УДК 004

Д.Бобровський, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ДАНИХ GPRS-МЕРЕЖІ, РОЗГОРНУТОЇ НА ПРИСТРОЯХ, ЯКІ ПРАЦЮЮТЬ ПІД ОС ANDROID

У статті розроблено програмне забезпечення, яке призначено для системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. Метою розробки є дослідження та принципи побудови системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. Об'єктом дослідження є процес захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. Предметом дослідження є методи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

системи захисту даних, GPRS-мережа, Android

Постановка проблеми. Щоб можна було скористатися перевагами GSM мереж, їх необхідно захистити. Незахищені бездротові мережі відкривають практично необмежений доступ до корпоративної мережі для хакерів і інших зловмисників, які нерідко прагнуть лише одержати безкоштовний доступ в Internet. Відповідно, дані, які передаються по GPRS, потребують захисту.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

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

– Огляд існуючих систем захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

– Дослідження системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

– Програмна реалізація системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

Об'єктом дослідження є процес захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

Предметом дослідження є методи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Безпека мобільних даних є критично важливим пріоритетом у 2025 році, оскільки компанії стикаються зі зростанням кіберзагроз,

спрямованих на смартфони, планшети та інші підключені пристрої. Зростання мобільних кіберзагроз, витоків даних та атак шкідливого програмного забезпечення вимагає надійних заходів безпеки. Такі фактори, як віддалена робота, політика BYOD (Bring Your Own Device) та хмарні мобільні сервіси, ще більше ускладнюють проблеми безпеки. Організації повинні впроваджувати рішення для безпеки мобільних даних, щоб запобігти несанкціонованому доступу, витокам даних та фішинговим атакам.

Розуміння безпеки мобільних даних

Безпека мобільних даних передбачає захист конфіденційних даних на мобільних пристроях за допомогою шифрування, автентифікації та методів зменшення загроз.

Забезпечення безпеки мобільних даних має вирішальне значення для запобігання:

– Несанкціонований доступ та витоки даних.
– Атаки програм-вимагачів та шкідливих програм.
– Внутрішні загрози та спроби фітингу.

Як розвивається ландшафт мобільних загроз

Кібератаки продовжують зростати як за частотою, так і за винахідливістю, і нещодавні звіти лідерів галузі, таких як Verizon та IBM, відзначають стабільне зростання з року в рік. Сьогоднішні зловмисники не просто закидають широкі сітки – вони використовують складні методи, спеціально спрямовані на мобільні пристрої та їхніх користувачів.

Нові та постійні тенденції у сфері мобільних загроз включають:

– Розширене шкідливе програмне забезпечення та фішинг: Шкідливі програми та оманливі посилання можуть проникнути на ваш пристрій, видаючи себе за легітимні завантаження або повідомлення. Зловмисники використовують дедалі переконливіші тактики соціальної інженерії, щоб обманом змусити користувачів відмовитися від облікових даних або встановити шкідливе програмне забезпечення.

– Атаки типу «людина посередині»: пристрої в незахищених мережах вразливі до перехоплення зловмисниками їхніх повідомлень. Цей метод може призвести до витоку конфіденційних даних під час чогось такого простого, як перевірка електронної пошти в громадському Wi-Fi.

– Компрометація пристрою: Зловмисники використовують такі методи, як джейлбрейк та рутінг, для обходу обмежень безпеки, що надає їм глибший доступ до пристрою та його даних. Сучасні загрози здатні маскувати їхню активність, що ще більше ускладнює виявлення.

– Вразливості ОС: Зловмисники швидко використовують нещодавно виявлені вразливості в мобільних операційних системах (відстежуються як CVE), іноді швидше, ніж встигають випустити патчі.

– Контроль доступу до корпоративних ресурсів: Організації спостерігають дедалі більше спроб заражених пристроїв підключитися до внутрішніх мереж, що підвищує ризик витоку даних та несанкціонованого доступу до критично важливих для бізнесу активів.

Щоб випередити ці загрози, потрібні багаторівневі захисні рішення та постійне навчання, що гарантує готовність як пристроїв, так і користувачів до будь-яких загроз, які підкине їм ландшафт мобільних загроз, що розвивається.

Ключові проблеми безпеки в мобільних середовищах:

– Ризики незахищеного Wi-Fi: публічні мережі наражають користувачів мобільних телефонів на кіберзагрози.

– Шкідливі програми та мобільне програмне забезпечення: Зловмисники атакують пристрої через неперевірені програми.

– Ризики втрати та витоку даних: втрачені/викрадені пристрої можуть поставити під загрозу конфіденційні дані.

– Прогалини в безпеці BYOD та корпоративних пристроїв: балансування безпеки з продуктивністю користувачів.

Виявлення та запобігання розширеному джейлбрейку та рутінгу

Надійні рішення для мобільної безпеки використовують низку стратегій для виявлення та протидії складним спробам джейлбрейка (iOS) та рутування (Android) пристроїв. Ці інструменти постійно контролюють цілісність пристроїв шляхом:

– Сканування на наявність незвичайних модифікацій системи або несанкціонованих змін у файлах ОС.

– Виявлення наявності сторонніх інструментів керування, які часто використовуються для джейлбрейка/рутингу.

– Використання поведінкової аналітики для позначення підозрілої активності та підвищення привілеїв.

– Забезпечення автоматичного виконання дій відповідності, таких як обмеження доступу до пристроїв або запуск віддаленого стирання, у разі виявлення потенційної компрометації.

Провідні платформи, такі як Lookout, Zimperium та Symantec, інтегрують ці заходи виявлення загроз, щоб забезпечити доступ до конфіденційних бізнес-ресурсів лише безпечним пристроям, що відповідають політикам.

Вплив генеративного штучного інтелекту на мобільну безпеку

Генеративний штучний інтелект швидко трансформує ландшафт мобільних загроз, впроваджуючи нові та складні методи атак, які вимагають нашої уваги. Від переконливих фішингових повідомлень, що генеруються на льоту, до автоматизованих атак соціальної інженерії, загрози на базі штучного інтелекту тепер можуть обходити традиційні засоби захисту з безпрецедентною швидкістю та тонкістю.

Щоб випереджати ці ризики, що змінюються, організаціям слід:

– Впроваджуйте виявлення загроз на основі штучного інтелекту: використовуйте інструменти безпеки від таких постачальників, як Palo Alto Networks та Symantec, які використовують машинне навчання для виявлення незвичайної поведінки та нових загроз.

– Навчайте користувачів шахрайству на основі штучного інтелекту: регулярно навчайте співробітників та користувачів мобільних пристроїв розпізнавати дипфейкові дзвінки, голосовий фішинг (вішинг) та ретельно розроблені шкідливі повідомлення.

– Впроваджуйте безперервне сканування програм: використовуйте рішення, які відстежують шкідливі програми та код, створений або розроблений за допомогою методів генеративного штучного інтелекту.

– Посилення контролю автентифікації: поєднання біометричної автентифікації та адаптивної багатофакторної автентифікації (MFA) для мінімізації ризику підробки облікових даних за допомогою штучного інтелекту або видання себе за іншу особу.

Інвестування в рішення, що розвиваються разом із загрозами, спричиненими штучним інтелектом, може бути вирішальним фактором між реагуванням на порушення та його запобіганням. Проактивна адаптація зараз є важливою для сучасної мобільної безпеки.

Як виявляються та управляються вразливості операційної системи

Програмне забезпечення для захисту мобільних даних проактивно сканує пристрої на наявність вразливостей операційної системи, постійно відстежуючи нові виявлені CVE (поширені вразливості та ризики). Провідні рішення використовують оцінку ризиків у режимі реального часу, регулярно перевіряючи налаштування пристроїв, конфігурації системи та дозволи. Розширені інструменти від таких постачальників, як Symantec та Lookout, сповіщають адміністраторів щоразу, коли вони виявляють ознаки компрометації, несанкціоновані зміни конфігурації або спроби рутування чи джейлбрейка пристрою.

Ці рішення допомагають IT-командам випереджати загрози завдяки:

- Виявлення та позначення невиправлених вразливостей і ризикованих конфігурацій.
- Надання автоматизованих інструкцій або опцій віддаленого виправлення.
- Блокування спроб компрометації до того, як відбудеться експлуатація.

Підтримуючи постійний контроль за станом операційної системи та забезпечуючи дотримання надійних конфігурацій, організації можуть значно знизити ризик успішних мобільних атак або витоків даних.

Ключові характеристики, які слід шукати в програмному забезпеченні для безпеки мобільних даних

– Розширений захист від мобільних загроз (MTD): виявлення фішингу, шкідливого програмного забезпечення та загроз нульового дня на основі штучного інтелекту.

– Наскрізне шифрування: Безпечний мобільний зв'язок, електронна пошта та обмін файлами.

– Безпечна контейнеризація: ізоляція бізнес-даних та особистих даних на одному пристрої.

– Можливості віддаленого стирання та блокування: запобігання втраті даних у разі крадіжки або компрометації пристрою.

– Багатофакторна автентифікація (MFA) та біометричний захист: забезпечення безпечного входу.

– Запобігання втраті даних (DLP): обмеження несанкціонованого доступу до даних та їх передачі.

– Мобільний VPN та мережева безпека: захист даних у публічних та корпоративних мережах.

– Хмарне керування мобільною безпекою: керування політиками безпеки для віддалених користувачів.

Інфраструктура мережевої безпеки: попередження нових загроз

Інфраструктура безпеки мобільних мереж відіграє ключову роль у допомозі підприємствам проактивно захищатися від нових і постійно зростаючих загроз. Використовуючи передові засоби захисту на пристроях, подібні до тих, що містяться в провідних пакетах безпеки для настільних комп’ютерів, організації можуть забезпечити безпеку мобільних кінцевих точок, навіть коли користувачі підключаються через незахищені мережі Wi-Fi або стільникового зв’язку.

Деякі ключові переваги включають:

– Виявлення загроз у режимі реального часу: Розширена система безпеки на рівні мережі постійно відстежує шкідливу активність, включаючи спроби фішингу, підозрілий трафік та атаки типу «людина посередник», зупиняючи загрози до того, як вони вплинуть на пристрої або конфіденційні дані.

– Безшовна інтеграція: Ці рішення працюють разом з існуючими політиками безпеки підприємства, поширюючи на мобільні пристрої той самий надійний захист, який уже діє для традиційних кінцевих точок.

– Захист з будь-якого місця: Співробітники часто підключаються з аеропортів, готелів або кав’ярень. Надійний рівень мережевої безпеки гарантує захист конфіденційних бізнес-даних незалежно від місцезнаходження.

Впроваджуючи комплексні стратегії мережевої безпеки від таких постачальників, як Lookout, Zimperium та Symantec, організації можуть значно зменшити свій вплив як відомих, так і нових кіберзагроз на мобільних платформах.

Блокування заражених пристроїв з корпоративних ресурсів

Провідні платформи безпеки використовують комбінацію моніторингу стану пристроїв у режимі реального часу та динамічного контролю доступу, щоб захистити конфіденційні дані компанії від скомпрометованих пристроїв. Коли виявляються загрози – будь то шкідливе програмне забезпечення, фішингові атаки чи неавторизовані програми – програмне забезпечення автоматично скасовує або обмежує доступ до корпоративних мереж, хмарних сервісів та критично важливих для бізнесу програм.

Наприклад, такі рішення, як Lookout та Zimperium, використовують оцінки ризиків на основі штучного інтелекту для постійного сканування пристроїв. Якщо виявлено загрозу, платформа може:

– Миттєво ізолюйте пристрій від корпоративних VPN, електронної пошти та інструментів для співпраці.

– Застосування політик умовного доступу через інтеграцію з постачальниками ідентифікаційних даних (таких як Okta або Microsoft Entra).

– За потреби активувати протоколи віддаленого стирання.

Поєднуючи автоматичне виявлення, забезпечення дотримання політик та сегментацію на рівні мережі, ці платформи допомагають забезпечити доступ до ресурсів вашої організації лише справних пристроїв, що відповідають вимогам.

Переваги єдиного захисту кінцевих точок в одному клієнті

Керування безпекою мобільних даних для сучасних віддалених працівників може швидко перетворитися на жонглювання десятками інструментів, кожен з яких має свої особливості та портали. Саме тут на допомогу приходить універсальний клієнт захисту кінцевих точок, який поєднує платформи захисту кінцевих точок (EPP), засоби виявлення та реагування на кінцеві точки (EDR) та розширене виявлення та реагування (XDR) в одному оптимізованому пакеті.

Чому варто об'єднати кошти до одного клієнта:

– Спрощене керування безпекою: маючи все під одним дахом, IT-команди можуть контролювати, налаштовувати та застосовувати політики з централізованої панелі інструментів, що зменшує адміністративні труднощі.

– Зменшення складності та покращення продуктивності: Запуск кількох агентів безпеки часто призводить до уповільнення роботи системи та проблем сумісності. Уніфікований клієнт потребує менше ресурсів та зменшує ризик конфліктів.

– Комплексна видимість загроз: інтеграція EPP, EDR та XDR забезпечує швидше виявлення загроз та реагування на них на кінцевих точках, у мережах та хмарних середовищах, чого важко досягти за допомогою об’єднаних інструментів.

– Стабільне покриття: Від програм-вимагачів до шкідливих програм нульового дня, єдине консолідоване рішення гарантує відсутність прогалин у безпеці між непов’язаними інструментами.

– Спрощені оновлення та виправлення: Замість того, щоб витрачати час на оновлення для кількох окремих програм, єдиний клієнт дозволяє розгортати найновіші засоби захисту одночасно, забезпечуючи стійкість усіх кінцевих точок до нових загроз.

Примітно, що провідні постачальники рішень безпеки, такі як CrowdStrike, SentinelOne та Sophos, застосували цей підхід, зробивши надійну комплексну безпеку кінцевих точок новим стандартом для гнучких та безпечних мобільних працівників.

Найкращі практики для посилення мобільної безпеки:

– Впроваджуйте стратегію захисту від мобільних загроз (MTD) – захищайтеся від шкідливого програмного забезпечення, фішингу та мережевих загроз.

– Забезпечте надійне мобільне шифрування та автентифікацію – використовуйте біометричні дані для входу та багатофакторну автентифікацію.

– Розгортання політик безпеки мобільних пристроїв підприємства – визначення правил безпечного використання програм і доступу до даних.

– Моніторинг та усунення ризиків мобільної безпеки – постійне відстеження вразливостей та неправильних конфігурацій.

– Увімкніть безпечний перегляд мобільних веб-сторінок та захист електронної пошти – запобігайте фішинговим атакам та атакам типу «людина посередині» (MITM).

– Забезпечте запобігання втраті даних (DLP) на мобільних пристроях – контролюйте обмін файлами та обмеження доступу.

Як забезпечити душевний спокій під час вибору програмного забезпечення для мобільної безпеки

Вибір правильного програмного забезпечення для мобільної безпеки має вирішальне значення для захисту ваших особистих даних та забезпечення душевного спокою. Ось як споживачі можуть прийняти обґрунтоване рішення:

1. Широко дослідіть: почніть з вивчення різних варіантів на ринку. Шукайте відгуки та експертні оцінки на надійних технологічних веб-сайтах. Ці дані можуть виявити сильні та слабкі сторони програмного забезпечення.

2. Порівняння функцій: Визначте основні функції, такі як захист від шкідливого програмного забезпечення, можливості захисту від фішингу та запобігання крадіжкам. Порівняйте продукти, щоб побачити, який з них пропонує повне покриття.

3. Перевірте незалежні тести: Шукайте програмне забезпечення, яке пройшло незалежне тестування у відомих лабораторіях кібербезпеки. Сертифікати від сторонніх організацій можуть гарантувати надійність та ефективність.

4. Відгуки користувачів: Відгуки користувачів безцінні. Перегляньте онлайн-форуми та магазини додатків, щоб дізнатися про реальний досвід, який може виявити потенційні проблеми або видатні функції.

5. Пробні версії: оберіть програмне забезпечення, яке пропонує безкоштовний пробний період. Це дозволить вам безпосередньо випробувати функціональність та оцінити зручність використання без початкових витрат.

6. Підтримка клієнтів: Надійна служба підтримки клієнтів може стати справжнім порятунком у разі технічних проблем. Перевірте, чи пропонує компанія доступні та оперативні варіанти підтримки.

Ретельно досліджуючи та оцінюючи рішення для мобільної безпеки на основі цих факторів, споживачі можуть вибрати продукт, який не лише відповідає їхнім потребам, але й забезпечує душевний спокій.

Розуміння переваг тестування програмного забезпечення для мобільної безпеки

У сучасну цифрову епоху забезпечення безпеки вашого мобільного пристрою є надзвичайно важливим. Але яку користь вам як споживачеві насправді приносить процес тестування та оцінки програмного забезпечення для мобільної безпеки? Давайте розглянемо це детальніше.

Обґрунтоване прийняття рішень

Коли експерти тестують та оцінюють варіанти мобільної безпеки, вони надають вам важливу інформацію про їхню продуктивність та ефективність. Замість того, щоб сліпо вибирати програмне забезпечення, ви маєте доступ до:

– Детальні звіти порівняння: Подивіться, як різні продукти порівнюються один з одним з точки зору функцій та рівнів захисту.

– Показники продуктивності: Зрозумійте, яке програмне забезпечення пропонує найкращий захист без шкоди для продуктивності вашого пристрою.

Посилена гарантія безпеки

Не все програмне забезпечення для мобільної безпеки однакове. Завдяки ретельному тестуванню:

1. Перевірка ефективності: Ви дізнаєтесь, які рішення є найефективнішими для блокування таких загроз, як шкідливе програмне забезпечення, спроби фішингу та підозрілі програми.

2. Оновлений захист: гарантує, що програмне забезпечення може адаптуватися до найновіших загроз безпеці, забезпечуючи безпеку ваших даних.

Ефективність витрат

Інвестування в правильне програмне забезпечення для мобільної безпеки означає розумні витрати. Огляди тестування можуть виділити:

– Співвідношення ціни та якості: Визначте продукти, які пропонують найкращі характеристики за розумною ціною.

– Уникнення помилок: заощаджуйте гроші, уникаючи неякісного програмного забезпечення, яке не забезпечує належного захисту.

Аналітика користувацького досвіду

Окрім безпеки, критично важливим є те, як програма взаємодіє з користувачами. Тестування показує:

– Простота використання: Дізнайтеся, яке програмне забезпечення має зручні інтерфейси, що роблять навігацію легкою.

– Підтримка клієнтів: Зрозумійте рівні підтримки, що пропонуються, якщо у вас виникнуть будь-які проблеми або вам знадобиться допомога.

Перетворюючи комплексне тестування на чіткі, практичні висновки, споживачі краще підготовлені до вибору програмного забезпечення для мобільної безпеки, яке не лише відповідає їхнім потребам, але й забезпечує душевний спокій у цифровому світі.

Для високих вимог безпеки галузі ми повинні забезпечити безпеку передачі даних. Які способи гарантують безпеку даних під час використання GPRS-модемів? Існує наступний спосіб вирішення проблеми: оператори APN або VPDN впроваджують технологію тунелювання VPDN, що передбачає інкапсуляцію даних у корпоративній мережі для передачі в тунелі. Основний процес тунелювання полягає в тому, що на інтерфейсі між вихідною локальною мережею (LAN) та загальнодоступною мережею дані упаковуються в контейнер у форматі передачі даних загальнодоступної мережі. На інтерфейсі з загальнодоступною мережею LAN цільове рішення інкапсулює дані та знімає навантаження.

Логічний шлях – це інкапсульовані пакети, що передаються через Інтернет, що називається «тунелюванням». Для забезпечення плавної інкапсуляції, передачі та декапсуляції даних використовується протокол зв'язку, який забезпечує безперебійну роботу ядра. Може використовуватися для міжрегіональної групової інтрамережі, спеціалізованої мережі постачальників професійних інформаційних послуг, магістральних мереж, фінансових державних послуг, банківських та інших послуг для доступу до бізнес-мереж. У практичному застосуванні операторам необхідно відкрити відповідний бізнес-проект, а для його реалізації – прокласти власну лінію зв'язку. Недоліком є громіздкість бізнес-процедур, висока вартість використання та непридатність для загальних проектів. Якщо ви не можете подати заявку на спеціальні мережеві послуги, чи є інші способи забезпечити безпеку даних? Це може бути забезпечено лише апаратним забезпеченням.

У галузі GPRS-модемів зазвичай немає такої функції. У Сямень комунікаційні компанії протягом багатьох років досліджували бездротове термінальне обладнання для передачі даних, і останній продукт компанії – WCTU. Підтримка шифрування даних, підтримка шифрування для DES, 3DES, AES. Під час налаштування WCTU лише запустіть відповідні налаштування. Коли дані WCTU пакетуються, вони використовують шифрування DES, 3DES та AES. Такі дані не турбуються про безпеку в Інтернеті. Ця функція зручна та проста у використанні, її слід популяризувати.

Щоб ефективно керувати своєю мережею та приймати обґрунтовані рішення, вам потрібно збирати інформацію про моделі мережевого трафіку. Якщо у вас виникли проблеми, пов'язані з підключенням або безпекою, вам потрібно мати змогу виявляти зміни в трафіку. Carrier Security надає набір інструментів, що відповідають особливим потребам стільникових мереж.

Журнали та сповіщення відстеження GTP

Служба безпеки оператора записує інформацію про активність сигналізації GTP, що стосується стільникового зв'язку, включаючи APN, IMSI, режим вибору, адреси GSN тощо. Інформація, записана в цих журналах, може допомогти вам визначити, чому певний трафік GTP може бути відхилений або заблокований, а також вирішити, чи слід налаштувати Політику безпеки для прийняття цього трафіку.

Шлюз перевірки GTP Carrier Security генерує широкий спектр детальних сповіщень безпеки у разі порушень протоколу та політики безпеки, включаючи деталі PDU, інформацію про мережу та тип порушення протоколу. Carrier Security також надає сповіщення, специфічні для GTP, про неправильно сформовані пакети та шкідливу активність.

Запис даних GTP з незрівнянних PDU

Carrier Security може записувати GTP-трафік, який не відповідає правилу GTP у базі правил. Зазвичай трафік, який не відповідає правилу, реєструється в загальному журналі як простий Drop. Carrier Security надає інструмент для збору цих даних за допомогою спеціальних полів, пов'язаних із GTP, які можуть допомогти виявити причину цих падінь.

Бухгалтерський облік GTP

Встановивши правило трафіку користувача GTP на Log, Carrier Security створює запис у журналі для кожного завершеного контексту PDP , який відповідає правилу. У журналі записується загальна кількість користувацьких пакетів (n_pdu) та байтів (n_byte), переданих у площині користувача під час контексту PDP . Carrier Security створює журнали для таких подій:

- Видалення контексту/сеансу PDP.
- Закінчення терміну дії тунелю.
- Відпочинок у тунелі.
- Активний шлюз не працює (у режимі високої доступності).

Захист від надмірних журналів

Через малу кількість пакетів стільникового зв'язку, Carrier Security щодня записує величезну кількість даних, набагато більше, ніж типовий брандмауер Check Point. Цей збір даних є важливим для точної діагностики стану мережі та усунення помилок мережі.

Така інтенсивна активність ведення журналу може зробити деякі системи більш вразливими до атак типу «відмова в обслуговуванні» (DoS). Carrier Security захищає від цього типу атаки, встановлюючи similar loggingпоріг, вище якого аналогічні журнали не генеруються. Цю функцію можна налаштувати.

За замовчуванням – кожні 10 секунд.

Режим лише монітора

Режим лише моніторингу відстежує певний несанкціонований трафік, не блокуючи його. У цьому режимі брандмауер продовжує перевіряти трафік GTP, але не застосовує жодних засобів захисту, пов'язаних з GTP. Він продовжує застосовувати правила безпеки, пов'язані з GTP, реєструвати активність, пов'язану з GTP, а також створювати журнали помилок і сповіщення GTP. Режим лише моніторингу дозволяє операторам переглядати результати змін глобальних властивостей і налаштувань, що стосуються перевірки GTP. Цей режим корисний для запобігання непередбачуваній поведінці під час першого впровадження безпеки оператора, а також щоразу, коли в глобальні властивості вносяться зміни.

Після ретельного перегляду журналів та переконання, що зміни не перешкоджають легітимному стільниковому трафіку, оператор стільникового зв'язку може вимкнути режим «Тільки моніторинг», а брандмауер може почати блокувати шкідливий GTP-трафік.

Carrier Security слідкує за тунелями GTP та зберігає їх statetак, як це було б у звичайному режимі роботи. Таким чином, ви можете плавно вмикати та вимикати режим лише моніторингу – вся інформація про тунель продовжує існувати в обох режимах, і жодні тунелі не втрачаються під час переходу.

Налаштування моніторингу

- Створювати розширений журнал для незбіганих PDU. Реєструє GTP-пакети, які не збігаються з попередніми правилами, за допомогою розширених полів журналу, пов'язаних з GTP, Carrier Security. Ці журнали мають коричневий колір, а їхній атрибут Action порожній. Значення за замовчуванням – checked.

– Опція відстеження порушення протоколу дозволяє встановити відповідну опцію відстеження або сповіщення, яка використовуватиметься у разі виявлення порушення протоколу (спотвореного пакета). Налаштування за замовчуванням – Log.

GPRS-мережа має зв'язку з великою кількістю зовнішніх мереж (інтернет, роумінг-партнери, корпоративні клієнти, провайдери GRX (GPRS Roaming Exchange), і т.д.). Таке сусідство й партнерські відносини ставлять перед мобільними операторами підвищені вимоги по забезпеченню безпеки переданих даних. Так як зв'язок з партнерами й доступ в інтернет здійснюється по протоколі IP, а усередині GPRS-магістралі дані інкапсулюються в небезпечні тунелі GTP, те границю GPRS-мережі необхідно надійно захищати.

Основну погрозу представляють напрямки Gi і Gp, так як використовуючи протокол IP, будь-який користувач може посилати довільні пакети в GPRS-мережу. Оскільки оператори не обмежують типи користувальницького трафіку, користувачі мобільних терміналів перебувають повністю відкритими для всіх недуг інтернету (віруси, хробаки, трояни, DoS і т.д.). Відповідно, не захищені й користувальницькі дані, які відправляються в зовнішні мережі. Також більшість атак можуть бути спрямовані на саму GPRS-інфраструктуру (Gn), викликаючи відмову або некоректну роботу устаткування.

Типи атак на потенційно небезпечних GPRS-інтерфейсах:

1.Gp-інтерфейс:

– паразитний трафік роумінг-партнера;

– DNS флуд;

– GTP флуд;

– довільне видалення PDP- контекстів користувачів;

– некоректна BGP-інформація;

– підміна DNS-відповідей;

– підміна запитів Create/Update PDP Context;

– overbilling attacks.

2.Gi-інтерфейс:

– DoS-атаки;

– флуд з IP-адрес мобільних станцій;

– влучення в корпоративну мережу іншого клієнта.

3.Gn-інтерфейс:

– підміна GGSN/SGSN;

– підміна запиту видалення PDP-контекстів користувачів;

– атаки мобільних користувачів друг проти друга.

Завдання захисту Gn і Gp інтерфейсів ускладнює особливість комунікацій, які ведуться там по засобом протоколу GTP.

Принцип роботи GTP кардинально відрізняється від інших IP-протоколів: GTP-тунель може бути розподілений по декількох IP-сесіях, і навпаки – одна IP-сесія може містити трохи GTP-тунелів. Такий принцип роботи робить практично марним застосування класичних IP-Firewall для фільтрації GTP-трафіку. Виходячи з того, що звістка IP-трафік на інтерфейсах Gn і Gp інкапсульован в GTP, на даних інтерфейсах необхідний GTP Firewall для перевірки коректності функціонування GTP.

Безліч атак функціонує на більше високих рівнях подання даних (Layer 5-7), ніж ті, з якими працює фаєрвол (Layer 2-4). Тому, як другий ешелон захисту від атак рівня додатків, потрібна система запобігання вторгнень. Аналізуючи легітимний трафік, що пройшов через Firewall на Layer 2-4 дана система проведе високорівневий аналіз і зможе виявити й запобігти атакам, що ховаються в трафіку додатків. Стосовно до GPRS-мережі, такий підхід вибудовування системи захисту особливо ефективний у точці підключення до мережі інтернет (інтерфейс Gi).

Пропонується використовувати ефективне рішення для операторів зв'язку, що здатно забезпечувати безпека трафіку в будь-якій точці GPRS-мережі. Мова йде про лінійку високопродуктивних шлюзів безпеки Juniper High-End SRX з підтримкою GTP. Пристрою

Juniper HE SRX – це універсальна модульна платформа, що поєднує функціонала різнорідних пристроїв (firewall, маршрутизатор, комутатор, UTM, IDP) в одному шасі. Всі пристрої працюють під керуванням надійної платформи JunOS, що успішно зарекомендувала себе в сегменті магістральних рішень. Модульна архітектура SRX дозволяє гнучко масштабувати продуктивність для виконання необхідного функціонала. Підтримка протоколу GTP робить їхнім незамінним рішенням питань безпеки для мобільних GPRS-операторів зв'язку, що легко інтегрується з технологією GPRS Tunneling Protocol.

Впровадження Juniper HE SRX у на найнебезпечніших ділянках GPRS-мережі, а саме, на інтерфейсах Gn і Gp, забезпечить перевірку коректності роботи протоколу GTP і контроль інформаційних потоків між PLMN. А наявність убудованої системи запобігання вторгнень (Juniper IDP) дозволяє High-End SRX забезпечувати фільтрацію трафіку й високоінтелектуальний захист від атак одночасно. Дана особливість оптимально підходить для захисту Gi інтерфейсу GPRS-мережі, що забезпечує взаємодію з небезпечним Інтернет.

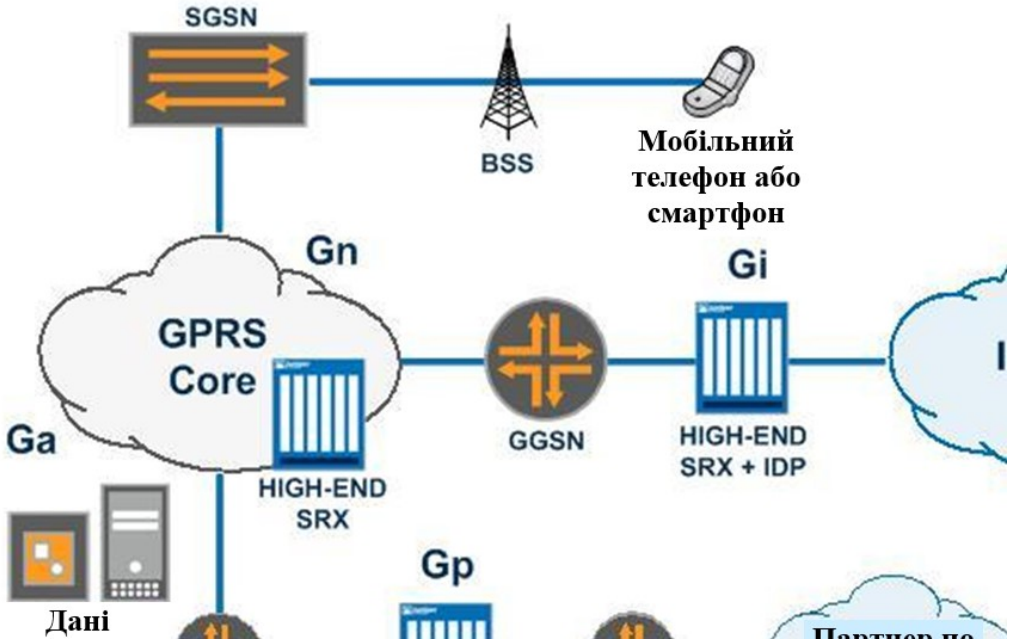

Рисунок 1 – Структурна схема системи

При впровадженні SRX важливо враховувати місце в топології GPRS-мережі.

Інтерфейс Gp

У даній точці важливо виділити сервіси, необхідні для взаємодії з роумінг-партнерами прямо або через GRX. У загальному випадку для підключення роумінг-абонента, необхідно забезпечити зв'язок локального SGSN і GGSN його оператора. Для встановлення такого підключення використовується GTP. Крім цього, між PLMN різних операторів повинні функціонувати мережні протоколи BGP і DNS (перетворення імен APN). Основні погрози на Gp інтерфейсі пов'язані з функціонуванням GTP. Для зменшення даних ризиків рекомендовано вживати наступних заходів:

- фільтрація вхідних/вихідних пакетів: запобігає обміну даними з невідомимим роумінг-операторами (при підключенні до GRX) і можливість спуфінг-атак від імені локальної PLMN;
- stateful-фільтрація GTP-пакетів: фільтрація GTP-сесій з невідомими PLMN для запобігання атак і розвантаження локальних GSN;
- обмеження смуги GTP: запобігання DoS-атак, виділення достатньої смуги для роботи GTP, BGP, DNS;
- установлення IPSec-тунелів з роумінгами-партнерами: забезпечення автентифікації й конфіденційності переданих даних;

− запобігання overbilling-атак: повідомлення Gi Firewall про “завислі” сесії для запобігання переплати абонента.

Інтерфейс Gn

Погрози можуть виходити як зсередини мережі оператора, так і бути спрямованими на устаткування мережі. Залежно від інтенсивності атаки можливий варіант тимчасового виводу з ладу устаткування мережі. Це у свою чергу виливається в простої, втрату сервісу, прибутки й невдоволення абонентів. Для усунення даних ризиків рекомендується використовувати політики розмежування доступу й фільтрацію пакетів на основі стану GTP-сесій. Наприклад, у випадку атаки із застосуванням підміни адреси GGSN, запит GTP PDP Context Delete буде відкинутий якщо перед цим не було GTP PDP Context Create повідомлення.

Інтерфейс Gi

Становить особливу небезпеку, хоч і не вимагає декапсуляції й контролю GTP. Основні механізми захисту включають:

− поділ логічних тунелів для підключення корпоративних клієнтів і впровадження IPSec у випадку використання каналів Інтернет;

− пріоритезація трафіку корпоративних користувачів і IPSec для недопущення можливості відмови каналів абонентів;

− інспектування пакетів з урахуванням стану сесій – використання політик розв'язне тільки ініціювання підключень із боку мобільних станцій;

− фільтрація вхідних/вихідних пакетів – запобігає можливість пересилання даних від IP-адрес мобільної станції, отриманих для виходу в Інтернет, на іншу мобільну станцію;

− запобігання overbilling-атак.

Також загальним підходом при реалізації механізмів безпеки в GPRS-мережах є використання часток IP-адрес для внутрішніх елементів інфраструктури мережі.

Функціонал для безпеки GTP включає:

1. GTP packet sanity check (перевірка заголовка кожного пакета GTP/UDP на відповідність стандарту).

2. GTP stateful inspection (перевірка GTP пакетів на відповідність поточному стану GTP-тунелю в контексті передачі попередніх пакетів; при одержанні пакета не приналежному поточному стану GTP обміну, пристрій відкидає пакет).

3. GGSN redirection (функція перенапрямку запиту GTP PDP Context Create; у запиті вказуються IP-адреси інших GGSN, після чого GTP-U і GTP-C повідомлення посилають зазначеним IP).

4.Policy-based GTP inspection (обмеження доступу між різними PLMN на основі визначення політик безпеки шляхом асоціації PLMN із зонами безпеки).

5. GTP message length filtering (фільтрація GTP-пакетів, що не відповідають мінімальній або максимальній довжині GTP-повідомлення).

6. GTP message type screening (фільтрація GTP-пакетів певного типу).

7. GTP IMSI prefix and APN filtering (фільтрація GTP-пакетів від невідомих PLMN на основі ідентифікатора мережі абонента (IMSI) і шляхи доступу абонента (APN)).

8. Removal of IEs of GTP R6 (функція видалення специфічних атрибутів 3GPP заголовки пакета GTP при наступній передачі в мережі 2GPP).

9. GSN rate limiting (зниження навантаження на GSN за допомогою обмеження швидкості обробки GTP-C пакетів).

10. GTP sequence number validation (функція перевірки порядкових номерів повідомлень G-PDU під час PDP-активації контексту).

11. Cleanup of hanging GTP tunnel (автоматичне видалення “висячих” GTP-тунелів).

12. GTP traffic logging (функція протоколювання GTP-пакетів на основі статусу (forwarded, prohibited, rate-limited, state-invalid, tunnel-limited))

13. GTP tunnel failover for high availability (функція підтримки активних GTP-сесій у режимі відказостійкості).

Переваги:

1. Модульна архітектура.

2. Можливість гнучкого масштабування.

3. Функціонал повноцінного маршрутизатора, фаєрволу, системи запобігання вторгнень і UTM (антивірус, антиспам, веб-фільтр, контент-фильтр).

4. Повна підтримка GTP і механізмів забезпечення його безпеки.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

– Досліджена система захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

– На основі отриманих результатів досліджень створена програмна реалізація системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.Розроблені алгоритми дозволяють успішно вирішувати завдання захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. 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. 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.
2. 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.
3. 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
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
17. 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
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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,
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.