инфраструктуры в различных странах мира, в т.ч. и в Украине, например, в случае утечки информации с ограниченным доступом или государственных информационных ресурсов, которые обрабатываются в этих системах. Выявлено дополнительную необходимость учитывать и другие тяжелые последствия для национальных интересов от разглашения сведений, составляющих именно государственную тайну в результате возможной реализации кибератаки при формировании перечня информационно-телекоммуникационных систем объектов критической инфраструктуры государства. Представлены предложения к формированию единого классификатора негативных последствий кибератак на информационно-телекоммуникационные системы объектов критической инфраструктуры государства с учетом обработки в этих системах и других видов информации с ограниченным доступом как конфиденциальная (в.ч. персональные данные) и служебная информация.

Ключевые слова: кибератака, информация с ограниченным доступом, информационно-телекоммуникационная система, критическая инфраструктура государства, негативные последствия, оценивание ущерба.

ANALYSIS OF BASIC TERMINOLOGY AND NEGATIVE CONSEQUENCES FROM CYBER ATTAKS ON INFORMATION-TELECOMMUNICATION SYSTEMS OF OBJECTS STATE'S CRITICAL INFRASTRUCTURE

The article analyzes the basic terminology and variety of negative consequences to which cyber attack can lead to information and telecommunication systems of critical infrastructure objects in various countries of the world, including. and in Ukraine, for example, in case of leakage of information with limited access or state information resources that are processed in these systems. It has been shown that it is necessary to take into account other severe consequences for national interests from disclosure of information that constitutes state secrets as a result of the possible implementation of cyber attacks in the formation of a list of information and telecommunications systems for critical infrastructure of the state. Proposals to the formation of a single classifier of the negative consequences of cyber attacks on information and telecommunications systems of critical infrastructure facilities of the state, taking into account the processing in these systems and other types of information with limited access as confidential (including personal data) and service information.

Keywords: cyberattack, restricted information, information and telecommunication system, critical infrastructure of the state, negative effects, damage assessment.

Дрейс Юрій Олександрович, кандидат технічних наук, доцент, завідувач кафедри інноваційних технологій професійної освіти Національного авіаційного університету.
E-mail: y.dreis@nau.edu.ua.
Дрейс Юрий Александрович, кандидат технических наук, доцент, заведующий кафедрой инновационных технологий профессионального образования Национального авиационного университета.
Dreis Yurii, PhD in Eng., Associate Professor, Head of the Department of Innovative Technologies Professional Education, National Aviation University (Kyiv, Ukraine).

DOI: 10.18372/2410-7840.19.11901
УДК 351.746:007–047.44

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ В БЕЗДРОТОВИХ МЕРЕЖАХ СТАНДАРТУ IEEE 802.11

Володимир Базилевич

Функціонування будь-якого сучасного підприємства базується на використанні інформаційних технологій, зокрема комп'ютерних мереж. Сучасні реалії зобов'язують при проектуванні мереж робити акцент на мобільність та масштабованість. Для ефективного вирішення цих задач доцільно використовувати бездротові комп'ютерні мережі стандарту IEEE 802.11. В той же час використання бездротових мереж створює нові виклики, пов'язані з розробкою системи захисту від кіберзагроз. В даній статі аналізуються та порівнюються методи, які використовуються для створення відповідних систем, визначаються переваги та недоліки кожного з них, акцентуючи увагу на програмний аспект захисту, як такий, що найчастіше стає об'єктом кібератак. Проведений аналіз дозволяє визначити доцільність використання того чи іншого методу захисту або їх комбінації в залежності від вихідних умов, ресурсів та цілей, що ставляться при побудові системи захисту.

Ключові слова: *комп'ютерні мережі, стандарт IEEE 802.11, методи захисту, Wi-Fi, кібербезпека.*

Постановка проблеми. У зв'язку з різким збільшенням популярності мобільних пристроїв (смартфонів, планшетів, ноутбуків і т.д.) на ринку України за останні декілька років зросла і необхідність у розгортанні нових та модернізації існуючих комп'ютерних мереж з акцентом на бездротові технології. За даними агентства мобільного маркетингу LEAD9 [1] 71% користувачів глобальної мережі інтернет використовують для доступу мобільні пристрої. Відповідно створюється нагальна необхідність у створені та оптимізації сучасних корпоративних та приватних комп'ютерних мереж та систем їх захисту від кіберзагроз. На відміну від дротових мереж, бездротові більш вразливі та мають низку загроз, які притаманні саме такому способу передачі даних [2] і, відповідно, не враховуються при побудові системи захисту від кіберзагроз для дротових мереж. З появою бездротових мереж паралельно почали розвиватись і методи захисту їх від стороннього втручання, цей процес відбувається і тепер. Аналіз методів захисту бездротових мереж, що є основним завданням даної статті, включає в себе класифікацію та порівняння сучасних методів і технологій захисту та їх комбінацій, виокремлення сильних та слабких сторін.

Аналіз останніх досліджень і публікацій. Дослідженнями кіберзагроз та методів захисту комп'ютерних мереж присвячені роботи багатьох вітчизняних та зарубіжних вчених, зокрема: А.Г. Корченко[3], С.В. Казмірчук [4], Д.Б. Мехеда [5], Ю.М. Ткач [5], В.С. Коваленко, Л.А. Шувалової, J. Xiong, K. Jamieson, G. Gounaris та ін.

Виділення не вирішених раніше частин загальної проблеми. Попри значну увагу вчених до цієї проблеми не існує єдиного підходу до класифікації та детермінації методів захисту бездротових комп'ютерних мереж стандарту IEEE 802.11.

Мета статті. Головною метою даної роботи є аналіз існуючих методів захисту бездротових комп'ютерних мереж, їх класифікація та порівняння.

Виклад основного матеріалу. На сьогоднішній день, в Україні, кількість користувачів, що виходять в інтернет з мобільних пристроїв перевищила кількість тих, що користуються стаціонарними пристроями. Відповідно зросла і кількість бездротових мереж. При цьому, через відносну простоту розгортки таких мереж, часто це відбувається без залучення спеціалістів, наприклад відкриті точки доступу кафе, ресторанів, кінотеатрів, торгових центрів, тощо. В той же час, як правило, відповідні точки доступу підключаються до локальних мереж закладів та установ, що в сукупності з некваліфікованим налаштуванням та адмініструванням дає зростання можливих кіберзагроз в декілька разів. За даними перевірки департаментом кіберполіції близько 75% всіх бездротових мереж Wi-Fi можуть бути успішно атаковані. У кожній другій системі з бездротової мережі можливий доступ до локальної комп'ютерної мережі установ приватного та державного секторів. При цьому способи атак на корпоративні та державні інфраструктури, як і раніше, базуються на використанні поширених загальновідомих вразливостей і недоліків програмного забезпечення. Проведений спеціалістами департаменту аналіз свідчить про те, що уразливості критичного рівня присутні в майже половині інформаційних інфраструктур приватного та державного секторів. Приватні дослідники зазначають, що значну частку таких уразливостей (40%) становлять помилки у налаштуванні програмного забезпечення, помилки у програмному коді (27% систем) та відсутність, або не своєчасність оновлень безпеки (20% систем). [6]. Таким чином створення ефективної системи захисту бездротових мереж на основі існуючих методів є актуальним завданням в умовах постійно зростаючої мобільності кінцевих пристроїв.

Класифікувати методи захисту можна за різними ознаками, в першу чергу існують методи фізичного, технічного та програмного захисту. В даному дослідженні акцент робиться на останньому, як такому, що найбільше піддається налаштуванню. Що ж стосується методів програмного захисту, вони в свою чергу поділяються на декілька категорій: методи обмеження доступу; методи автентифікації та шифрування.

До методів обмеження доступу належать:

1. Фільтрування MAC-адрес. Даний метод дозволяє визначити список пристроїв і дозволити лише цим пристроям доступ до вашої мережі Wi-Fi (whitelist), або навпаки заборонити певним пристроям доступ (blacklist). На жаль цей метод ефективний лише в теорії, на практиці такий захист складно налаштовувати і дуже легко обійти. Це одна із функцій маршрутизатора Wi-Fi, яка створює помилкове відчуття безпеки.

Працює цей метод дуже просто, кожен мережевий пристрій має унікальну фізичну адресу (MAC-адресу), яка ідентифікує його в мережі. Як правило, маршрутизатор дозволяє будь-якому пристрою підключатися, якщо він знає відповідну парольну фразу. За допомогою фільтрації MAC-адреси маршрутизатор спочатку порівнює MAC-

адресу пристрою з затвердженим списком MAC-адрес і надає пристрою доступ до мережі, лише в разі якщо його MAC-адреса була схвалена. Звучить досить добре, проте MAC-адреси можуть легко підробляти (клонувати) в багатьох операційних системах, тому будь-який пристрій може претендувати на одне з дозволених унікальних MAC-адрес. MAC-адреси також легко отримати. Вони надсилаються по повітрю, коли кожен пакет переходить до пристрою та з нього, оскільки MAC-адреса використовується для того, щоб кожний пакет потрапляв на правильний пристрій. Все що потрібно зловмиснику, це стежити за трафіком Wi-Fi декілька секунд, дослідити пакети, що були передані за цей час, щоб знайти MAC-адресу дозволеного пристрою, змінити MAC-адресу свого пристрою на таку дозволену MAC-адресу та підключатися на місце цього пристрою.

Це зробити неможливо, поки довірений пристрій підключений до мережі, але атака "deauth" (деавтентифікація) або "deassoc" (деассоціація), які примусово відключають пристрій від мережі Wi-Fi, дозволить зловмисникові зайняти його місце [7]. Зловмисник з набором інструментів, таких як Kali Linux, може використовувати програму Wireshark для перехоплення пакету, запустити швидку команду для зміни своєї MAC-адреси, використовувати aireplay-ng для надсилання пакетів deassociation для цього клієнта, а потім підключитися на його місце. Цей процес може зайняти менше 30 секунд. І це лише ручний метод, який передбачає виконувати кожен крок вручну - не слід також забувати про автоматизовані інструменти або скрипти, які можуть зробити це швидше. Тож цей метод, хоча і існує, проте не забезпечує ефективного захисту мережі.

2. Режим прихованого SSID (Service Set Identifier). SSID – це ідентифікатор мережі, який за замовченням надсилається маршрутизатором або точкою доступу бездротової мережі у режимі broadcast, тобто усім. Зазвичай точки доступу мережі Wi-Fi надсилають своє мережеве ім'я як один з інформаційних елементів, які входять до деяких кадрів керування, ці елементи, або маяки, з інформаційним елементом, ідентифікатором якого є 0. Ця структура параметрів показана на рис. 1.

Приховати SSID, тобто припинити його транслювати в ефір, також вважається одним із методів захисту. Проте, на нашу думку, це іще один не ефективни і скоріше оманливий метод захисту. За словами одного з фахівців Microsoft, Steve Riley : SSID – це мережеве ім'я, а не пароль. Бездротова мережа має SSID, щоб відрізняти її від інших бездротових мереж поблизу. SSID ніколи не розроблявся, щоб бути прихованим, і тому не забезпечить вашу мережу будь-яким захистом, якщо ви намагаєтесь сховати його [8].

Відповідь на запитання чому вищеописаний метод не є ефективним дуже проста. Дуже легко знайти ідентифікатор "прихованої" мережі - все, що для цього потрібно зробити - це використовувати програму, таку як inSSIDer, NetStumbler або Kismet, щоб короткочасно сканувати ефір та показати всі існуючі мережі в радіусі доступу.

3. Статична IP-адресація. Даний методи захисту полягає у відключені динамічного призначення локальних IP-адрес центральною станцією (маршрутизатором), натомість вимагаючи від користувачів вручну налаштовувати відповідні параметри мережі (адресу, маску, DNS – сервер, шлюз, тощо). Про те цей метод також не э ефективним, адже обійти його може навіть низько кваліфікований зловмисник з мінімальними знаннями про комп'ютерні мереж. До того ж такий спосіб адресації значно ускладнює адміністрування мережі, зокрема в частині додавання нових вузлів, погіршує масштабування мережі, що неприпустимо в бездротових мережах, адже за визначенням вони, навпаки, мають покращувати цей параметр.

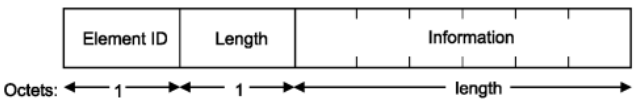

Рис. 1. Структура параметрів кадру

Тож вищеописані методи обмеження доступу на сьогодні не є ефективними при побудові системи захисту від кіберзагроз бездротових мереж.

Наступна категорія методів захисти, це методи аутентифікації. До них належать, зокрема:

1. Відкрита автентифікація (Open).

Відкрита автентифікація дозволяє будь-якому бездротовому пристрою автентифікуватись, а потім намагатися встановити зв'язок з точкою доступу. Це не завжди означає, що одразу після автентифікації буде надано доступ до мережі. Після автентифікації може бути запитано пароль, ключову фразу, додаткові ідентифікаційні дані, тощо. Про те такий метод аутентифікації також не захищає мережу і може використовуватись лише на точках доступу, що відділені від основної мережі додатковими засобами захисту, наприклад брандмауером.

2. Автентифікація зі спільним ключем (WEP, WPA).

Даний метод автентифікації є найпопулярнішим, а його ефективність залежить від стандарту

захисту, який використовується для його реалізації. Під час автентифікації за допомогою спільного ключа ключі клієнта та точки доступу повинні співпадати.

Першим стандартом захисту з використанням спільного ключа був WEP (Wired equivalent privacy), проте попри свою гучну назву (Захист еквівалентний дротовому) цей стандарт має слабкі місця (бекдори) через які процес несанкціонованого доступу до мережі стає дуже простим. Стандарт використовує алгоритм потокового шифрування RC4 (рис. 2), який був розроблений ще в 1987 році Роном Рівестом. До переваг даного алгоритму можна віднести лише швидкодію та простоту реалізації.

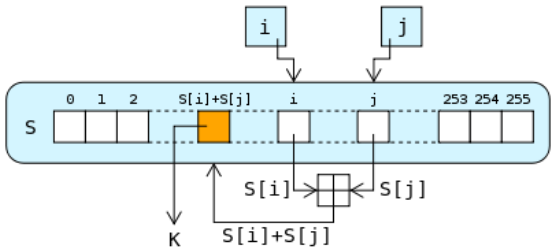

Рис. 2. Схема шифрування одного символу відкритого тексту за допомогою RC4

Що ж стосується недоліків, то основним є те, що на сьогодні існують дієві методи атаки на цей алгоритм, що робить його використання не доцільним в сучасних системах. Атака стають можливі через те, що RC4 вимагає, щоб вектори ініціалізації (IV) були випадковими, реалізація RC4 в WEP повторює, IV приблизно кожні 6000 кадрів. Прослуховуючи мережу, наприклад за допомогою набору програм Aircrack-ng, можна захопити достатню кількість IV і розшифрувати ключ! Тому цей стандарт хоч і підтримується більшістю маршрутизаторів, проте з 2004 року офіційно вважається застарілим.

На зміну стандарту WEP прийшов стандарт WPA (Wi-Fi protected access), цей стандарт виключив можливість простого способу атаки через прослуховування трафіка завдяки відмові від RC4 і, відповідно, зникненню необхідності повторно використання ключів шифрування. В основі стандарту WPA лежить TKIP (Temporary Key Integrity Protocol) – протокол тимчасової цілісності ключів. TKIP динамічно генерує новий 128-бітний ключ для кожного пакета і тим самим запобігає WEP-скомпрометованим типам атак. TKIP та відповідний стандарт WPA реалізують три нові функції безпеки для вирішення проблем безпеки, що виникали в WEP-захищених мережах [6]. По-перше, TKIP реалізує ключову функцію змішування, яка поєднує таємний корінний ключ з вектором ініціалізації, перш ніж передавати його до ініціалізації RC4. По-друге, WPA реалізує лічильник послідовності, щоб захистити мережу від повторних атак. Пакети, що надходять не по встановленому порядку, будуть відхилені точкою доступу. По-третє, TKIP реалізує 64-розрядну перевірку цілісності повідомлень (MIC). В якості алгоритму шифрування TKIP також використовує RC4. TKIP також надає механізм повторного набору. TKIP гарантує, що кожен пакет даних надсилатиметься з унікальним ключем шифрування.

Змішування ключів збільшує складність розшифровки ключів, надаючи зловмиснику суттєво менше даних, які були зашифровані за допомогою будь-якого одного ключа. WPA також реалізує новий код цілісності повідомлень, MIC. Перевірка цілісності повідомлення запобігає прийняттю підроблених пакетів. Під WEP було можливим змінити пакет, вміст якого був відомий, навіть якщо він не був розшифрований. Проте, незважаючи на ці зміни, слабкість захисту деяких з цих доповнень дозволила створити нові, хоч і більш складні, способи атак. Протокол TKIP не вважається надійним і офіційно не підтримується стандартом 802.11 з 2012 року.

Друга версія стандарту WPA2 виправила помилки попередньої та вважається найефективнішим методом захисту автентифікації зі спільним ключем. В основі даного стандарту лежить протокол шифрування CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol), який в свою чергу базується на принципово новому алгоритмі шифрування AES (Advanced Encryption Standard). AES базується на принципі проектування, відомому як мережа заміщення-перестановки, що поєднанує як заміщення, так і перестановку, і швидко працює як у програмному, так і в апаратному забезпеченні. На відміну від свого попередника DES, AES не використовує мережу Feistel. AES - це варіант Rijndael, який має фіксований розмір 128 біт, а розмір ключа 128, 192 або 256 біт. На відміну від цього, специфікація Rijndael як така визначається за розмірами блоків і ключів, які можуть бути довільними, кратними 32біт, і займати мінімум 128 і максимум 256 біт.

AES працює на 4 × 4 стовпчиковій матриці порядку байтів, які називаються станом, хоча деякі версії Rijndael мають більший розмір блоку і мають додаткові стовпці в стані (див. рис. 3). Більшість розрахунків AES виконуються в певному кінцевому полі.

Розмір ключа, який використовується для шифру AES, визначає кількість повторень раунду шифрування, які перетворюють вхідні дані, що називається відкритим текстом, у кінцевий результат, що

називається шифрованим текстом. Кількість циклів повторення виглядає наступним чином:

– 10 циклів повторення для 128-бітних ключів;
– 12 циклів повторення для 192-бітних ключів;
– 14 циклів повторення для 256-бітних ключів.

Кожен раунд складається з кількох етапів обробки, кожен з яких містить чотири подібних, але різні етапи, включаючи один, який залежить від самого ключа шифрування. Набір зворотних раундів застосовується для перетворення шифру тексту назад у вихідний відкритий текст, використовуючи той самий ключ шифрування.

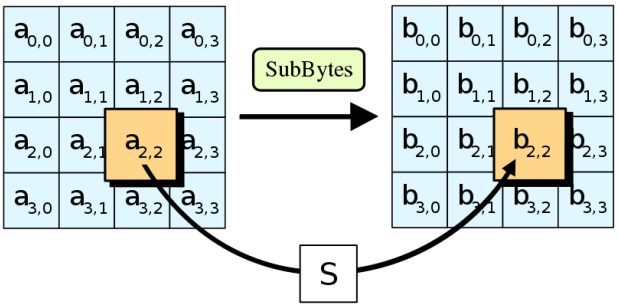

Рис. 3. Крок SubBytes, один з чотирьох етапів у раунді AES-шифрування

Вдала атака на мережу, захищену за стандартом WPA2 з ключем, розміром 256 біт хоча і можлива теоретично, проте вимагає високої кваліфікації зловмисника, спеціального програмного/технічного забезпечення, та, що найголовніше, значного проміжку часу. Ефективно і відносно просто атакувати таку мережу можна лише при використанні слабкого кодового слова(паролю), такого як словникове слово, простий набір цифр, тощо.

Тож серед описаних вище методів використання стандарту WPA2 у комбінації з протоколом CCMP забезпечить найвищий рівень захисту і вважається найбільш вдалим рішенням при побудові системи захисту приватних мереж.

3. Автентифікація за допомогою RADIUS-сервера.

Remote Authentication Dial In User Service (RADIUS) або Віддалений ідентифікаційний набір в службі користувача - це протокол, що забезпеує трирівневу систему: автентифікація, авторизація та облік та використовується для віддаленого доступу до мережі. RADIUS спочатку був розроблений як саморбний стандарт, але пізніше був опублікований в документах ISOC RFC 2138 та RFC 2139. Ідея полягає в тому, що існує сервер, який виконує функції «охоронця», перевіряючи ідентифікацію через ім'я користувача та пароль, які вже заздалегідь визначені користувачем. Сервер RADIUS також може бути налаштований для виконання політик та обмежень користувачів, а також запису облікової інформації, такої як час підключення для таких цілей, як платіж.

Такий метод захисту досить надійний, проте вимагає додаткового обладнання, налаштування та може застосовуватись лише в комбінації з іншими методами захисту. Такий підхід захисту бездротових мереж, як правило застосовують у корпоративних мережах.

Висновки. Провівши аналіз та порівнявши особливості вищеописаних методів захисту можна зазначити, що технології обмеження доступу не є надійними при побудові систем захисту комп'ютерних мереж стандарту IEEE 802.11, що ж стосується методів авторизації та шифрування, то лише використання комбінації сучасних протоколів/алгоритмів та коректне налаштування мережевого обладнання дозволяє отримати прийнятний рівень безпеки. В той же час, для створення надійної системи захисту, окрім програмного захисту слід також враховувати необхідність постійного моніторингу роботи мережі, організацію технічного та фізичного захисту.

На нашу думку серед проаналізованих методів найбільш ефективною є комбінація використання стандарту захисту WPA2 та протоколу шифрування CCMP (який базується на алгоритмі AES) з використанням складного ключа доступу (наприклад 14-и значний набір випадкових цифр та літер).

ЛІТЕРАТУРА

[1]. *Кількість користувачів мобільних пристроїв в Україні перевищила кількість користувачів ПК*, дослідження, RBC Ukraine. – 2017. [Електронний ресурс] Режим доступу: https://www.rbc.ua/ukr/news/kolichestvo-polzovateley-mobilnyh-ustroystv-1489488909.html. [Дата доступу: липень 2017].

[2]. Д. Мехед, Ю. Ткач, В. Базилевич, Т. Петренко "Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11", *Захист інформації*, №4, С. 285–291, 2015.

[3]. О. Юдін, Г. Конахович, О. Корченко, *Захист інформації в мережах передачі даних: підруч.* К.: Вид-во ТОВ НВП "ІНТЕРСЕРВІС", 2009, 714 с.

[4]. А. Корченко, А. Архипов, С. Казмирчук, *Анализ и оценивание рисков информационной безопасности. Монография.* К.: ООО «Лазурит-Полиграф», 2013, 275 с

[5]. Д. Мехед, "Захист інформації в комп'ютерних мережах", *Технічні науки та технології : науковий журнал,* №2 (2), С. 140-146, 2015.

[6]. Кіберполіція: захист мереж WI-FI - на дуже низькому рівні, 2017. [Електронний ресурс]. Режим доступу: https://www.ukrinform.ua/rubric-technology/2281044-kiberpolicia-zahist-merez-wifi-na-duze-nizkomu-rivni.html. [Дата доступу: липень 2017].

[7]. C. Hoffman, Why You Shouldn't Use MAC Address Filtering On Your Wi-Fi Router, 2014. [Electronic resource]. Access mode: https:// www.howtogeek.com/204458/why-you-shouldn %E2%80%99t-use-mac-address-filtering-on-your-wi-fi-router/. [Date of access: july 2017].
[8]. S. Riley, Myth vs reality: Wireless SSIDs, *Microsoft TechNet*, 2007. [Electronic resource]. Access mode: https://blogs.technet.microsoft.com/steriley/2007/10/16/myth-vs-reality-wireless-ssids/. [Date of access: july 2017].

REFERENCES

[1]. Kilkist korystuvachiv mobilnyx prystroyiv v Ukrayini perevyshhyla kilkist korystuvachiv PK, - doslidzhennya . [Electronic resource]. Access mode: https://www.rbc.ua/ukr/news/kolichestvo-polzovateley-mobilnyh-ustroystv-1489488909.html. [Date of access: july 2017].
[2]. D. Mexed, Y. Tkach, V. Bazylevych, T. Petrenko, "Analysis information security threats network standard IEEE 802.11", Zahist ìnformacìï, no. 4, pp. 285–291, 2015.
[3]. O. Yudin, G. Konaxovych, O. Korchenko, *Data protection in data networks*, 2009, 714 p.
[4]. A. Korchenko, A. Arkhipov, S. Kazmirchuk, *The analysis and assessment risks information security. Monograph*, 2013, 275 p.
[5]. D. Mexed, Information security in computer network, *Texnichni nauky ta texnologiyi,* no. 2 (2), pp. 140-146, 2015.
[6]. Cyberpolice: Zahyst merezh WI-FI na duzhe nyzkomu rivni. [Electronic resource]. Access mode: https: // www. ukrinform. ua / rubric - technology/ 2281044- kiberpolicia- zahist- merez- wifi- na- duze-nizkomu-rivni.html. [Date of access: july 2017].
[7]. C. Hoffman, Why You Shouldn't Use MAC Address Filtering On Your Wi-Fi Router, 2014. [Electronic resource]. Access mode: https:// www.howtogeek. com/204458/why-you-shouldn%E2%80%99t-use-mac-address-filtering-on-your-wi-fi-router/. [Date of access: july 2017].
[8]. S. Riley, Myth vs reality: Wireless SSIDs, Microsoft TechNet, 2007. [Electronic resource]. Access mode: https://blogs.technet.microsoft.com/steriley/2007/10/16/myth-vs-reality-wireless-ssids/. [Date of access: july 2017].

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ОТ КИБЕРУГРОЗ В БЕСПРОВОДНЫХ СЕТЯХ СТАНДАРТА IEEE 802.11

Функционирование любого современного предприятия базируется на использовании информационных технологий, в частности компьютерных сетей. Современные реалии обязывают при проектировании сетей делать акцент на мобильность и масштабируемость. Для эффективного решения этих задач целесообразно использовать беспроводные компьютерные сети стандарта IEEE 802.11. В то же время использование беспроводных сетей создает новые вызовы, связанные с разработкой системы защиты от киберугроз. В данной статье анализируются и сравниваются методы, которые используются для создания соответствующих систем, определяются преимущества и недостатки каждого из них, акцентируя внимание на программный аспект защиты, как таковой, который чаще всего становится объектом кибератак. Проведенный анализ позволяет определить целесообразность использования того или иного метода защиты или их комбинации в зависимости от исходных условий, ресурсов и целей, которые ставятся при построении системы защиты.

Ключевые слова: компьютерные сети, стандарт IEEE 802.11, методы защиты, Wi-Fi, кибербезопасность.

ANALYSIS OF METHODS OF PROTECTION FROM CYBERTHREATS IN IEEE 802.11 NETWORKS

The functioning of any modern enterprise is based on the use of information technologies, particularly, computer networks. Modern realities require design the networks with mobility and scalability. In order to effectively address these issues, it is advisable to use wireless IEEE 802.11 computer networks. At the same time, the use of wireless networks creates new challenges related to the development of a system of protection against cyber threats. This article analyzes and compares the methods used to create relevant systems, identifies the strengths and weaknesses of each of them, focusing on the programmatic aspect of protection as one that most often becomes the object of a cyberattack. The conducted analysis allows us to determine the expediency of using one or another method of protection or their combination, depending on the initial conditions, resources and goals that are put into the construction of the protection system.

Keywords: computer networks, IEEE 802.11 standard, protection methods, Wi-Fi, cyber security

Базилевич Володимир Маркович, кандидат економічних наук, доцент кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету.
E–mail: bazvlamar@gmail.com
Базилевич Владимир Маркович, кандидат экономических наук, доцент кафедры кибербезопасности и математического моделирования Черниговского национального технологического университета.
Bazylevych Volodymyr, PhD, associate professor of cybersecurity and mathematical simulation department, Chernihiv National University of Technology.