УДК 004.891

к.т.н., доц. **Джулій В.М.** (ХмНУ)
к.т.н., доц. **Красильников С.Р.** (ХмНУ)
Божук С.О. (ХмНУ)

МЕТОДИ ТА АЛГОРИТМИ ВИЯВЛЕННЯ АТАК В БЕЗДРОТОВИХ МЕРЕЖАХ ПЕРЕДАЧІ ДАНИХ

У статті запропоновані алгоритми виявлення атак в бездротовій мережі на основі застосування класифікованої моделі.

Бездротове середовище передачі даних в силу своїх особливостей створює потенційні умови для прослуховування мережевого трафіку і неконтрольованого підключення до бездротової мережі зловмисників, які знаходяться в зоні її дії. 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 використовуються як технічні засоби захисту, так і організаційні заходи.

На теперішній час відсутні роботи по застосуванню методів інтелектуального аналізу даних в задачах виявлення атак на локальні бездротові мережі. У зв'язку з цим виникає проблема вибору оптимального вектора ознак, специфічних для подій безпеки в бездротових мережах, які будуть використовуватися в ході класифікації даних подій. Задача розробки алгоритмічного та програмного забезпечення системи, що дозволяє автоматизувати процес виявлення бездротових атак на основі застосування сучасних методів інтелектуального аналізу параметрів мережевого трафіку, є актуальною. 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.

Проведений аналіз загроз і їх джерел та побудова їх моделей, дозволяють більш точно оцінювати безпеку мережевої активності і рівень довіри до її джерела. Запропоновані алгоритми виявлення атак в бездротовій мережі на основі застосування класифікованої моделі з використанням технологій інтелектуального аналізу даних. Аналіз алгоритмів дозволяє зробити висновок про їх застосовності в складі системи виявлення атак.

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

Вступ. Бездротове середовище передачі даних в силу своїх особливостей створює потенційні умови для прослуховування мережевого трафіку і неконтрольованого підключення до бездротової мережі зловмисників, які знаходяться в зоні її дії.

На підставі проведеного аналізу проблем захисту інформації в бездротових мережах можна визначити перелік можливих загроз інформаційній системі організації. За видами можливих джерел загроз виділяють два класи загроз:

– загрози, пов'язані з навмисними або ненавмисними діями осіб, що мають доступ до інформаційної системи (внутрішній порушник);

– загрози, пов'язані з навмисними або ненавмисними діями осіб, які не мають доступу до інформаційної системи, що реалізують загрози з зовнішніх мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну (зовнішній порушник). Види порушників, характерних для інформаційної системи з заданими характеристиками і особливостями функціонування, виділяються на основі припущень про можливі цілі (мотивації) при реалізації загроз безпеці інформації цими порушниками. Цілями реалізації порушниками загроз безпеки інформації в інформаційній системі можуть виступати: а)нанесення збитків державі, окремим її сферам діяльності або секторам економіки; б)ідеологічні або політичні мотиви; в)організація терористичного акту; г)заподіяння майнової шкоди шляхом обману, зловживання довірою, шахрайства або іншим злочинним шляхом; д) дискредитація або дестабілізація діяльності органів державної влади, організацій; е)отримання конкурентних переваг; ж)впровадження додаткових функціональних можливостей в програмне забезпечення або програмно-технічні засоби на етапі розробки; з)цікавість або бажання самореалізації; і)виявлення вразливостей з метою їх подальшого продажу і отримання фінансової вигоди; к)реалізація загроз безпеці інформації з помсти; л)реалізація загроз безпеці інформації ненавмисно через необережність або некваліфікованих дій.

Постановка задачі. Бездротові мережі передачі даних схильні, в тому числі з причини недосконалості протоколів, до різних типів атак. Рядові користувачі і невеликі організації, як правило, обмежуються використанням антивірусного програмного забезпечення, яке на сучасному етапі розвитку має ряд додаткових модулів захисту. Великі підприємства змушені купувати дорогі системи виявлення та запобігання атакам.

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 точки бездротового доступу; засоби захисту на стороні користувача (клієнта).

Як було відзначено, в доступній літературі відсутні роботи по застосуванню методів інтелектуального аналізу даних в задачах виявлення атак на локальні бездротові мережі. У зв'язку з цим виникає проблема вибору оптимального вектора ознак, специфічних для подій безпеки в бездротових мережах, які будуть використовуватися в ході класифікації даних подій. Задача розробки алгоритмічного та програмного забезпечення системи, що дозволяє автоматизувати процес виявлення бездротових атак на основі застосування сучасних методів інтелектуального аналізу параметрів мережевого трафіку, є актуальною.

Основна частина. Основу функціонування бездротової системи виявлення атак становить класифікаційна модель, на базі якої приймається рішення про віднесення фрагмента мережевого трафіку до нормальної активності або до будь-якого типу атаки. Для організації безпечного функціонування корпоративної бездротової 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 і т. д.; постійний моніторинг радіоефіру, включаючи фізичний рівень, виявлення і аналіз підозрілої активності.

Умовою, що забезпечує можливість реалізації наведених загроз безпеки оброблюваної в системі інформації, можуть бути недоліки або слабкі місця в компонентах інформаційної системи, мережевих протоколах і програмному забезпеченні. Основою атак в бездротових мережах служить перехоплення мережевого трафіку від / до точки доступу або трафіку між двома підключеними станціями, а також впровадження додаткових (підроблених) даних в сеанс бездротового зв'язку. Атаки можуть бути спрямовані на різні об'єкти мережевої інфраструктури. Компоненти обміну даними в бездротовій локальній мережі та точки потенційних атак представлені на рис. 1.

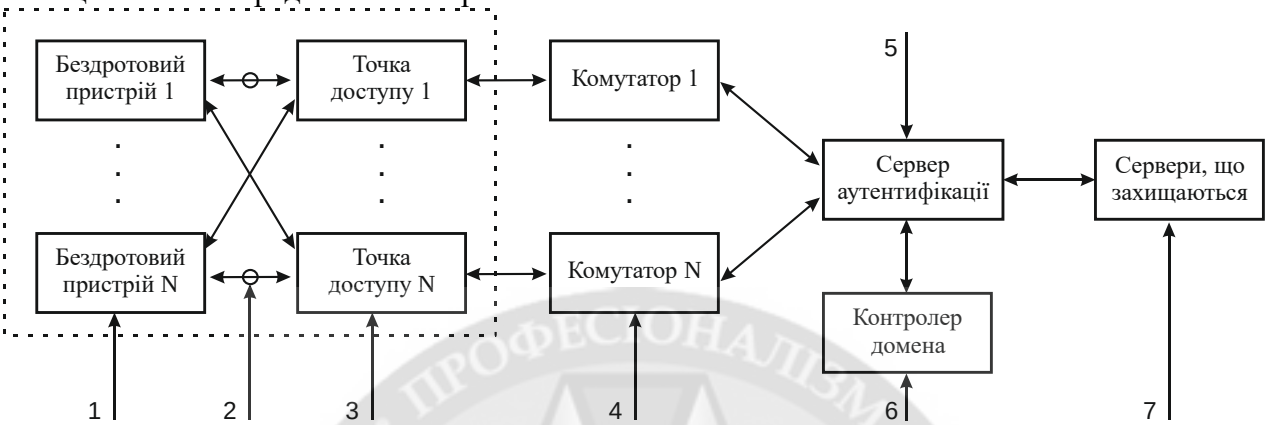

Рис. 1. Компоненти обміну даними через бездротову локальну мережу і точки атак

Окремим блоком виділені безпосередньо пристрої бездротового компонента інформаційної системи.

Атаки, групи 1, спрямовані безпосередньо на клієнтський пристрій (комп'ютер, ноутбук, мобільний пристрій). Точка атаки 2 - це бездротове середовище передачі. Пристрій користувача взаємодіє з однією з точок доступу, яка розташована на границі корпоративної мережі і схильна до атак 3. Наступним вузлом, який бере участь в обміні даними, є мережевий комутатор (точка атаки 4). Користувач отримує доступ до внутрішніх ресурсів інформаційної системи після аутентифікації на виділеному сервері (точка атаки 5), яка обмінюється інформацією про облікові дані користувачів з контролером домену (точка атаки 6). У разі співпадання наданих користувачем даних сервер аутентифікації направляє в точку доступу повідомлення про успішну аутентифікацію, яка, в свою чергу, надає доступ користувачеві до даних, розташованих на корпоративних серверах (точка атаки 7). Атаки можуть бути реалізовані на різних рівнях моделі OSI: прикладному, транспортному, мережевому, канальному і фізичному. Специфічними для бездротових мереж є фізичний і канальний рівні, на використанні яких заснований стандарт IEEE 802.11. Саме використання вразливостей протоколів і технологій цих рівнів є основою проведення атак на бездротову мережу і початковою стадією атак на інформаційну систему через несанкціоноване отримання доступу до бездротової мережі.

Для виявлення бездротових атак, розроблені відповідні алгоритми побудови класифікуємої моделі, що становить ядро бази знань бездротової системи виявлення атак, на основі: методу опорних векторів, методу k-найближчих сусідів, дерев прийняття рішень, а також нейронних мереж. На рис. 2 наведена узагальнена блок-схема алгоритму виявлення атак в локальній бездротовій мережі. На першому етапі формуються масиви для запису прослуханих в ефірі кадрів F і виділених з них параметрів P, а також масив Pет, в який зберігаються еталонні значення параметрів, виміряні в режимі навчання системи виявлення атак. Також формуються масив T, в який набирається статистика мережевої активності на заданому інтервалі часу Δt, масив даних про віщаючих бездротових точках доступу M і заповнюється перелік інформації про довірених корпоративних точках доступу Мет: MAC-адрес, номер займаного радіоканалу, дозволені до використання протоколи шифрування і аутентифікації і ін. Далі проводиться збір даних з сенсорів, їх первинний аналіз з метою

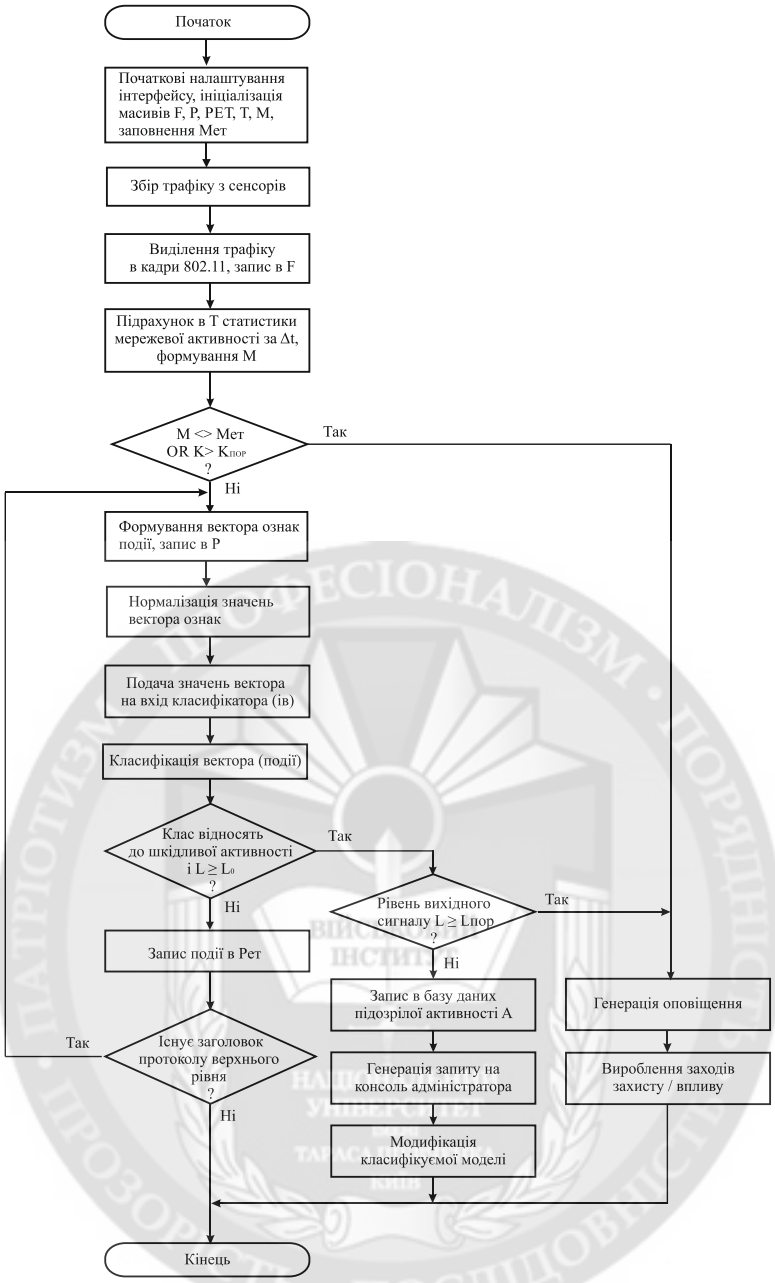

Рис. 2. Алгоритм виявлення бездротових мережевих атак

виділення трафіку в окремі кадри формату 802.11 і збереження їх в масив F. Потім 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 класифікуємої моделі, що представляє собою набір вирішальних правил, неявно порівнюючи значення ознак з відповідними значеннями в масиві Рет. 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 Lпор інформація про подію передається в модуль прийняття рішень, який генерує повідомлення на консоль адміністратора, а також на підставі встановлених налаштувань розроблює заходи захисту або впливу на пристрій зловмисника. В іншому випадку, якщо Lo ≤ L <Lпор, де Lo - мінімально допустимий рівень сигналу, що свідчить про підозрілу мережеву активність, то аналізований вектор ознак події зберігається в базі підозрілої активності A для подальшого аналізу. 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 класифікуємої моделі (до навчання) і додавання записів про події в базу сигнатур S. Крім того, для виявлення окремих типів атак в масив T набирається статистика кількості кадрів певного типу на заданому інтервалі часу Δt з однаковими значеннями параметрів «Тип кадру», «Адреса джерела», «Адреса одержувача» і ін. Додатково в процесі функціонування системи виявлення атак проводиться поповнення масиву даних про віщаючих бездротових точках доступу M. При перевищенні порогового значення Kпор 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 Мет генерується повідомлення про підозрілий пристрій в радіоефірі.

Побудова класифікуємої моделі відбувається на стадії навчання системи виявлення атак. Для навчання системи виявлення атак необхідна навчальна вибірка, що складається із записів про поточні бездротові мережеві з'єднання. Кожне з'єднання має характерний набір ознак (вхідних параметрів) і присвоєну мітку класу. На підставі проведеного аналізу про необхідність застосування інтелектуальних технологій виявлення атак в бездротових мережах розроблені алгоритми побудови класифікуємої моделі, що становлять ядро бази знань бездротової системи виявлення атак, на основі методу опорних векторів, k-найближчих сусідів, дерев прийняття рішень, а також нейронних мереж. На рис. 3 представлена схема побудови нейромережевої системи виявлення атак.

Рис. 3. Схема побудови нейромережевої системи виявлення атак

Величина сумарної квадратичної помилки навчання E розраховується за формулою:

$$E=\sum_{i=1}^{I}\sum_{k=1}^{n}\left[\varepsilon_k^{(i)}\right]^2=\sum_{i=1}^{I}\sum_{k=1}^{n}\left(y_k^{(i)}-S_k^{(i)}\right)^2,$$

де $y_k^{(i)}$ - вихідний сигнал *k*-го нейрона при обробці *i*-го запису, $S_k^{(i)}$ - бажане значення сигналу *k*-го нейрона згідно *i*-й сигнатурі, $\varepsilon_k^{(i)}$ - величина помилки *k*-го нейрона вихідного шару нейронної мережі. Для мінімізації квадратичної помилки використовується алгоритм градієнтного спуску, в ході якого кожна вага зв'язку між *j*-м і *l*-м нейронами W_{jl} змінюється на ΔW_{jl} після одного циклу навчання *n* зі швидкістю навчання *L*:

$$W_{jl}(n+1)=W_{jl}(n)+\Delta W_{jl}(n)=W_{jl}(n)-L\left(\frac{\partial E}{\partial W_{jl}}\right)_n.$$

На рис. 4 представлений алгоритм навчання нейронної мережі, використовуваний в якості базового компонента системи виявлення атак, методом зворотного поширення помилки на прикладі багатошарового персептрона.

Навчання нейронної мережі проводиться з учителем за наступним алгоритмом:

1. Проводиться введення параметрів навчання: Епор - порогове значення сумарної квадратичної помилки; N - кількість циклів навчання; M - момент навчання; L - швидкість навчання, і первинна ініціалізація ваг W зв'язків між нейронами.

2. З навчальної вибірки береться і = 1 зразок {вектор ознак, цільове значення} і значення його ознак подаються на вхідні нейрони.

3. Кожен вхідний нейрон передає отриманий сигнал всім нейронам в наступних шарах.

4. Виміряються сигнали, видані вихідними нейронами, і проводиться інтерпретація виданих сигналів, після чого за допомогою цільової функції обчислюється величина помилки ε для кожного нейрона, що характеризує відмінність між виданими мережею відповіддю і цільовим значенням, що містяться в зразку.

5. Якщо ε дорівнює нулю (або досить малому значенню), то це означає, що необхідна відповідність отриманого та відомого відповідей досягнуто. Інакше за допомогою ε обчислюються поправочні коефіцієнти для кожної синаптичної ваги зв'язків ΔW, після чого проводиться підстроювання синаптичних ваг.

6. Здійснюється перехід до наступного зразка вибірки, і повторюються перераховані вище кроки.

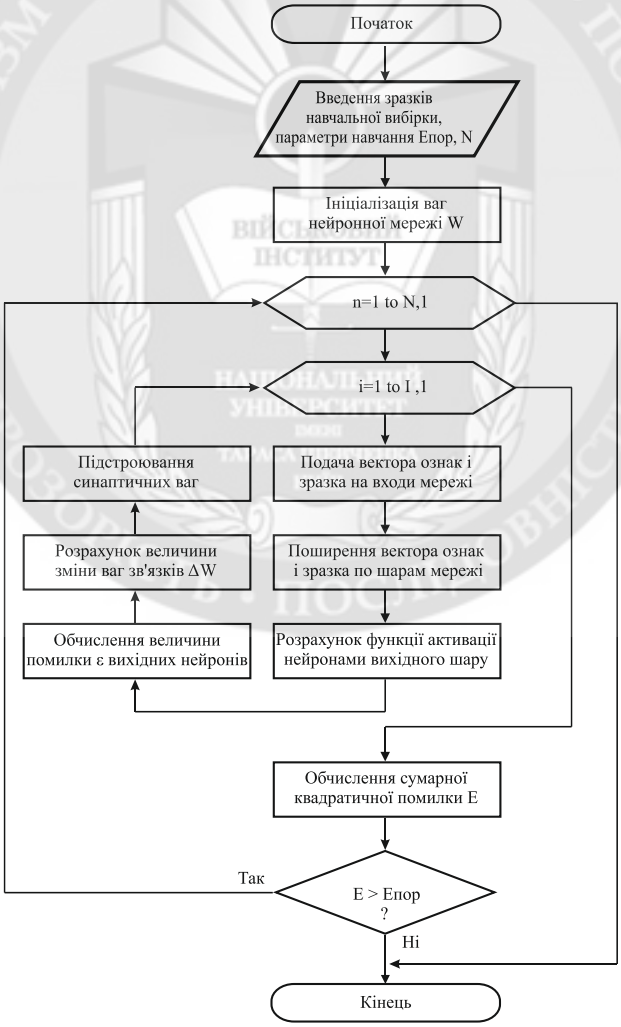

Рис. 4. Алгоритм навчання нейронної мережі

Прохід по всім зразкам навчальної вибірки вважається одним циклом навчання. Після проходження циклу обчислюється величина сумарної квадратичної помилки E і порівнюється з граничним значенням Епор. Алгоритм припиняє роботу при досягненні сумарної квадратичної помилкою порогового значення в ході процесу навчання або після виконання певної кількості ітерацій. На виході алгоритму формується класифікована модель.

Після побудови класифікованої моделі на стадії навчання, система виявлення атак переводиться в режим повнофункціональної роботи і на входи сенсорів подається реальний мережевий трафік. При цьому в міру функціонування відбувається донавчання системи виявлення атак при аналізі підозрілої мережевої активності. Таким чином, для виявлення атак в бездротової мережі розроблені алгоритми на основі технологій інтелектуального аналізу даних.

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. Проведений аналіз загроз і їх джерел та побудова їх моделей, дозволяють більш точно оцінювати безпеку мережевої активності і рівень довіри до її джерела. Запропоновані алгоритми виявлення атак в бездротової мережі на основі застосування класифікованої моделі з використанням технологій інтелектуального аналізу даних. Аналіз алгоритмів дозволяє зробити висновок про їх застосовності в складі системи виявлення атак.

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, О.М. Горбатюк, 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. Лукацкий А.В. Обнаружение атак. /А.В. Лукацкий – СПб.: БХВ-Петербург, 2003. – 608 с.

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. Vasiliev V.I. Intellectual protection of information: Textbook. allowance / V.I. Vasiliev. - 2 nd ed., Rev. - M .: Mechanical Engineering, 2012. - 171 p.

2. Gordeychik S.V. Safety of wireless networks. / S.V. Gordeychik, V.V. Dubrovin - M .: Hot line - Telecom, 2008. - 288 p.

3. Guzairov M.B., Mashkina I.V. Managing the protection of information based on intelligent technology: a tutorial./M.B. Guzairov, I.V. Mashkina- M .: Mechanical Engineering, 2013. - 241 p.

4. Lenkov S.V. Conceptual scheme of the system of intellectual data processing / S.V. Lenkov, V.M. Julie, O.M. Gorbatyuk, N.M. Bernas // Collection of scientific works of the Military Institute of Kyiv National Taras Shevchenko University. - K .: VIKNU, 2014. - Vip. No. 46. - C.181-190

5. Lenkov S.V. Analysis of existing methods and algorithms for detecting attacks in wireless data transmission networks / S.V. Lenkov, V.M. Julie, O.M. Gorbatyuk, N.M. Bernas, S.O. Bozhk // Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv. - K .: VIKNU, 2017. - Vip. No. 56. - C.124-1326. Lukatsky A.V. Detection of attacks. / A.V. Lukatsky - St. Petersburg: BHV-Petersburg, 2003. - 608 p.

7. Tanenbaum E. Computer networks. 5 th ed. / E. Tanenbaum, D. Wetherall- St. Petersburg: Peter, 2012. - 960 p.

8. Yefimova, L.L. Information security of networks. Russian and foreign experience: Monograph/L. L. Yefimova, S.A. Kocherga. - M.: UNITY-DANA, 2013. - 239 p.

9. Partyka, T.L. Information security: Manual/T. L. Partyka, I.I. Popov. - M.: Forum, 2012. - 432 p.

10. Petrov, S.V. Information security: Manual / S.V. Petrov, I.P. Slinkova, V.V. Gafner. - M.: ART, 2012. - 296 p.

11. Shangin, V.F. Information security of computer systems and networks: Manual / V.F. Shangin. - M.: IDES FORUM, Research Center INFRA-M, 2013. - 416 p.

12. Айвенс То. Computer networks. Cunnings. / K.Ayvens – SPb.: St. Petersburg, 2006. – 298 pages silt.

13. Zavgorodny V.I. Complex information security in computer systems: Manual. / V.I Zavgorodny. – M.: Lagos; PBOYuL N.A. Egorov, 2001. – 264 pages: silt.

14. Galatenko V. A. Bases of information security: course of lectures: Manual / Edition third/VA. Galatenko Under the editorship of the Academician of RAS V.B. Betelin / - M.:INTUIT.RU "the Internet university of Information Technologies", 2006. - 208 pages.

15. Babash, A.V. Information security. Laboratory practical work: Manual / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: Knorus, 2013. - 136 p.

Рецензент: д.т.н., проф. Барабаш О.В., завідувач кафедри вищої математики Державного університету телекомунікацій

к.т.н., доц. Джулий В.Н., к.т.н., доц. Красильников С.Р., Божук С.О.

МЕТОДЫ И АЛГОРИТМЫ ОБНАРУЖЕНИЯ АТАК В БЕСПРОВОДНЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

В статье предложены алгоритмы обнаружения атак в беспроводной сети на основе применения классифицированной модели.

Беспроводная среда передачи данных в силу своих особенностей создает потенциальные условия для прослушивания сетевого трафика и неконтролируемого подключения к беспроводной сети злоумышленников, которые находятся в зоне ее действия. 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 используются как технические средства защиты, так и организационные мероприятия. В настоящее время отсутствуют работы по применению методов интеллектуального анализа данных в задачах обнаружения атак на локальные беспроводные сети. В связи с этим возникает проблема выбора оптимального вектора признаков, специфичных для событий безопасности в беспроводных сетях, которые будут использоваться в ходе классификации данных событий. Задача разработки алгоритмического и программного обеспечения системы, позволяющей автоматизировать процесс выявления беспроводных атак на основе применения современных методов интеллектуального анализа

параметров сетевого трафика, является актуальной. 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 злонамеренной активности. Проведенный анализ угроз и их источников и построение их моделей, позволяющих более точно оценивать безопасность сетевой активности и уровень доверия к ее источнику. Предложенные алгоритмы обнаружения атак в беспроводной сети на основе применения классифицированной модели с использованием технологий интеллектуального анализа данных. Анализ алгоритмов позволяет сделать вывод об их применимости в составе системы обнаружения атак.

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

Ph.D. Juliy V.N., Ph.D. Krasilnikov S.R., Bozhuk S.O.

METHODS AND ALGORITHMS OF ATTACK DETECTION IN WIRELESS DATA NETWORKS

The algorithms for attacks detecting in a wireless network based on the application of a classified model are proposed in the article.

The wireless communication environment, due to its features, creates potential conditions for listening to the network traffic and uncontrolled connection to a wireless network of intruders who are in the zone of its operation. Wireless data networks are prone to various types of attacks due to its imperfections of protocols. In order to solve these problems of information security providing in wireless networks, both technical protection measures and organizational arrangements are used. At present, there are no works on the of data mining application methods in problems of detecting attacks on local wireless networks. In this connection, the problem of choosing an optimal vector of characteristics specific to security events in wireless networks that will be used during the classification of these events arises. The task of developing algorithmic and software systems that allows to automate the process of detecting wireless attacks based on using of intelligent analysis modern methods of network traffic parameters is relevant. The widespread of wireless using \ in corporate information systems makes it necessary to pay active attention to solving their inherent information security problems. At the same time, existing security measures, including commercial wireless intrusion detection systems, do not provide full protection against malicious activity. The analysis of threats and their sources and the construction of their models, allowing to assess the safety of network activity and the level of confidence in its source more accurately. The proposed algorithms for detecting attacks in a wireless network are based on the application of a classified model using data mining technologies. The analysis of algorithms allows to make a conclusion about their applicability in the system of attack detection.

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