та запобігання активності додатків.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуального моніторингу та запобігання активності додатків.

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

– Огляд існуючих систем інтелектуального моніторингу та запобігання активності додатків.

– Дослідження системи інтелектуального моніторингу та запобігання активності додатків.

– Програмна реалізація системи інтелектуального моніторингу та запобігання активності додатків.

Об'єктом дослідження є процес інтелектуального моніторингу та запобігання активності додатків.

Предметом дослідження є методи інтелектуального моніторингу та запобігання активності додатків.

Методи дослідження базуються на методах інтелектуального моніторингу, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Розглянемо реалізацію системи моніторингу й запобігання активності додатків, що була реалізована у вигляді антивірусу.

Автономний антивірус включає систему запобігання вторгнень HIPS. У тесті протидії 30 експлойтам, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, виявив і заблокував більше половини з них, що краще результатів Bitdefender і Kaspersky. Norton заблокував дві-третини атак, причому все з них на мережному рівні.

Складна система контролю пристроїв більше підходить для корпоративних середовищ, чим для звичайних споживачів, хоча сам продукт більше орієнтований на домашніх користувачів. Технічно підковані люди можуть запобігти підключенню зовнішніх пристроїв, включаючи кард-рідери, Bluetooth і зовнішні USB-пристрої. Для довірених пристроїв можна створювати виключення.

На сторінці "Сервіс" користувачеві доступні файли журналу подій і список доданих у карантин файлів. Інші інструменти призначені для агентів технічної підтримки при віддаленому усуненні проблем. Серед таких утиліт – запущені процеси, графік активності файлової системи й інструмент для створення знімків стану системи для наступного порівняння.

Базовий фаєрвол

Під час тестування фаєрвол коректно перевів всі системні порти в схований режим і успішно протистояв веб-атакам. Проте, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не впорався з тестом, у якому використовувалися запити команди ping – це означає, що кіберзлочинець зможе з'ясувати реальну IP-адресу комп'ютера.

Ще однією перевіркою роботи двостороннього фаєрвола є випробування на блокування спроб зловживання мережними підключеннями. Програмний контроль програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, може працювати в декількох режимах. Стандартний автоматичний режим дозволяє весь вихідний трафік і блокує підозрілий вхідний трафік.

При перемиканні в інтерактивний режим, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, поводиться як традиційний фаєрвол, тобто при кожній спробі доступу в мережу з боку невідомої програми, продукт виводить користувальницький запит подальшої дії. Проте. функція контролю має кілька розширених опцій. Фаєрвол може застосувати ваш вибір один раз, створити на його основі постійне правило або запам'ятати вибір до завершення роботи програми. За замовчуванням, вибір не запам'ятовується, тобто користувачеві прийде щораз реагувати на запити.

Після натискання по посиланню докладної інформації, користувачеві показується інформація про видавця, репутацію файлу й віддаленому комп'ютері й портах. При виборі розширених налаштувань можна редагувати правила фаєрвола за допомогою окремих IP-адрес і номерів портів. Звичайним користувачам ці можливості не придадуться.

Багато продуктів, зокрема Norton і Kaspersky, приймають рішення програмного контролю самостійно й не покладаються на недосвідчених користувачів. ZoneAlarm Extreme Security 2017 для обробки додатків використовує масивну базу даних відомих надійних файлів і автоматично налаштовує програмний контроль. В інтерактивному режимі фаєрволу

програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, потрібно вручну визначати правила для всіх програм і навіть для компонентів Windows – не найкращий підхід.

Один зі способів уникнути нескінченного потоку запитів – використовувати режим навчання. У даному режимі програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, виконує моніторинг всіх програм, які одержують доступ у мережу й створює правила дозволу доступу. Режим навчання автоматично завершиться через два тижні, хоча даний період можна змінювати. Після цього запитів буде помітно менше. Також можна розглянути вибір режиму на основі політик, що блокує всі підключення за винятком тих, які дозволені правилами фаєрвола.

Мережний захист у програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, NOD32 Internet Security є розширеною в порівнянні з можливостями автономного антивірусу. Проте, у тесті експлойтів, обидва продукти показали однакові результати.

По вкрай мері, фаєрвол програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, успішно пручався прямим таргетованим атакам. Комплексний антивірус має два видимих процеси й одну службу, але в процесі тестування знайти спосіб для їхнього відключення за допомогою шкідливих технік не вдалося.

Фаєрвол програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, відверто розчарував. Він не зміг захистити від витоку реальної IP-адреси, а програмний контроль не повністю справляється зі своїм завданням. В інтерактивному режимі програма завалює користувача запитами. Це традиційний фаєрвол на базі застарілих технологій. Багато сучасних продуктів пропонують більше передові рішення.

Захист домашньої мережі

При виборі панелі “Захист домашньої мережі” у головному вікні антивірусу з'являється зображення карти мережі. Виявлені пристрої відображаються у вигляді іконок у концентричних колах. При цьому маршрутизатор і локальний пристрій показуються в самому центрі. Наступне коло показує недавно підключені пристрої, а саме далеке коло – пристрою, підключені за останній місяць.

Якщо програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не може одержати ім'я, то відображає IP-адреса. Майстер мережі дозволяє з'ясувати, що ховається за IP-адресу й допомагає додати зрозумілу назву. З режиму детального перегляду можна вибрати посилання усунення проблем, щоб подивитися заблокований фаєрволом трафік з даного пристрою.

Натисніть кнопку “Сканувати маршрутизатор”, щоб програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, перевірив налаштування безпеки вашого роутера. Буде запущено кілька тестів на проникнення, націлених на роутер. При виявленні проблем, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, відразу ж запропонує їх усунути.

Захист банківських платежів

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, приділяє особливу увагу даної функції, тому що одна із трьох панелей на головному екрані присвячена захисту банкінгу. При виборі панелі відкривається захищена версія вашого браузера за замовчуванням із зеленою рамкою й баннером “Захищене” на верхній панелі. Браузер відкриває сторінку, що пояснює мета даної функції й рекомендує використовувати її тільки для інтернет-банкінгу й проведення фінансові транзакції, а не для звичайного серфінгу. Після установки антивірусу потрібно виконувати перезавантаження комп'ютера, щоб захист банківської оплати запрацював. Функція підтримує роботу з Chrome, Firefox і Internet Explorer. Користувачі Opera, Vivaldi і інших браузерів не зможуть їй скористатися.

Також, як і функція "Безпечні платежі" у продуктах "Лабораторії Касперського", захист банківських платежів автоматично активується при відвідуванні відомого фінансового сайту у звичайному, незахищеному браузері. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, запропонує запустити безпечний браузер і запитає, потрібно чи запам'ятати цей вибір на постійній основі.

Обмежений батьківський контроль

Доступ до системи батьківського контролю програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, схований глибоко в налаштуваннях. У лівому навігаційному меню потрібно вибрати пункт “Налаштування”, а потім потрібно перейти в розділ “Засоби безпеки”. Після включення ви побачите список облікових записів Windows. Щоб завершити конфігурацію, потрібно вказати, які аккаунти належать дорослим, а які – дітям.

Залежно від віку дитини, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, визначає, які із трьох десятків категорій умісту будуть піддаватися блокуванню. При детальному розгляді правил можна побачити, що кожна категорія має вікові обмеження – для всіх, 12+, 18+ або заборонене. Зверніть увагу, що навіть для облікових записів дорослих будуть блокуватися категорії Кримінал і Шкідливе ПЗ. Одночасно в області видимості перебуває всього три категорії, тому налаштування системи викликає серйозні труднощі.

При тестуванні контент-фільтр працював надійно. Фільтр працює в будь-якому браузері й не відключається простими мережними командами, які були успішні з деякими конкурентами. Під час випробування не вдалося виявити сайти, які уникли блокування. При блокуванні програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, показує в браузері просте попередження, схожі оповіщення відображаються при виявленні фішінг-погрози або шкідливого сайту. Дитина не зможе запросити перегляд заблокованого сайту, як це можна зробити в Symantec Norton Family Premier.

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, обробляє захищені HTTPS сайти іншим образом. Він не може підмінити заблокований ресурс інформаційною сторінкою, тому в браузері з'являється повідомлення про помилку, а спливаюче повідомлення пояснює, що відбулося.

В основному додатку програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, батьки можуть переглядати список заблокованих сайтів із вказівкою дати й часу спроби відвідування, обліковому запису й категорії контенту.

На цьому можливості батьківського контролю закінчуються. Тут ви не знайдете функцію керування контактами в мессенджерах, аналітики соціальних мереж або контролю відеоігор по їхньому рейтингу. Крім того, недоступне керування часом використання Інтернету й комп'ютера. Батьківський контроль сильно урізаний, але працює добре.

Точний антиспам

Автономний антивірус програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, має ефективний убудований захист електронної пошти. Компонент сканує вхідну пошту POP3 і IMAP і вихідну пошту SMTP на предмет шкідливих программ. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, підтримує інтеграцію з Outlook, Outlook Express / Windows Mail або Windows Live Mail для розширеного контролю. При виявленні шкідливого ПЗ інструмент видаляє небезпечне вкладення й додає його назва до теми повідомлення. У комплексному антивірусі є ще повноцінний спам-фільтр.

Щоб включити антиспам, перейдіть у Налаштування > Захист Інтернету й виберіть іконку шестірні поруч із секцією “Захист від спаму”. Налаштувань не так багато. Користувач може включити розширений захист від спаму, що повинна поліпшити точність. Дана функція відключена за замовчуванням, тому що серйозно знижує швидкість обробки пошти. Можна

поміняти стандартну мітку [SPAM] і включити оцінку спаму. За замовчуванням антиспам імпортує список контактів і адресатів ваших повідомлень у виключення. Також туди містяться листи, які були вручну визнані не спамом. Доступно ручне редагування білого й чорного списку адресатів. У сучасних умовах спам-фільтр потрібний не всім, тому що багато поштових провайдерів уже мають дану функцію. Якщо вам усе ще потрібний окремий антиспам, то програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, прекрасно справляється із цим завданням.

Захист веб-камери

Повідомлення про випадки стеження за допомогою веб-камери з'являються із тривожною регулярністю. Звичайно, можна заклеїти камеру изолентой, але якщо ви часто берете участь у веб-конференціях, постійне заклеювання й відклеювання може стомити.

Захист веб-камери в програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, є доповненням програмного контролю, але більше простим у використанні. Користувач може заблокувати будь-які спроби доступ до камери й відключати захист тільки під час користування Skype. Якщо витратити небагато часу на налаштування, то можна вказати, які програми можуть одержувати доступ до камери й включити відображення оповіщення перед наданням доступу. Перевірити функцію в дії не вдалося, але для користувачів веб-камер вона може бути реально корисної.

Невеликий вплив на продуктивність

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, показав середній вплив на ресурси системи. У тесті виміру часу завантаження системи, антивірус сповільнив час завантаження всього на 11 відсотків, що краще середнього показника.

Розширений фаєрвол

Фаєрвол програмного продукту моніторингу й запобігання активності додатків, що був розроблений у даній роботі, справляється з базовими завданнями – відбиття атак на порти й перемикання всіх системних портів у схований режим. За замовчуванням програмний контроль обмежується дозволом вихідного трафіка й блокуванням підозрілого вхідного трафіка. В інтерактивному режимі при кожній спробі виходу в Інтернет з боку нової програми з'являється діалогове вікно із запитом подальшої дії. Фаєрволи в Kaspersky і Norton уміє автоматично обробляти дозволу для відомих надійних і шкідливих програм і пильно стежать за невідомими застосунками. Такий підхід є більше передовим, чим просто покласти ці обов'язки на плечі користувача. З позитивної сторони, не вдалося знайти спосіб для програмного відключення захисту ESET.

При запуску інструмента “Захист домашньої мережі” з'являється прорублена карта домашньої мережі з усіма підключеними пристроями. Ваш пристрій і роутер показуються в центрі, а інші пристрої розташовуються в концентричних колах залежно від залежності від дати підключення. При виборі кнопки сканування маршрутизатора програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, перевірить налаштування безпеки роутера й запропонує виправлення потенційних проблем.

Також як "Безпечні платежі" в Kaspersky, захист банківських операцій у програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, автоматично вступає в дію при відвідуванні фінансового сайту. Продукт пропонує запустити сайт у захищеному браузері з можливістю запам'ятати цей вибір.

Система батьківського контролю налаштовується окремо для кожного облікового запису Windows. Залежно від віку дитини застосовуються профілі, які дозволяють блокувати деякі з більше 30 категорій умісту. Можна самостійно налаштовувати фільтрацію. Категорії Кримінал і Шкідливе ПЗ блокуються навіть для аккаунтів дорослих. Компонент добре відробив при тестуванні, але не пропонує розширених функцій, а займається лише фільтрацією контенту й реєстрацією активності.

Спам-фільтр обробляє поштові аккаунти POP3 і IMAP і підтримує інтеграцію з популярними поштовими клієнтами. При використанні підтримуваного поштовика потрібно

налаштувати правило для автоматичної переадресації небажаної пошти в папку спаму. Ваші контакти автоматично попадають у список виключень і ніколи не блокуються. Також доступний чорний список для джерел спаму.

Боїтеся стеження за допомогою веб-камери? Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, вам готовий допомогти. Ви можете відключити використання веб-камери, коли вона вам не потрібна й дозволити доступ для окремих программ. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, може також попереджати при кожній спробі доступу до веб-камери.

Споконвічно здавалося, що додаткові функції повинні не кращим образом позначитися на продуктивності в порівнянні з комплексом початкового рівня. Однак, проведені випробування не виявили помітної різниці. Продукт небагато знижує швидкість завантаження системи й файлових ситуацій, але при реальному використання помітна з не відчувалася.

Потужний менеджер паролів

Менеджер паролів заснований на Sticky Password Premium, але одержав далеко не всі функції Sticky Password. Наприклад, користувач може синхронізувати паролі між декількома комп'ютерами й Mac, але не пропонує підтримку мобільних пристроїв. Також відсутня функція синхронізація паролів у бездротовій мережі Wi-Fi.

Спочатку потрібно створити майстер-пароль. Спливаюча підказка повідомляє, що майстер-пароль повинен складатися із заголовних, малих літер і цифр, а його довжина повинна бути не менш 8 знаків. Увести пароль можна за допомогою віртуальної клавіатури, щоб перестрахуватися від кейлоггерів. Під час моніторингу були перехоплені лише координати курсору, тому небажаний глядач ніколи не довідається, по яких клавішах ви кликали.

Можна налаштувати розблокування менеджера паролів при підключенні якого-небудь USB або Bluetooth пристрою. Проте, це не двофакторна автентифікація, тому що даний спосіб повністю заміняє введення майстр-пароля.

Менеджер паролів підтримують інтеграцію з Chrome, Firefox, Internet Explorer і значним списком менш популярних браузерів: Pale Moon, Comodo Dragon і SeaMonkey. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, уміє імпортувати паролі із браузерів, але на відміну від оригінальної версії Sticky Password, не імпортує закладки. Також підтримується імпорт даних з RoboForm, KeePass, LastPass, Dashlane.

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, захоплює облікові дані при авторизації на безпечних сайтах. Під час захвата користувач може задати зрозумілу назву для запису й визначити підходящу для неї категорію. Нову групу в цей момент створити не вийде на відміну від LastPass. Однак, в основному вікні менеджера паролів можна створити будь-яка кількість груп, включаючи вкладені групи. Ці категорії стануть пунктами й підпунктами основного меню списку паролів, що розкривається при натисканні по кнопці браузерного розширення.

При повторному відвідуванні програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, пропонує заповнити ваші облікові дані. Продукт упевнено обробляє події зміни паролів. Проте, при відвідуванні сайту з нестандартною формою авторизації, просто зберегти уведені дані не вийде, хоча дана можливість передбачена в LastPass і Sticky Password.

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, також захоплює облікові дані при створенні нового аккаунта. Убудований генератор допомагає створити захищений пароль для облікового запису. За замовчуванням програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, генерує 15-значний пароль, що містить заголовні букви, малі літери й цифри. Для посиленого захисту можна додати спецсимволи.

Також як RoboForm, LastPass і деякі інші продукти, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, уміє захоплювати й підставляти паролі додатків. Просто перетягнете курсор у вигляді хрестика у вікно уведення пароля, уведіть дані й збережете запис. Потім програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, сам подбає про автоматичний вхід.

Користувач може створювати кілька профілів – колекцій персональних даних для заповнення веб-форм. Для кожного профілю потрібно ввести персональну, контактну інформацію й ділові дані. При бажанні можна додати реквізити банківських рахунків або кредитних карт. При відвідуванні сторінки з веб-формою, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, виводить червону границю навколо полів заповнення. Просто натисніть по кнопці панелі інструментів і виберіть бажаний профіль заповнення. Як і багато інших програм, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, заповнює не всі форми, але в цілому справляється успішно. RoboForm Everywhere 7 спеціалізується на заповненні форм, підтримує більше типів полів, чим конкуренти й допускає кілька записів для одного типу поля.

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не пропонує наочної аналітики паролів, як у випадку з LastPass, Dashlane, або LogMeOnce Password Management. Замість цього він попереджає про паролі з низьким рівнем безпеки. Але не варто всерйоз покладатися на даний рейтинг, тому що 6-значний пароль, що використовує два набори символів буде вважатися нормальним. Слабкий пароль “Monkey” не з'явиться в списку попереджень.

У програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, відсутній ще кілька функцій оригінального Sticky Password. Тут недоступна онлайн консоль для керування пристроями. Наприклад, не можна заблокувати менеджер на загубленому пристрої або заборонити додавання нових пристроїв. Функція захищених заміток дозволяє зберігати важливу інформацію, що буде синхронізуватися між пристроями. Портативну версію менеджера паролів теж не вдасться створити в ESET. Навіть без цих функцій, менеджер паролів програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, є потужних інструмент, що по своїх можливостях перевершує багато автономних рішень.

Безпечне шифрування даних

Існує велика кількість ризиків втрати даних. Деякі трояни крадуть приватні дані й відправляють їх кіберзлочинцям. Загублений ноутбук може привести до витоку даних. Нарешті, ваші документи можуть бути доступні цікавим членам родини або колегам по роботі. Кращий спосіб захистити важливі дані – використовувати захищене шифрування. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, саме пропонує таку функцію.

Як і схожа функція в Bitdefender Internet Security 2017, Захист даних у програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, створює будь-яку кількість віртуальних зашифрованих дисків. Вам залишається ввести назву диска й розташування файлу, що буде містити дані віртуального диска. Ви можете вибрати доступні значення ємності диска: 500 Мб, 1 Гб, 5 Гб, 10 Гб, або 100 Гб або можете вказати довільний обсяг. Додайте пароль, і все готово до роботи.

Сторінка для уведення паролів нагадує, що у випадку втрати пароля, ви втратите доступ до ваших файлів, і навіть фахівці програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не зможуть допомогти. Проте, доступна опція для автоматичної розшифровки диска для поточного облікового запису Windows. Для посиленої безпеки рекомендується відключити цю опцію, якщо ваш аккаунт Windows не захищений дуже сильним паролем.

При розблокуванні, віртуальний диск працює, як і будь-який інший локальний диск. Ви можете переміщати файли на диск і з диска, редагувати вміст і виконувати будь-які інші дії. На відміну від інших аналогічних компонентів в інших продуктах, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не має функції примусового блокування захищеного сховища. Це відбувається автоматично при виході з облікового запису або при перезавантаженні комп'ютера.

Немає ніякого сенсу в шифруванні файлів, якщо ви залишаєте незашифровані оригінали. Багато рішень для шифрування поставляються разом з файловими шредерами, які безпечно видаляють оригінальний об'єкт без можливості відновлення. Kaspersky уміє автоматично видаляти оригінали при шифруванні їхніх копій. На жаль, але в програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, інструмент безпечного очищення відсутній. Можна використовувати клавіатурне сполучення Shift+Del, у цьому випадку файл буде видалений минаючи кошик, але це не убезпечить від потенційного відновлення.

Створити віртуальне зашифроване сховище можна й на переносному USB-накопичувачі. Процес аналогічний, але не потрібно вказувати ім'я й обсяг. Нова папка з назвою Encrypted з'явиться на флешці, і програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, буде автоматично запитувати пароль при підключенні пристрою. Також можна налаштувати автоматичне розблокування для поточного облікового запису.

Антизлодій

Антизлодій – розповсюджена функція для мобільних антивірусів, у десктопних версіях захист від крадіжки зустрічається нечасто. Bitdefender є одним з деяких конкурентів, які можуть визначати місце розташування, блокувати й стирати дані на пристроях Windows. Функція Антизлодій у програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не підтримує віддалене очищення, але вміє визначати геолокацію пристрою, блокувати його й знімати зображення з веб-камери й скріншоти екрана.

Керування функціями захисту від крадіжки здійснюється на веб-порталі. Спочатку буде запропоновано пройти кроки оптимізації. Якщо на вашім ноутбуці або планшеті Windows настроєний автоматичний вхід без уведення пароля, то буде запитана активація входу по паролі. Крім того, буде створений “фантомний аккаунт”.

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, кожних 10 мінут буде одержувати дані про статус пристрої. Якщо ви пометете пристрій як загублене, то програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, виконає комплекс мір: система буде перезавантажена й буде виконаний автоматичний вхід в “фантомний аккаунт”. Почнеться збір даних про геолокації й передача скріншотів екрана. При бажанні можна вивести повідомлення, наприклад, із проханням повернути пристрій по контактній адресі. Моніторинг буде тривати протягом 14 днів. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, повідомить по електронній пошті про закінчення періоду моніторингу.

Під час тестування функція працювала максимально коректно. Після перезавантаження список реальних аккаунтів не відображався й був доступний тільки “фантомний”. Одержати доступ до реальних користувальницьких файлів не вдалося. Система дійсно була заблокована. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, кожних 10 хвилин захоплював зображення екрана, і актуальні скріншоти відразу ж з'являлися в онлайн консолі. Роботу функції зняття фотографій з веб-камери перевірити не вдалося через відсутність пристрою.

Для визначення місця розташування програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, аналізує сигнали бездротових мереж. У випадку підключення через Ethernet локація не буде розпізнана. У довідковій

системі повідомляється, що в цьому випадку можна перевірити список IP-адрес, до яких підключається пристрій і визначити зону пошуку. Під час тестування місця розташування пристрої було визначено некоректно – посередині ставка в 13 кілометрах від його реальної локації.

Захист від крадіжки – дійсно корисна функція для ноутбуків. Всі ноутбуки оснащуються модулями бездротового зв'язку, а значить ви зможете відстежити їхнє знаходження. Якщо ви встановили програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, на ноутбук, не забудьте пройти кроки оптимізації, просто на випадок, якщо вам знадобляться функції Антизлодія.

Кібербезпека стала першочерговою проблемою в комерційних системах введення даних, чому зловмисники все частіше потребують програмне забезпечення-вразливості програмного та апаратного забезпечення для компрометації інформаційно-технологічної інфраструктури. Нещодавні досягнення свідчать про сплеск використання нових вразливостей для зловмисної діяльності, підкреслюючи критичну потребу в надійному захисті від зловмиснихзагроз програмного забезпечення

Шкідливе програмне забезпечення – широкий термін, що охоплює шкідливе програмне забезпечення – це фрагмент коду, розроблений кіберзлочинцями для проникнення в комп’ютерні системи без згоди користувача, що є несанкціонованим. доступ до даних, знищення файлів та інші шкідливі дії [1], [2]. Зростання інформаційних технологій посилило серйозність шкідливого програмного забезпечення як основну загрозу.

Традиційні методики визначення на основі програмного забезпечення, які базуються на аналізі сигнатур стикаються з такими недоліками продуктивності, як обмеження статичного аналізу, неможливість виявлення обфускованих та важких обчислювальних витрат, особливо на системи з обмеженими ресурсами.

Ці проблеми сприяють через обмеження обчислювальної потужності та пропускної спроможності зв’язку середовища інтегрованих систем [3], [4], [5]. Для вирішення цих викликів вкрай необхідно розвивати ефективні та економічно вигідні контрзаходи кібербезпеки, зосереджуючись на захисті інформаційних користувачів та пом’якшення нових кіберзагроз [6].

Це забезпечує парадигму переходу до інтеграції заходів безпеки в базове апаратне забезпечення, встановлюючи підхід «знизу вгору» для зміцнення комп’ютерного використання пристроїв, а не ставлення до безпеки як до другорядної [7]. У системах, дали успішних програм у різних галузях, особливо в підвищенні системи безпеки [8], [9], [10].

Нещодавні дослідження підкреслюють важливість визначення шкідливих дій на рівнях апаратного забезпечення та архітектури процесорів через його швидкість, ефективність та меншу видимість для наявних експлуатацій зловмисника.

З цим призначено апаратно-допоміжне шкідливе програмне забезпечення Методи виявлення (HMD), зокрема, з використанням машинного навчання з використанням функції продуктивності апаратного лічильника (HPC), з'являється як рішення недоліків традиційного програмного виявлення шкідливих програм [11], [12], [13], [14], [15].

Високопродуктивні процесори (HPC) – це спеціалізовані регістри в межах системи продуктивності. Блок моніторингу (PMU), вбудований в сучасні мікропроцесори, відстежують події апаратного забезпечення програми (наприклад, кількість виконаних циклів, інструкцій, пов’язаних з ними промахів кешу тощо)[16], [17], [18], [19].

Крім того, технології машинного навчання продемонстрували ефективність виявлення та класифікації аномалій у межах простору низького рівня оцінки. Використовуючи машинне навчання, системи можуть ефективно розпізнавати потенціал загрози та проактивно реагувати на зміни в поведінці в реальний час [7], [20].

Поточні дослідження в галузі інтелектуального виявлення шкідливих програм на Рівень апаратного забезпечення охоплюють різні обчислювальні платформи, такі як вбудовані системи, Інтернет речей і високонавантажені системи продуктивності.

Переважно використовуємо найсучасніші дослідження HMD-особливо наголошуємо на розробці та розробці стандартів передових методів машинного навчання для протидії еволюції загрози шкідливого програмного забезпечення.

У даній роботі наведено поглиблений аналіз апаратно-допоміжних методи виявлення шкідливого програмного забезпечення, зосереджені на останніх досягненнях у використанні штучного інтелекту та машинного навчання для покращення захисту систем від шкідливих нападів.

Зростання кількості та складності інфекцій шкідливим програмним забезпеченням впливає на окремих осіб та організації. Ці шкідливі програми з різноманітними функціональними можливостями розроблені для шкідливих цілей, таких як дистанційне керування, крадіжка даних, несанкціонований доступ, знищення файлів та проведення атак типу «відмова в обслуговуванні» [1], [10].

Наведемо огляд процесу підходів на основі машинного навчання, розроблених для підвищення кібербезпеки, зокрема в контексті апаратного виявлення шкідливого програмного забезпечення. Цей процес охоплює етапи від моніторингу програм для профілювання даних високопродуктивних обчислень, розробки функцій та навчання детекторів на основі машинного навчання та онлайн-виводу. Безперервне навчання моделей машинного навчання шляхом аналізу низькорівневих мікроархітектурних особливостей має на меті розпізнавання та протидію шкідливим шаблонам. Цей проактивний та інтелектуальний підхід захищає архітектуру процесора від потенційних загроз, що охоплюють не лише шкідливе програмне забезпечення, але й атаки по мікроархітектурних бічних каналах [21], [22].

Розробка ефективних апаратних детекторів шкідливого програмного забезпечення на основі машинного навчання починається з таких ключових кроків, як збір даних та вибір функцій [7], [11], [14], [16]. У сучасних мікропроцесорах можна збирати численні мікроархітектурні події, але вибір відповідних низькорівневих функцій є важливим для уникнення обчислювальної складності та затримок, пов'язаних з високовимірними наборами даних. Зокрема, ідентифікація суттєвих низькорівневих мікроархітектурних функцій є критично важливою для апаратного виявлення шкідливого програмного забезпечення з кількох причин:

– Велика кількість мікроархітектурних подій (наприклад, 100+ в Intel Xeon) призводить до високовимірних даних [14].

– Обробка необроблених наборів даних передбачає обчислювальну складність та спричиняє затримки [23].

– Вибір відповідних мікроархітектурних подій створює труднощі у визначенні нетривіальних подій для різних класів шкідливих програм [15].

Ця проблема ускладнюється обмеженою доступністю регістрів HPC у різних процесорах, зазвичай від 2 до 8.

Проблема обмеженої кількості регістрів HPC, тісно пов'язана з виявленням шкідливого програмного забезпечення під час виконання, обговорює значну проблему HMD, розглянуту в нещодавніх роботах [14], [15]. Вона включає визначення мінімального набору HPC, які точно фіксують характеристики шкідливих атак, тим самим мінімізуючи непотрібні обчислювальні витрати. Це прагнення забезпечує розробку ефективного контрзаходу безпеки на основі машинного навчання з мінімальним впливом на продуктивність системи. Щодо обмежень архітектури базового процесора, особливо в обчислювальних платформах з обмеженими ресурсами, таких як вбудовані системи та пристрої Інтернету речей з обмеженими регістрами HPC, ефективне, але точне виявлення під час виконання залежить від вибору критичних ознак. Нещодавні дослідження HMD, такі як [14], [15], [19], розглядали ефективне HMD під час виконання, визначаючи мінімальний набір основних подій лічильника продуктивності, необхідних для збору даних за один прогін.

Існує чотири основні кроки процесу розробки ознак:

– Очищення ознак включає аналіз необроблених даних для пошуку порожніх записів, викидів та будь-яких інших аномальних записів даних, щоб їх можна було видалити з процесу машинного навчання. Це також може забезпечити зворотний зв'язок для покращення збору даних.

– Нормалізація ознак є критичним кроком для масштабування табличних даних вздовж значень стовпців або рядків, запобігаючи домінуванню деяких даних або ознак з великими значеннями в процесі навчання. Цей метод є ефективним, особливо для алгоритмів машинного навчання, які чутливі до значень відстані між ознаками. Поширені методи нормалізації включають нормалізацію L1/L2 та нормалізацію MinMax.

– Вибір ознак включає аналіз важливості ознак, аналіз кореляції ознак та вибір найкращих ознак. Цей процес зазвичай виконується офлайн та ефективно тестується для цільової моделі машинного навчання.

– Вилучення ознак полягає у вилученні записів даних з найкращими ознаками для формулювання навчального набору даних. На етапі онлайн-виведення це означає вилучення онлайн-даних, які мають ті ж найкращі ознаки та розмірність, що й навчальний набір для обробки висновків за допомогою детекторів машинного навчання.

Вибрані ознаки високопродуктивних обчислень використовуються для навчання окремих детекторів на основі машинного навчання. Класифікатор прагне встановити кореляцію між значеннями ознак та поведінкою програми, прагнучи передбачити наявність шкідливих шаблонів (доброякісних або типу атаки). Кілька методів вибору ознак відіграли важливу роль у попередніх зусиллях HMD на основі машинного навчання. До них належать такі методи, як оцінка атрибутів кореляції [14], [24], [25], [15], [26], [27], аналіз головних компонент [15], [26], [28], оцінка коефіцієнта підсилення [16], [19], [29] та оцінка Фішера [30], [12].

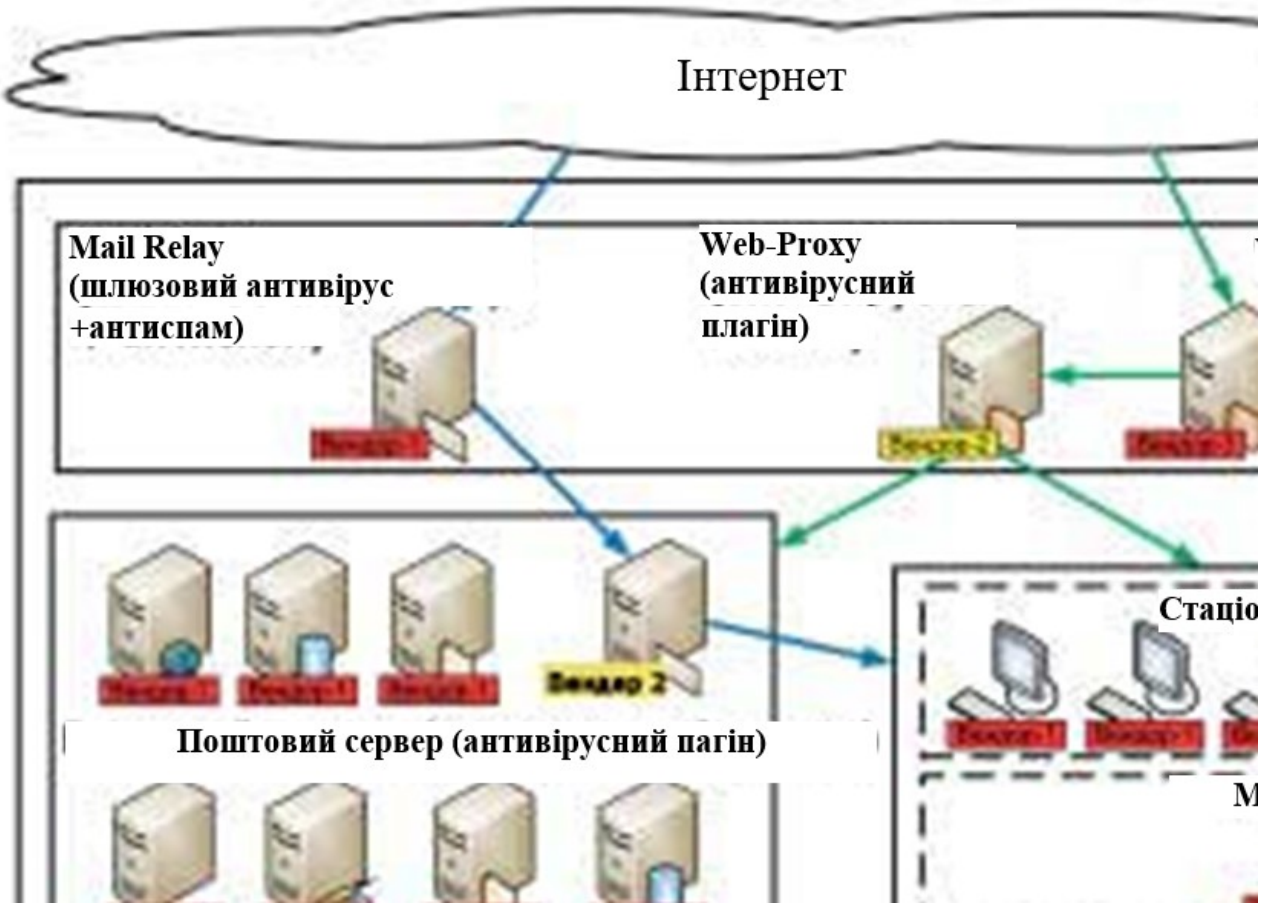

Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального моніторингу та запобігання активності додатків. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем інтелектуального моніторингу та запобігання активності додатків.

– Досліджена система інтелектуального моніторингу та запобігання активності додатків.

– На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального моніторингу та запобігання активності додатків.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуального моніторингу та запобігання активності додатків. 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. 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
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
15. 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
16. 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.
17. 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.
18. 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.
19. 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.
20. 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 ȟозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
21. 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.
22. 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.
23. 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.
24. 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,
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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
31. 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.