УДК 004.891

к.т.н., доц. **Джулій В.М.** (ХмНУ)
Лєнков О.С. (ПФ «Арій»)
Ряба Л.О. (ВІКНУ)

МОДЕЛІ ТА АЛГОРИТМИ ВИЯВЛЕННЯ АТАК В БЕЗДРОТОВИХ МЕРЕЖАХ ПЕРЕДАЧІ ДАНИХ

В статті запропоновано комплекс системних моделей процесу функціонування виявлення атак в складі інформаційної системи, заснованих на методології IDEF0 і IDEF1X, що дозволяють деталізувати процес виявлення атак в бездротових мережах і інтегрувати систему виявлення атак з компонентами інтегрованої системи захисту інформації в організації з урахуванням вимог нормативних документів.

Бездротові мережі передачі даних схильні, в тому числі з причини недосконалості протоколів, до різних типів атак. Для вирішення зазначених проблем забезпечення безпеки інформації в бездротових мережах запропоновано алгоритми виявлення атак на основі класифікуючої моделі з використанням методів інтелектуального аналізу даних, які на відміну від існуючих алгоритмів дозволяють підвищити точність виявлення атак і знизити кількість помилкових спрацьовувань за рахунок попереднього навчання і донавчання системи на даних реального мережевого трафіку. Для оцінки ефективності алгоритмів пропонується їх апробація методом імітаційного моделювання. Аналіз запропонованих алгоритмів дозволяє зробити висновок про їх застосовності в складі системи виявлення атак, які становлять ядро бази знань бездротової системи виявлення атак.

Широке розповсюдження бездротових локальних мереж та їх застосування в корпоративних інформаційних системах призводить до необхідності приділяти активну увагу вирішенню притаманних їм проблем інформаційної безпеки. При цьому існуючі засоби захисту, в тому числі комерційні бездротові системи виявлення атак, не забезпечують повноцінного захисту від зловмисної активності. Запропонована архітектура інтелектуальної системи виявлення бездротових атак, яка функціонує на основі розроблених алгоритмів виявлення атак і їх об'єднання в ансамбль, застосування яких дозволяє з більш високою точністю і повнотою виявляти і блокувати атаки на бездротовий компонент інформаційної системи.

Ключові слова: бездротові мережі, моделі, алгоритми, ефективність виявлення атак, метод, мережевий трафік, інформаційна безпека.

Вступ. В останні роки атаки на бездротові локальні мережі стали звичайним явищем. За статистичними даними було виявлено та заблоковано понад 6,1 млрд шкідливих атак на комп'ютери і мобільні пристрої користувачів. Всього за останні п'ять років число мережевих атак зросла в 4,7 рази. Звичайні користувачі і невеликі організації, як правило, обмежуються використанням антивірусного програмного забезпечення, яке на сучасному етапі розвитку має ряд додаткових модулів захисту (вбудовані міжмережеві екрани, перевірка електронної пошти і т.д.). На даний момент в якості основних методів злому Wi-Fi застосовуються атака по словниках паролів і перебір паролів методом «грубої сили». Для цього бездротовий мережевий адаптер переводиться в режим моніторингу, сканується трафік і зберігаються необхідні пакети. Далі здійснюється деаутентифікація клієнта мережі або очікується момент підключення нового користувача з метою захоплення кадрів, що містять аутентифікаційну інформацію, після чого вже в оффлайн режимі за допомогою спеціальної програми підбирається пароль. Для прискорення підбору може використовуватися обчислювальна потужність графічного процесора.

Широке поширення Wi-Fi мереж призвело до спроби зробити налаштування простішої бездротової мережі для людей, що не володіють навичками комп'ютерної грамотності. Результатом стала технологія Wi-Fi Protected Setup (WPS). WPS автоматично призначає ім'я мережі і включає шифрування для захисту бездротової мережі від несанкціонованого доступу, при цьому немає необхідності вручну налаштовувати кожен параметр. WPS реалізується на більшості вироблених в даний час бездротових точках доступу, включаючи Cisco, Linksys,

Zyxel, D-Link і Netgear. Крім того, на багатьох пристроях дана функція включена за замовчуванням.

Однак реалізація ідеї використання WPS має недолік, який дозволяє зловмисникові виконати атаку шляхом підбору PIN-коду, за яким відбувається аутентифікація користувача. Хоча довжина PIN-коду складається із 8 цифр, він розділений на дві половини, причому остання цифра є контрольною сумою коду. Це зменшує максимально можливу кількість спроб аутентифікації, необхідних для підбору PIN-коду. Підбір PIN-коду дає атакуючому повний доступ до мережі, проте, якщо точка доступу транслює в двох діапазонах частот одночасно, то його знання дозволяє відновити всі ключі WPA.

З вищесказаного можна зробити висновок, що налаштування параметрів бездротового підключення повинно проводитися вручну грамотним фахівцем і відповідно до інструкцій та рекомендацій виробників обладнання.

Питання захищеності бездротових локальних мереж на даний момент залишаються відкритими. Основні проблеми захисту інформації в безпровідних мережах полягають в наступному: поширення сигналу за межі контрольованої зони; легкий доступ зловмисника до бездротового каналу передачі в порівнянні з кабельними мережами; використання вразливостей протоколів і методів аутентифікації; відсутність повноцінного захисту від атак при випуску доповнень до стандартів; можливі помилки в налаштуванні різних компонентів бездротової мережі.

Постановка задачі. Для організації безпечного функціонування бездротової корпоративної мережі необхідно вибудувати систему багаторівневого захисту. Дана система включає в себе наступні рубежі (заходи): захист периметра бездротової мережі: точок доступу і пристроїв користувачів; забезпечення безпеки сеансів зв'язку: застосування надійних методів аутентифікації, стійких алгоритмів шифрування тощо; постійний моніторинг радіоефіру, включаючи фізичний рівень, виявлення і аналіз підозрілої активності.

Для вирішення зазначених проблем забезпечення безпеки інформації в бездротових мережах використовуються як технічні засоби захисту, так і організаційні заходи. Технічні засоби захисту по об'єкту застосування можна розділити на три основні групи: засоби захисту бездротової мережі в цілому; засоби захисту на точці бездротового доступу; засоби захисту на стороні користувача (клієнта).

Тонке і грамотне налаштування пристроїв, застосування сучасних найбільш захищених протоколів дозволяє знизити ймовірність реалізації загроз. Однак і вони мають свої недоліки, наприклад, відсутність в технології WPA 2 аутентифікації запитів на дисоціацію і деаутентифікацію, в результаті чого з'являється можливість реалізації атаки роз'єднання абонентів та подальшого впровадження помилкового об'єкта мережі.

Класичні засоби захисту безсилі проти принципово нових класів бездротових загроз. При цьому необхідно не тільки захищати свою мережу і своїх користувачів, але і не можна порушувати функціонування бездротових мереж сусідів.

Широке поширення бездротових локальних мереж і застосування їх в корпоративних інформаційних системах призводить до необхідності приділяти активну увагу вирішенню властивих їм проблем інформаційної безпеки. При цьому існуючі засоби захисту, в тому числі комерційні бездротові системи виявлення атак, не забезпечують повноцінного захисту від шкідливої мережевої активності.

Основна частина. Для успішного аналізу особливостей функціонування системи виявлення атак і ступеня її впливу на об'єкт, що захищається, необхідно скласти її формалізований опис у вигляді функціональної моделі. Для вирішення цих цілей використано системне моделювання за методологією IDEF0, яка дозволяє побудувати функціональні моделі, що відображають структуру і функції проектованої системи, а також потоки матеріальних об'єктів і інформації, що зв'язують ці функції. Методологія заснована на графічному підході до опису (моделювання) систем SADT (System Analysis and Design Technique), для якої характерно: графічне представлення блокового моделювання: функція відображається у вигляді блоку, а інтерфейси входу/виходу представляються дугами, що

входять в блок і виходять з нього відповідно; опис взаємодії блоків між собою за допомогою інтерфейсних дуг, що виражають "обмеження", які, в свою чергу, встановлюють, коли і яким чином функції виконуються й управляються; обмеження на кожному рівні декомпозиції кількості блоків (3-6); взаємозв'язок діаграм через номери блоків; відсутність повторюваних найменувань, унікальність міток; синтаксичні правила для блоків і дуг; розділення вхідних (оброблюваних) і керуючих даних; відсутність впливу організаційної структури на функціональну модель.

Результатом використання методології SADT є функціональна модель, що складається з діаграм, текстових фрагментів і глосарію, пов'язаних між собою посиланнями. Головними компонентами моделі є діаграми, всі функції і інтерфейси на яких представлені у вигляді блоків і дуг. Точка з'єднання дуги з блоком визначає тип інтерфейсу: керуюча інформація входить в блок зверху; інформація, що обробляється відображається з лівого боку блоку; результати виконання функції показуються з правого боку блоку; механізм (автоматизована система або людина), що виконує операцію, представляється у вигляді дуги, що входить в блок знизу.

Модель IDEF0 являє собою сукупність ієрархічно впорядкованих і взаємопов'язаних діаграм. Так як система виявлення атак є складовою частиною інформаційної системи, то моделювання необхідно починати з неї.

На рис. 1 представлена функціональна модель інформаційної системи. В процесі роботи інформаційна система може піддаватися різним загрозам (атакам).

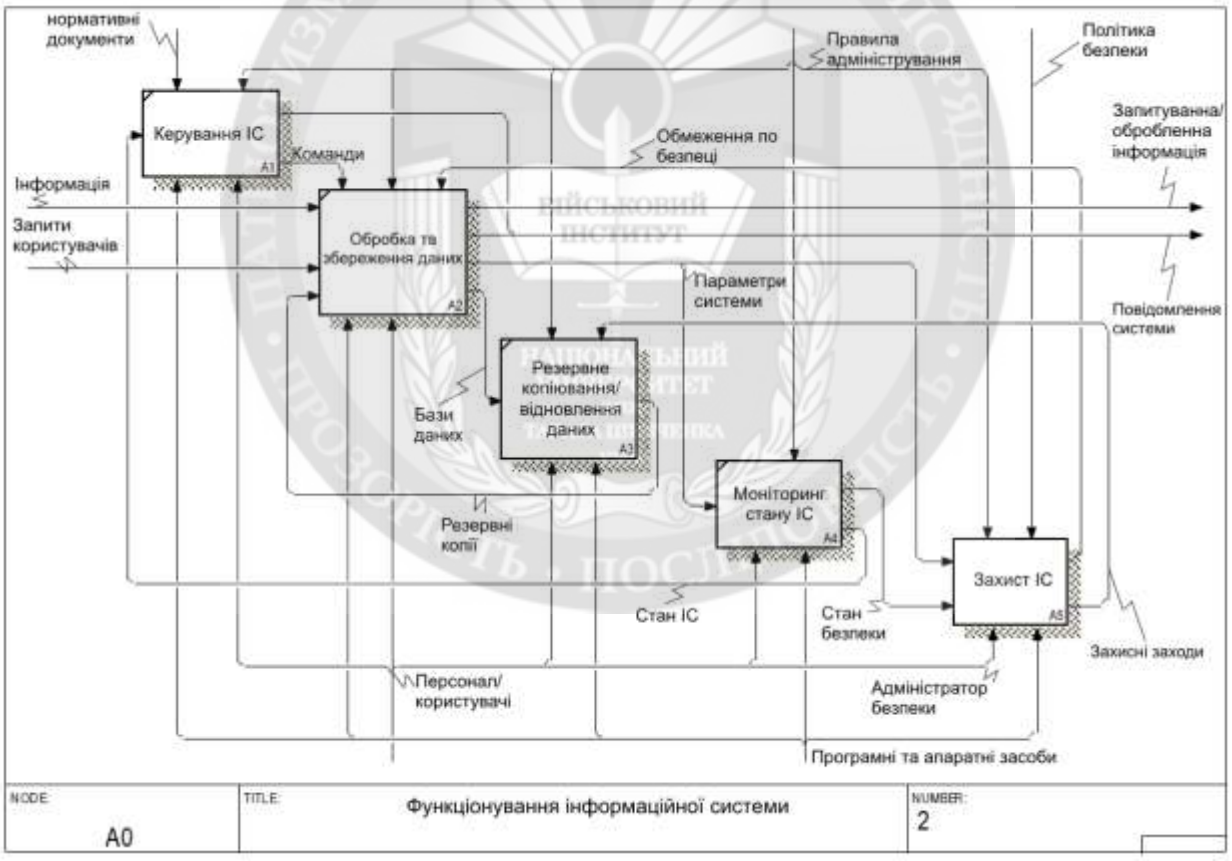

Рис. 1. Функціональна модель інформаційної системи

Як механізми (ресурси) для функціонування ІС виступають програмні та апаратні засоби і персонал організації. Управління здійснюється за допомогою команд адміністраторів на основі нормативних документів, правил та інструкцій, а також положень політики безпеки. Результатом функціонування ІС є оброблена інформація або інші повідомлення, що виробляються в процесі функціонування системи.

Робота інформаційної системи, відповідно до функціональної моделі (рис. 1) здійснюється за рахунок виконання відповідних функцій наступними підсистемами: підсистема управління ІС: здійснює налаштування і управління компонентами ІС; підсистема обробки та зберігання даних: забезпечує збір, обробку, зберігання і видачу інформації; підсистема резервного копіювання даних: здійснює створення копій баз даних та їх відновлення у випадку збоїв і реалізації інформаційних загроз; підсистема моніторингу стану ІС: призначена для перевірки коректності роботи компонентів ІС; підсистема захисту ІС: реалізує захист ІС від атак відповідно до політики безпеки.

На практиці склад підсистеми захисту може різнитися залежно від конкретної реалізації, виду економічної діяльності та організаційно-правової форми організації і відповідних вимог щодо інформаційної безпеки нормативних документів регуляторів. При цьому деякі компоненти підсистеми часто реалізують цілий набір функцій захисту, наприклад, антивірусне програмне забезпечення включає в себе також засоби контролю цілісності, аналізу системних подій і персональний фаєрвол.

На рис. 2 представлена функціональна модель підсистеми захисту інформації.

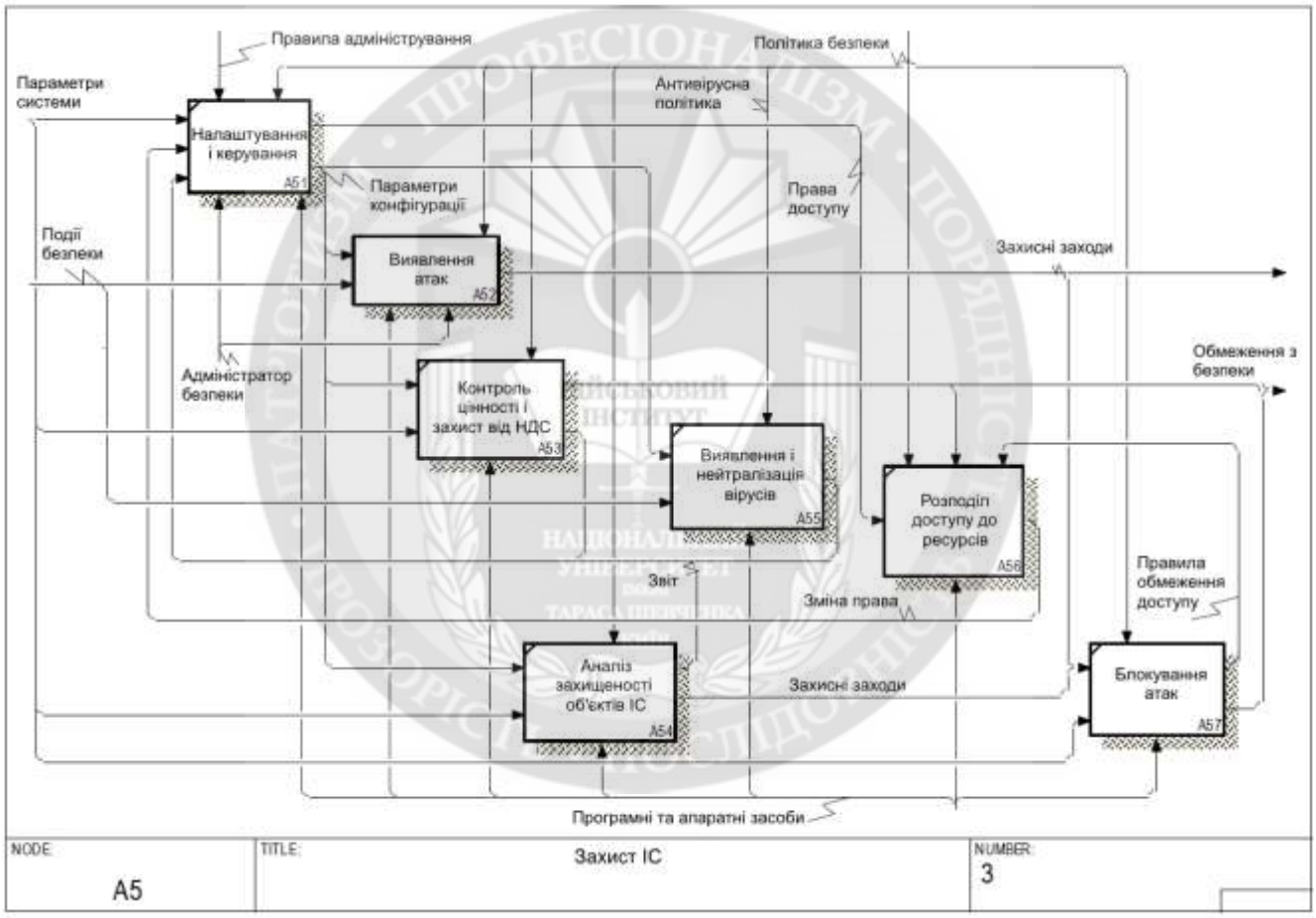

Рис. 2. Функціональна модель підсистеми захисту інформації

Функціональна модель підсистеми захисту інформації містить наступні компоненти: консоль управління для налаштування і керування компонентами системи захисту; система виявлення атак: проводить аналіз події безпеки на предмет наявності шкідливої активності; система контролю цілісності і захисту від несанкціонованого доступу: забезпечує контроль цілісності інформаційних об'єктів обчислювальної системи, контроль доступу до пристроїв і ресурсів, ідентифікацію, аутентифікацію користувача і реєстрацію його дій в системі; засіб аналізу захищеності об'єктів ІТ: виконує сканування об'єктів ІТ-інфраструктури на предмет наявності вразливостей; засіб виявлення і нейтралізації вірусів; система управління доступом: забезпечує функції налаштування та контролю доступу до даних і компонентів ІС; засоби

блокування атак: здійснюють блокування виявлених атак за допомогою захисних заходів (міжмережеві екрани, керовані мережеві комутатори і маршрутизатори, виділені бездротові пристрої тощо).

На рис. 3 представлена функціональна модель системи виявлення атак (СВА). Система включає в себе наступні компоненти: сенсори: здійснюють збір і первинну обробку даних про стан безпеки бездротової локальної мережі; консоль управління: призначена для налаштування адміністратором безпеки параметрів СВА; модуль навчання (донавчання) СВА: виконує побудову класифікуючої моделі на етапі навчання СВА, а також удосконалює модель в ході донавчання на реальній мережевій активності; база знань: містить сигнатури навчальної вибірки, побудовану класифікуючу модель, налаштування компонентів системи; модуль виявлення атак: проводить аналіз подій безпеки і на основі певних критеріїв (правил) класифікує шкідливу активність як атаку; модуль прийняття рішень: генерує запити / оповіщення на консоль і виробляє список захисних заходів для блокування атаки.

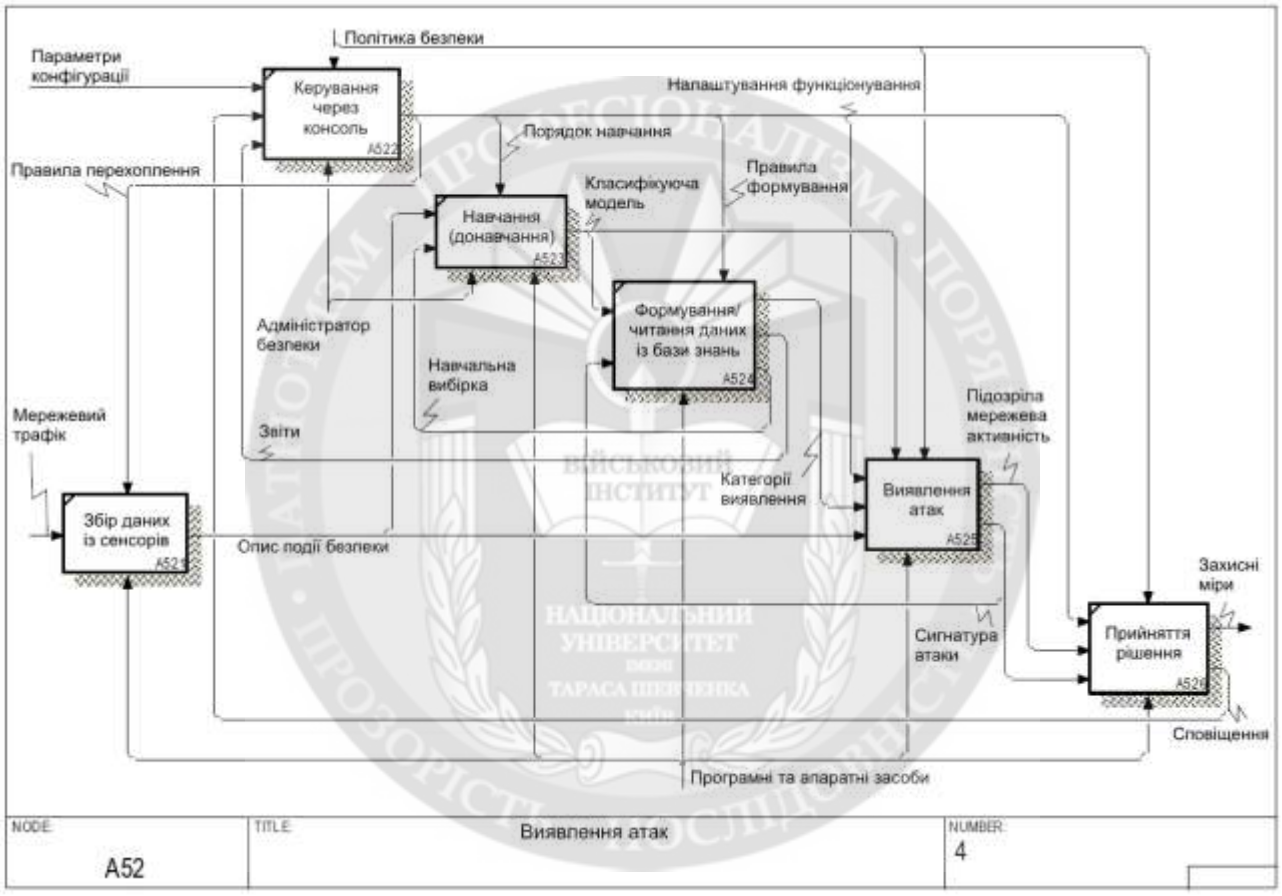

Рис. 3. Функціональна модель системи виявлення атак

Побудова функціональних моделей є обов'язковим етапом при проектуванні СВА, в ході якого розглянуті особливості технічної і програмної реалізації модулів і блоків, представлених на рис. 3. Склад пропонованої системи виявлення атак в бездротових мережах, в цілому, схожий зі структурою традиційних СВА, за винятком наявності модуля навчання (донавчання) системи і особливостей реалізації модуля виявлення атак. Крім того, в ході проектування виникає важливе завдання по вибору вектора ознак, специфічних для бездротових мереж, для детального опису подій безпеки. Побудова розглянутих функціональних моделей дозволяє визначити роль СВА в структурі ІС, яка полягає у виявленні загроз безпеки бездротової корпоративної мережі. На основі побудованих моделей отримано представлення про структуру СВА, склад і функції її компонентів, а також про взаємозв'язки між ними.

Для виявлення бездротових атак, на основі побудованих функціональних моделей розроблені відповідні алгоритми виявлення атак в локальній бездротовій мережі (рис. 4).

На першому етапі роботи алгоритму формуються масиви для запису прослуханих в ефірі кадрів F і виділених з них параметрів P, а також масив P_{em}, в якому зберігаються еталонні значення параметрів, виміряні в режимі навчання СВА. Також формуються масив T, в який записується статистика мережевої активності на заданому інтервалі часу Δt, масив даних про активні бездротові точки доступу M і заповнюється перелік інформації про довірених корпоративних точках доступу M_{em}: MAC-адреса, номер займаного радіоканалу, дозволені до використання протоколи шифрування і аутентифікації тощо.

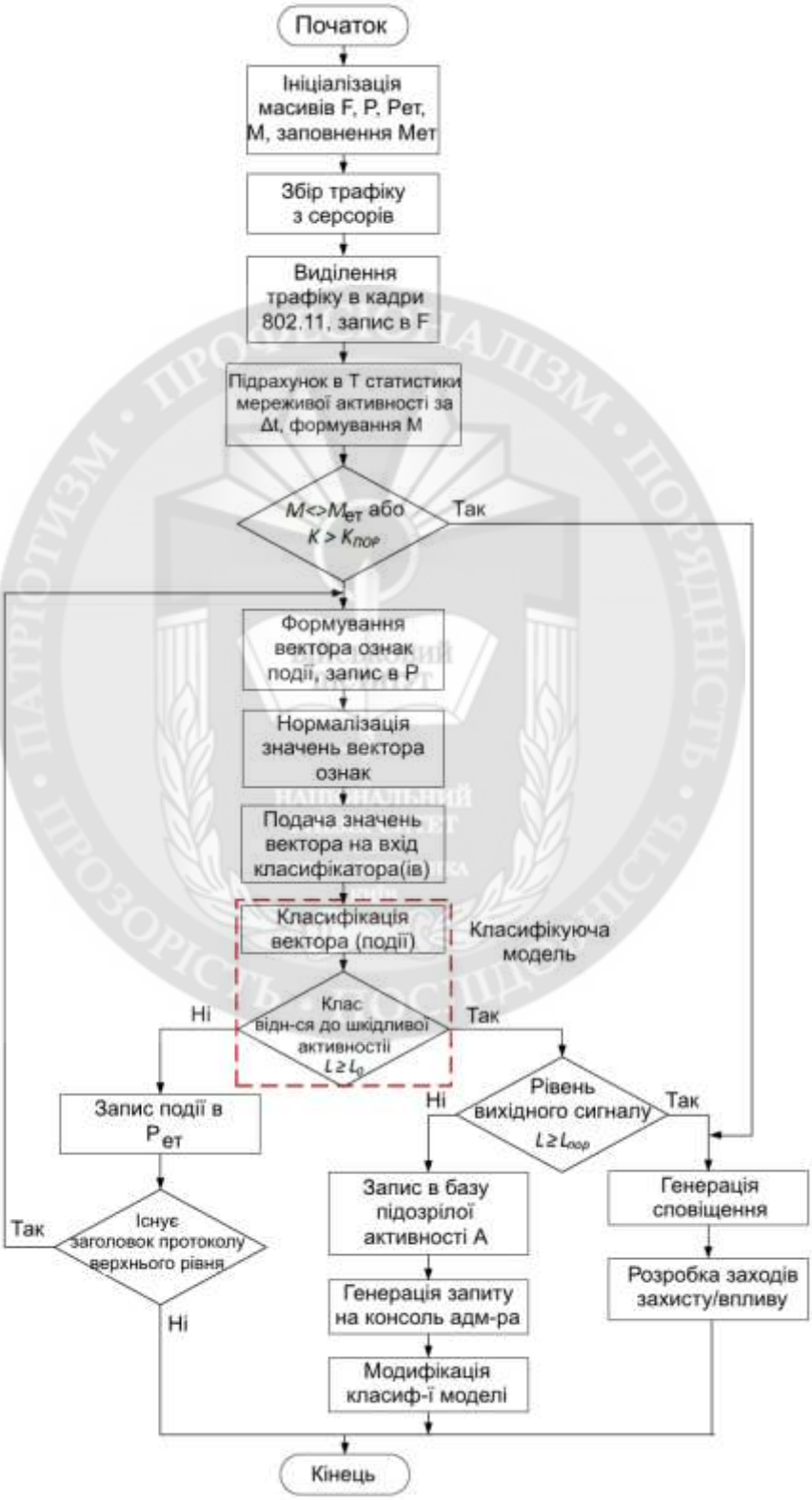

Рис. 4. Алгоритм виявлення бездротових мережевих атак

Наступним етапом є збір даних з сенсорів, їх первинний аналіз з метою виділення трафіку в окремі кадри формату 802.11 і збереження їх в масив *F*. Далі здійснюється формування векторів ознак подій і запис їх в масив *P*, нормалізація значень ознак і подача *P* на вхід класифікатора модуля виявлення атак. Відповідний блок виробляє класифікацію подій безпеки на базі класифікуючої моделі, що представляє собою набір вирішальних правил, неявно порівнюючи значення ознак з відповідними значеннями в масиві P_{em}. При виявленні відповідності вектора ознак якому-небудь типу шкідливої активності проводиться аналіз рівня вихідного сигналу класифікатора *L*. У разі досягнення або перевищення порогового рівня сигналу $L_{пор}$ інформація про подію передається в модуль прийняття рішень, який генерує оповіщення на консоль адміністратора, а також на підставі встановлених налаштувань розробляє заходи захисту або впливу на пристрій зловмисника. В іншому випадку аналізований вектор ознак події зберігається в базі підозрілої активності *A* для подальшого аналізу методами інтелектуального аналізу даних. Після досягнення потрібної кількості однотипних подій генерується запит на консоль адміністратора, який визначає наявність або відсутність шкідливої активності в даних подіях. На підставі його рішення проводиться модифікація класифікуючої моделі (донавчання) і додавання записів про події в базу сигнатур *S*.

Крім того, для виявлення окремих типів атак в масиві *T* набирається статистика кількості кадрів певного типу на заданому інтервалі часу Δt з однаковими значеннями параметрів: «Тип кадру», «Адреса джерела», «Адреса одержувача» і ін., а також типами протоколів верхнього рівня з числа використовуваних стандартних. Додатково в процесі функціонування СВА проводиться поповнення масиву даних про активні бездротові точки доступу *M*. При перевищенні порогового значення $K_{пор}$ кількості кадрів *K* однакового типу генерується оповіщення на консоль адміністратора про можливу DoS-атаку для подальшого виявлення і фізичного усунення її джерела. При розбіжності даних масиву *M* з заданими значеннями M_{em} генерується оповіщення про помилковий пристрій в радіоефірі.

Побудова класифікуючої моделі відбувається на стадії навчання системи виявлення атак. Для навчання СВА необхідна навчальна вибірка, що складається із записів про поточні бездротові з'єднаннях. Кожне з'єднання має характерний набір ознак (вхідних параметрів) і присвоєну мітку класу. Основу запропонованої архітектури інтелектуальної системи виявлення атак становить модульна схема організації взаємодії між компонентами з виділеної підсистемою сенсорів і централізованим управлінням через консоль адміністратора. Архітектура системи виявлення атак представлена на рис. 5.

Відмінною особливістю пропонованої архітектури є наявність модуля навчання (донавчання) системи і технологія реалізації модуля виявлення атак, заснована на застосуванні алгоритмів на базі методів ІАД. Таким чином, СВА, що класифікує модель, яка будується на основі сигнатур навчальної вибірки, має можливість навчатися в процесі роботи на реальному мережевому трафіку, що дозволяє виявляти з самого початку невідомі системі модифікації атак.

Проектована система виявлення атак складається з наступних компонентів: сенсори: здійснюють збір і первинну обробку даних про мережеву активність; модуль навчання (донавчання): виконує побудову класифікуючої моделі на етапі навчання системи, а також удосконалює модель в ході донавчання на реальній мережевій активності; база знань: містить сигнатури навчальної вибірки, побудовані класифікуючі моделі, налаштування компонентів системи; модуль виявлення атак: проводить аналіз подій безпеки і на основі критеріїв класифікує шкідливу активність як атаку; модуль прийняття рішень: генерує запити / оповіщення на консоль і виробляє список захисних заходів для блокування атаки; модуль реагування: сторонні засоби адміністрування локальних і мережевих програмних і апаратних засобів; консоль управління: призначена для налаштування адміністратором безпеки параметрів системи виявлення атак.

Сенсори, встановлені поблизу точок доступу, захищають бездротову мережу, перехоплюють мережевий трафік, формують події безпеки і пересилають їх в модуль виявлення атак. В якості сенсорів використовуються програми-агенти на виділених пристроях з бездротовим мережним адаптером в режимі моніторингу. Кожному сенсору присвоюється унікальний ідентифікатор (ID). Функції збору і генерації мережевого трафіку виконуються за допомогою динамічно підключеної бібліотеки, що реалізує стандартний інтерфейс прикладного програмування.

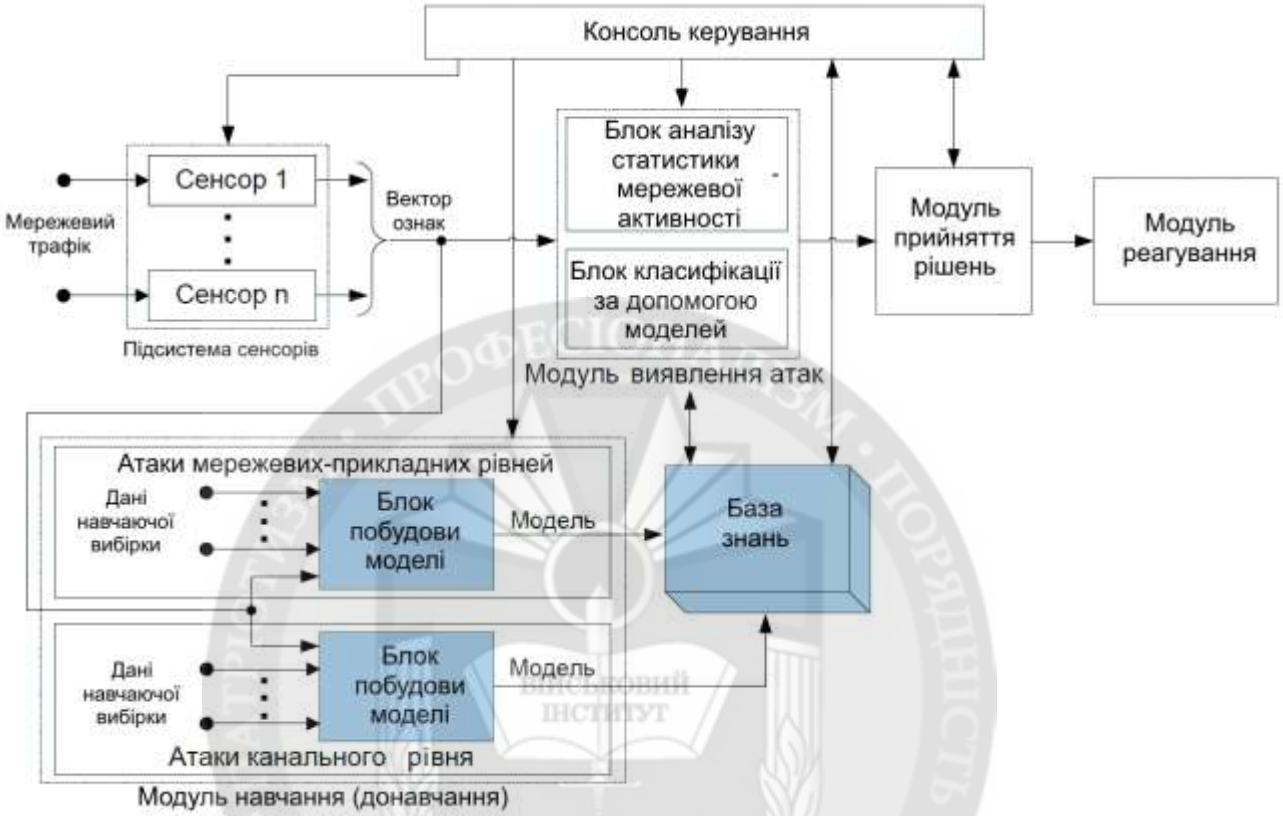

Рис. 5. Архітектура системи виявлення атак

Основою для виявлення атак є база знань, яка містить сигнатури відомих системі типів атак, ознаки, що вказують на прояв шкідливої активності, архів подій безпеки, а також параметри функціонування всіх компонентів СВА. Практична реалізація бази являє собою клієнт-серверну реляційну СУБД, реалізовану на окремому сервері або у вигляді кластера. Структура бази даних системи виявлення атак відображена в інформаційній моделі функціонування розробленого прототипу, побудованої за методологією IDEF1X.

Висновки. Широке розповсюдження бездротових локальних мереж та їх застосування в корпоративних інформаційних системах призводить до необхідності приділяти активну увагу вирішенню притаманних їм проблем інформаційної безпеки. Запропонований комплекс системних моделей процесу функціонування виявлення атак в складі інформаційної системи, заснованих на методології IDEF0 і IDEF1X, дозволить деталізувати процес виявлення атак в бездротових мережах і інтегрувати систему виявлення атак з компонентами інтегрованої системи захисту інформації в організації з урахуванням вимог нормативних документів. Запропоновані алгоритми виявлення атак в бездротовій мережі на основі застосування класифікуючої моделі з використанням методів інтелектуального аналізу даних, які на відміну від існуючих алгоритмів, дозволяють підвищити точність виявлення атак і знизити кількість помилкових спрацьовувань за рахунок попереднього навчання і донавчання системи на даних реального мережевого трафіку. Архітектура інтелектуальної системи виявлення бездротових атак, що функціонує на основі розроблених алгоритмів, дозволяє з більш високою точністю і повнотою виявляти і блокувати атаки на бездротовий компонент інформаційної системи.

ЛІТЕРАТУРА:

1. Васильев В.И. Интеллектуальные системы защиты информации: учеб. пособие / В. И. Васильев . – 2-е изд., испр. – М.: Машиностроение, 2012. – 171 с.

2. Гордейчик С.В.. Безопасность беспроводных сетей. / С.В. Гордейчик, В.В. Дубровин – М.: Горячая линия – Телеком, 2008. – 288 с.

3. Гузаиров М.Б., Машкина И.В. Управление защитой информации на основе интеллектуальных технологий: учебное пособие. / М.Б. Гузаиров, И.В. Машкина– М.: Машиностроение, 2013. – 241 с.

4. Лєнков С.В. Концептуальна схема системи інтелектуальної обробки даних / С.В. Лєнков, В.М. Джулій, О.М. Горбатюк, Н.М. Берназ // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2014. – Вип. № 46. – С.181-190

5. Лєнков С.В. Аналіз існуючих методів та алгоритмів виявлення атак в бездротових мережах передачі даних / С.В. Лєнков, В.М. Джулій, Н.М. Берназ, С.О. Божук // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 56. – С.124-132

6. Лєнков Є.С., Зайцев Д.В., Муляр І.В., Михалечко Р.М. Формування топології бездротової ad hoc мережі спеціального призначення на основі динаміки подвійних найкращих відповідей / Є.С. Лєнков, Д.В. Зайцев, І.В. Муляр, Р.М. Михалечко // Системи обробки інформації. – Харків, 2016. – Випуск 9 (146). – С 172-176.

7. Таненбаум Э. Компьютерные сети. 5-е изд. / Э.Таненбаум, Д. Уэзеролл– СПб.: Питер, 2012. – 960 с.

8. Ефимова, Л.Л. Информационная безопасность сетей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.

9. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.

10. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.

11. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.

12. Айвенс К. Компьютерные сети. Хитрости. / К.Айвенс – СПб.: Питер, 2006. – 298 с.ил.

13. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие. / В. И Завгородний. – М.: Логос; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.: ил.

14. Галатенко В.А. Основы информационной безопасности : курс лекций : учебное пособие / Издание третье / В.А. Галатенко Под ред. Академика РАН В.Б. Бетелина / - М.:ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. - 208 с.

15. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

REFERENCES:

1. Vasilev V.I. Intellektualnyie sistemyi zaschityi informatsii: ucheb. posobie / V. I. Vasilev . – 2-e izd., ispr. – M.: Mashinostroenie, 2012. – 171 s.

2. Gordeychik S.V.. Bezopasnost besprovodnyih setey. / S.V. Gordeychik, V.V. Dubrovin – M.: Goryachaya liniya – Telekom, 2008. – 288 s.

3. Guzairov M.B., Mashkina I.V. Upravlenie zaschitoy informatsii na osnove intellektualnyih tehnologiy: uchebnoe posobie. / M.B. Guzairov, I.V. Mashkina– M.: Mashinostroenie, 2013. – 241 s.

4. Lenkov S.V. Kontseptualna shema sistemi Intelektualnoyi obrobki danih / S.V. Lenkov, V.M. Dzhuliy, O.M. Gorbatyuk, N.M. Bernaz // Zbirnik naukovih prats Viyskovogo Institutu Kiyivskogo natsionalnogo universitetu imeni Tarasa Shevchenka. – K.: VIKNU, 2014. – Vip. No 46. – S.181-190

5. Lenkov S.V. AnalIz Isnuyuchih metodiv ta algoritmiv viyavlennya atak v bezdrotovih merezhah peredachI danih / S.V. Lenkov, V.M. Dzhuliy, N.M. Bernaz, S.O. Bozhuk // Zbirnik naukovih prats Viyskovogo Institutu Kiyivskogo natsionalnogo universitetu imeni Tarasa Shevchenka. – K.: VIKNU, 2017. – Vip. No 56. – S.124-132

6. Lenkov Ye.S., Zaytsev D.V., Mulyar I.V., Mykhalechko R.M. Formuvannya topolohiyi bezdrotovoyi ad hoc merezhi spetsial'noho pryznachennya na osnovi dynamiky podviynykh naykrashchykh vidpovidey / Ye.S. Lenkov, D.V. Zaytsev, I.V. Mulyar, R.M. Mykhalechko // Systemy obrobky informatsiyi. – Kharkiv, 2016. – Vypusk 9 (146). – S 172-176.

7. Tanenbaum E. Kompyuternyie seti. 5-e izd. / E.Tanenbaum, D. Uezeroll– SPb.: Piter, 2012. – 960 s.

8. Efimova, L.L. Informatsionnaya bezopasnost setey. Rossiyskiy i zarubezhnyiy opyit: Monografiya / L.L. Efimova, S.A. Kocherga. - M.: YuNITI-DANA, 2013. - 239 s.

9. Partyika, T.L. Informatsionnaya bezopasnost: Uchebnoe posobie / T.L. Partyika, I.I. Popov. - M.: Forum, 2012. - 432 s.

10. Petrov, S.V. Informatsionnaya bezopasnost: Uchebnoe posobie / S.V. Petrov, I.P. Slinkova, V.V. Gafner. - M.: ARTA, 2012. - 296 s.

11. Shangin, V.F. Informatsionnaya bezopasnost kompyuternyih sistem i setey: Uchebnoe posobie / V.F. Shangin. - M.: ID FORUM, NITs INFRA-M, 2013. - 416 s.

12. Ayvens K. Kompyuternyie seti. Hitrosti. / K.Ayvens – SPb.: Piter, 2006. – 298 s.il.

13. Zavgorodniy V. I. Kompleksnaya zaschita informatsii v kompyuternyih sistemah: Uchebnoe posobie. / V. I Zavgorodniy. – M.: Logos; PBOYuL N. A. Egorov, 2001. – 264 s.: il.

14. Galatenko V.A. Osnovyi informatsionnoy bezopasnosti : kurs lektsiy : uchebnoe posobie / Izdanie trete / V.A. Galatenko Pod red. Akademika RAN V.B. Betelina / - M.:INTUIT.RU «Internet-universitet Informatsionnyih Tehnologiy», 2006. - 208 s.

15. Babash, A.V. Informatsionnaya bezopasnost. Laboratornyiy praktikum: Uchebnoe posobie / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2013. - 136 s.

Рецензент: д.т.н., доц., Боряк К.Ф., завідувач кафедри метрології та метрологічного забезпечення Одеської державної академії технічного регулювання та якості, директор науково-дослідного інституту проблем стандартизації, сертифікації та експериментальної метрології

к.т.н. Джулий В.Н., Ленков А.С., Рябая Л.О.

МОДЕЛИ И АЛГОРИТМЫ ОБНАРУЖЕНИЯ АТАК В БЕСПРОВОДНЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

В статье предложен комплекс системных моделей процесса функционирования обнаружения атак в составе информационной системы, основанных на методологии IDEF0 и IDEF1X, позволяющие детализировать процесс обнаружения атак в беспроводных сетях и интегрировать систему обнаружения атак с компонентами интегрированной системы защиты информации в организации с учетом требований нормативных документов.

Беспроводные сети передачи данных склонны, в том числе по причине несовершенства протоколов, к различным типам атак. Для решения указанных проблем обеспечения безопасности информации в беспроводных сетях предложены алгоритмы обнаружения атак на основе классифицирующей модели с использованием методов интеллектуального анализа данных, которые в отличие от существующих алгоритмов позволяют повысить точность обнаружения атак и снизить количество ложных срабатываний за счет предварительного обучения и обучению системы на данных реального сетевого трафика. Для оценки эффективности алгоритмов предлагается их апробация методом имитационного моделирования.

Анализ предложенных алгоритмов позволяет сделать вывод об их применимости в составе системы обнаружения атак, которые составляют ядро базы знаний беспроводной системы обнаружения атак. Широкое распространение беспроводных локальных сетей и их применение в корпоративных информационных системах приводит к необходимости уделять активное внимание решению присущих им проблем информационной безопасности. При этом существующие средства защиты, в том числе коммерческие беспроводные системы обнаружения атак, не обеспечивают полноценной защиты от злонамеренного активности.

Предложенная архитектура интеллектуальной системы обнаружения беспроводных атак, которая функционирует на основе разработанных алгоритмов обнаружения атак и их объединения в ансамбль, применение которых позволяет с более высокой точностью и полнотой выявлять и блокировать атаки на беспроводную компонент информационной системы.

Ключевые слова: беспроводные сети, модели, алгоритмы, эффективность обнаружения атак, метод, сетевой трафик, информационная безопасность.

Ph.D. in Technical Sciences Dzhuliy V.M., Lenkov A.S., Riaba L.O.

MODES AND ALAGORITHMS OF ATTACK DETECTION IN NETWORK NETWORKS OF DATA TRANSMISSION

A set of system models of the detecting attacks operation in the composition of the information system is proposed in the article. They are based on the IDEF0 and IDEF1X methodologies, which allow to detail the process of detecting attacks in wireless networks and integrate the system of attacks detection with the components of the integrated information security system in the organization, taking into account the requirements of normative documents.

Wireless data networks are vulnerable to various types of attacks due to imperfect protocols. In order to solve these problems of security of information in wireless networks, algorithms for detecting attacks based on a ranking model using data mining methods are proposed. They, unlike the existing algorithms, allow to increase the accuracy of detection of attacks and reduce the number of false positives by the previous training and training the system on the data of real network traffic. To evaluate the effectiveness of algorithms, testing them using simulation model is proposed. The analysis of the proposed algorithms allows us to conclude about their applicability in the system of detection of attacks, which constitute the core knowledge base wireless attack detection system.

The widespread use of wireless local area networks and their application in corporate information systems leads to the need to pay close attention to solving their information security problems. In this case, existing security features, including commercial wireless detection systems, do not provide full protection against malicious activity. The proposed architecture of intelligent detection system for wireless attacks, which operates on the basis of developed algorithms for detecting attacks and their integration into an ensemble, the application of which allows to detect and block attacks on the wireless component of the information system with greater accuracy and completeness.

Keywords: wireless networks, models, algorithms, attack detection efficiency, method, network traffic, information security.