

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І
ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

Кваліфікаційна наукова
праця на правах рукопису

ПЛАТОНЕНКО АРТЕМ ВАДИМОВИЧ

УДК 004:004.056:004.7(043.3)

ДИСЕРТАЦІЯ

**«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ
СИСТЕМ БЕЗДРОТОВОГО ЗВ'ЯЗКУ НА ОСНОВІ
ВДОСКОНАЛЕННЯ ПАРОЛЬНИХ ПОЛІТИК»**

05.13.06 – інформаційні технології

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело

_____ А. В. Платоненко

Науковий керівник
Бурячок Володимир Леонідович
доктор технічних наук, професор
завідувач кафедри інформаційної
та кібернетичної безпеки
Київський університет
імені Бориса Грінченка

Київ - 2019

АНОТАЦІЯ

Платоненко А. В. Технологія забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології. – Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України, Київ, 2019.

Дисертація присвячена розв'язанню актуального наукового завдання, що полягає в розробленні технології забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик.

Сучасні мобільні пристрої стали невід'ємною частиною нашого життя, але окрім зручності та багатьох технічних можливостей вони несуть за собою все більшу небезпеку для інформації, яка в них зберігається та передається.

З використанням високошвидкісних мобільних мереж, загрози інформаційної безпеки для державних та приватних установ дедалі збільшуються, оскільки працівники все частіше використовують мобільні пристрої для віддаленої роботи.

Для зловмисників відкриваються більші технічні можливості для здійснення атак, що потребує впровадження засобів захисту інформації. Зважаючи, на таке, питання щодо забезпечення функціональної безпеки (доступності та цілісності) систем бездротового зв'язку є надзвичайно актуальними.

Способи, які використовувались для вирішення проблеми (парольні політики користувачів з обмеженням по кількості символів; генерування паролів на основі поєднанні декількох слів, або заміни слів іншою мовою; генерування випадкових чисел для вибору слів за таблицею, генератори випадкових значень паролів з певної множини символів і т.п.), не повною мірою відповідають викликам сьогодення. Розробка технології забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик за рахунок генерування паролю з використанням інтегрованого підходу, є актуальною науковою задачею, що має теоретичне і практичне значення.

Тематика дисертаційної роботи та одержані результати безпосередньо пов'язані з «Основними науковими напрямками та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014-2018 роки», а також Стратегією кібербезпеки України від 15 березня 2016 року №96/2016. Результати роботи відображені у звітах з науково-дослідної роботи «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем (ІКС) в умовах впливу кібернетичних атак» (номер державної реєстрації 0114U000391).

Проведені дослідження базуються на методах теорії множин (для формалізації процесів формування вимог до парольних політик, а також ідентифікації і визначення повноти їх забезпечення), теорії ймовірностей і математичної статистики (для розробки й дослідження алгоритмів генерування парольних множин), експертного оцінювання (для визначення коефіцієнтів стійкості, а також встановлення зв'язків між базовим способом генерування паролів та відповідними способами-аналогами), математичного моделювання (для оцінювання повноти виконання множини вимог), порівняння (для визначення оптимального способу генерування паролів), графічний (для відображення моделей атак та парольних множин), формалізації (для опису розробленого способу ускладнення паролів).

Об'єкт дослідження – процес забезпечення функціональної безпеки систем бездротового зв'язку. *Предмет дослідження* – інформаційна технологія забезпечення функціональної безпеки систем бездротового зв'язку в умовах загроз і обмежень, визначених специфічними умовами функціонування таких систем.

Проведено аналіз статистичних даних щодо наявності мобільних пристроїв та їх підключень мешканцями України, а також множини актуальних загроз та уразливостей для систем бездротового зв'язку в умовах кібернетичних атак.

Сформовано загальну модель перехоплення та захисту інформації в бездротових мережах.

Розроблено метод обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, для забезпечення їх надійності функціональної безпеки і живучості в умовах кібернетичних атак, за рахунок вибору раціонального способу генерування паролів серед множини існуючих.

Вдосконаленню спосіб генерування випадкових паролів, а також досліджено даний вдосконалений спосіб генерування ускладнених паролів.

Сформовано рекомендації щодо застосування на базі існуючих засобів захисту систем бездротового зв'язку стандарту IEEE 802.11 запропонованого способу.

Для впровадження розробленого способу сформовано алгоритм, який описує всі етапи та дає змогу створити необхідне програмне забезпечення для автоматизованого генерування стійкого паролю в залежності від вимог системи, для якої він буде використовуватись.

Новизна роботи полягає в подальшому розвитку теоретичних і практичних методів та моделей забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик, за рахунок:

- розробки та обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, на відміну від подібних, шляхом оцінки ступеня близькості між базовим способом генерування паролів і кожним способом-аналогом, що дозволяє на відміну від подібних, серед множини існуючих способів генерування паролів обрати спосіб, найбільш раціональний з точки зору його вдосконалення та забезпечити функціональну безпеку систем бездротового зв'язку в умовах впливу кібернетичних атак;

- удосконалення способу генерування випадкових паролів для систем бездротового зв'язку, завдяки урахуванню можливості співпадіння з паролями системи словників та використанню інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів (обраних за правилом комбінації з введенням певного ускладнення), що забезпечує, порівняно з аналогами, підвищення рівня захищеності систем бездротового зв'язку стандарту IEEE 802.11 від можливого злому (спроб несанкціонованого доступу) в $3,73 \cdot 10^4$ разів.

Результати дисертаційного дослідження впроваджено у навчальний процес Київського університету імені Бориса Грінченка, а також в практику розроблення політик інформаційної безпеки двох підприємств.

Практична цінність отриманих результатів полягає в програмній реалізації:

по-перше, методу формування парольних політик, що дозволяє раціонально обрати спосіб генерування паролів серед множини існуючих;

по-друге, способу генерування ускладнених паролів в системах бездротового зв'язку, що дозволяє сформувати стійкий до підбору пароль.

Використання зловмисниками комплексного підходу для спроб несанкціонованого доступу до систем бездротового зв'язку (шляхом об'єднання соціальної інженерії та перехоплення даних з використанням зловмисного програмного забезпечення), а також нових видів кібератак, що дозволяють приховано встановлювати шкідливе ПЗ на мобільні пристрої може сприяти зниженню ефективності існуючих методів та засобів захисту бездротових мереж.

Враховуючи статистику та проведені в роботі розрахунки, можна стверджувати, що впровадження способу генерування ускладнених паролів дозволить суттєво підвищити рівень захищеності бездротових мереж.

Перспективним напрямком подальших досліджень є підтримка в актуальному стані бази словників паролів для впровадження аналізу та подальша повна автоматизація запропонованого способу.

Ключові слова: інформаційна безпека, загрози інформаційної безпеки, бездротові мережі, захист мереж від несанкціонованого доступу, захист мобільних пристроїв, пароль, генерування паролів, стійкі паролі, парольні політики.

ANNOTATION

A. Platonenko. Techodology of providing functional security for wireless communication systems based on the improvement of the password policies. - On the manuscript basis. Qualification scientific work on the rights of manuscript.

The technique of ensuring the functional safety of wireless communication systems based on the analysis of password policies

The dissertation is for the degree of a candidate of technical sciences in specialty 05.13.06 - Information technologies. - Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, 2019.

The dissertation is devoted to the solution of the actual scientific problem, which consists in providing functional security for wireless communication systems on the basis of improvement passwords corporate policies.

Modern mobile devices have become an integral part of our lives, but in addition to convenience and many technical capabilities, they carry an increasing danger for the information stored and transmitted.

With the use of high-speed mobile networks, information security threats for public and private institutions are increasing as workers increasingly use mobile devices for remote work.

Attackers have greater technical capacity to carry out attacks that require information security. Against this background, the issues of ensuring the functional security (accessibility and integrity) of wireless systems are extremely urgent.

Methods used to solve the problem (password policies of users with a character limit; generating passwords based on a combination of multiple words; or replacing words with another language; generating random numbers to select words by table .p.) do not fully meet the challenges of today. The development of wireless security technology based on the improvement of password policies by generating a password using an integrated approach is a pressing scientific challenge of both theoretical and practical importance.

The topic of the dissertation and the results obtained are directly related to the "Basic scientific directions and the most important problems of basic research in the field of natural, technical and human sciences of the NAS of Ukraine for 2014-2018", as well as to the Cybersecurity Strategy of Ukraine of March 15, 2016 №96 / 2016. The results of the work are reflected in the reports on the research work "Development of methods and means of increasing the survivability of information and communication systems in the conditions of the impact of cyber-attacks" (state registration number 0114U000391).

The conducted researches are based on methods of set theory (for formalization of processes of formation of requirements for password policies, as well as identification and determination of completeness of their provision), theory of probabilities and mathematical statistics (for development and research of algorithms for generation of password sets), expert evaluation (for determination of coefficients of stability , as well as establishing links between the basic password generation method and the corresponding analog methods), mathematical modeling (to evaluate the completeness of the multiple requirements), comparison (to determine the optimal method of generating passwords), graphics (for the models attacks and password set) formalization (to describe the method developed complications passwords).

Object of study is the process of ensuring the functional security of wireless communication systems. *The subject of the research* is information technology for ensuring the functional security of wireless systems in the conditions of threats and restrictions determined by the specific conditions of such systems operation.

The statistics on the availability of mobile devices and their connections by Ukrainian residents are analyzed, as well as many current threats and vulnerabilities for wireless systems in the context of cyber-attacks.

A general model of interception and protection of information in wireless networks has been formed.

A method of substantiating the solution to improve password policies in wireless systems has been developed to ensure their functional security and survivability in

cyber-attacks by choosing a rational method of generating passwords among many existing ones.

Improved method for generating random passwords, and explored this advanced method for generating complex passwords.

Recommendations have been made to apply the proposed IEEE 802.11 wireless method based on existing wireless security features.

To implement the developed method, an algorithm was developed that describes all the steps and allows you to create the necessary software to automatically generate a stable password, depending on the requirements of the system for which it will be used.

The novelty of the work lies in the further development of theoretical and practical methods and models for ensuring the functional security of wireless systems based on the improvement of password policies through:

- developing and validating solutions to improve password policies in wireless systems, as opposed to similar ones, by assessing the degree of closeness between the basic method of password generation and each unlike any of the many existing password-generating methods, choose the method that is most streamlined in terms of improving it and ensure the functional security of wireless systems in the face of cyber-attack;

- improving the method of generating random passwords for wireless systems by taking into account the ability to match the passwords of the vocabulary system and using an integrated approach to generate more stable passwords by length and character set (chosen by the combination rule with some complication), compared to its counterparts, the IEEE 802.11 wireless security system is increased by $3.73 \cdot 10^4$ times from possible hacking (unauthorized access attempts).

The results of the dissertation research were implemented in the educational process of the Kyiv University named after Boris Grinchenko, as well as in the practice of developing information security policies of the two enterprises.

The practical value of the obtained results lies in the software implementation:

first, a password policymaking method that allows you to rationally choose how to generate passwords among multiple existing ones;

secondly, a method of generating complicated passwords in wireless systems that allows you to generate a password-resistant password.

Using a malicious approach to malicious access to wireless systems (by combining social engineering and data capture using malware), as well as new types of cyberattacks that allow hidden malware to be installed on mobile devices can reduce efficiency existing methods and remedies for wireless networks. Considering the statistics and the calculations made in the work, it can be argued that the introduction of a method of generating complicated passwords will significantly increase the security level of wireless networks.

A promising direction for further research is to keep the database of passwords vocabulary up-to-date for analysis and to further fully automate the proposed method.

Keywords: information security, threats of information security, wireless networks, protection of networks from unauthorized access, protection of mobile devices, password, password generation, stable passwords, password policies

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Колективна монографія в іноземному науковому виданні:

1. Opirskyi Ivan. Use of near field communication technology for automated profile replication/ Opirskyi Ivan, Ivanchenko Ihor, **Platonenko Artem**, Skladannyi Pavlo, Roshchuk Mariia. // Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, Bielsko-Biala, Poland.

Статті в іноземних наукових виданнях:

2. Odiyanenko H. V. Evaluation of parameters and compensation of noises in protected telecommunication systems / H. V. Odiyanenko, G. N. Rozorynov, **A. V. Platonenko**. // Научно-практический журнал Западно-Казахстанского аграрно-технического университета имени Жангир хана "Наука и образование". – 2014. – С. 91–94.

3. Одияненко Е. В. Синтез оптимальной структуры системы защиты информации / Е. В. Одияненко, Г. Н. Розоринов, **А. В. Платоненко**. // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Часть I. – 2014. – С. 443–445.

Статті у наукових фахових виданнях України:

4. Розорінов Г. М. Захист інформаційних систем від потужних електромагнітних випромінювань / Г. М. Розорінов, **А. В. Платоненко**. // Сучасний захист інформації. – 2014. – №3. – С. 16–20.

5. Розоринов Г. Н. Пассивная оптическая сеть с кодовым разделением каналов / Г. Н. Розоринов, **А. В. Платоненко**. // Телекомунікаційні та інформаційні технології. – 2014. – №4. – С. 20–26.

6. **Платоненко А. В.** Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко. // Сучасний захист інформації. – 2015. – №4. – С. 86–90.

7. Аносов А. О. Модель перехоплення та захист інформації в бездротових мережах / А. О. Аносов, **А. В. Платоненко**. // Сучасний захист інформації. – 2017. – №2. – С. 90–94.

8. **Платоненко А. В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту / А. В. Платоненко. // Сучасний захист інформації. – 2017. – №1. – С. 128–132.

9. Аносов А. О. Генерування унікального паролю зі змінним правилом ускладнення / А. О. Аносов, **А. В. Платоненко**. // Сучасний захист інформації. – 2017. – №3. – С. 82–86.

10. Бурячок В.Л. Генерування паролю для бездротових мереж з використанням змінного правила ускладнення/ В.Л. Бурячок, А. О. Аносов, **А.В Платоненко**. // Захист інформації. – 2019. – Том 21, №1. – С. 52–59.

11. Бурячок В.Л. Вибір раціонального способу генерування паролів серед множини існуючих / В.Л. Бурячок, **А.В Платоненко**, О.В. Семко. // Безпека інформації. – 2019. – Том 25, № 1. – С. 59–64.

Публікації у наукометричних базах Scopus i Web of Science:

12. Vladymyrenko Maksym. Analysis of implementation results of the distributed access control system. / Maksym Vladymyrenko, Sokolov Volodymyr, Buriachok Volodymyr, **Platonenko Artem**. // Preprint. PIC S&T`2019 IEEE conference, Kyiv.

Тези наукових доповідей:

13. **Платоненко А.В.** Захист інформації у безпроводових мережах WI-FI./ Платоненко А.В. // Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави» – Київ: ДУТ, 2014 – С.40-41.

14. **Платоненко А.В.** Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах. / Платоненко А.В. // Науково-технічна конференція «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.34-35.

15. **Платоненко А.В.** Сучасні загрози інформаційної безпеки для пристроїв у корпоративних мережах. Матеріали Міжнародної науково-технічної конференції «Актуальні проблеми розвитку науки і техніки» – Київ: ДУТ, 2015 – С.128.

16. **Платоненко А.В.** Сучасні загрози інформаційної безпеки для державних та приватних установ України. / Платоненко А.В. // II Міжнародна науково-технічна конференція «Актуальні проблеми розвитку науки і техніки» – Київ: ДУТ, 2015 – С.137-138.

17. **Платоненко А.В.** Сучасні загрози інформаційної безпеки та засоби захисту від них. / Платоненко А.В. // Міжнародна науково-технічна конференція студентства та молоді «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.159-160.

18. **Платоненко А.В.** Актуальні загрози інформаційної безпеки сучасних мобільних пристроїв у мережах нового покоління. / Платоненко А.В. // II Міжнародна науково-практична конференція «Тенденції розвитку конвергентних мереж: рішення пост - NGN, 4G та 5G» – Київ: ДУТ, 2016 – С.182-183.

19. **Платоненко А.В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв в Україні. / Платоненко А.В. // III Міжнародна науково-технічна конференція студентства та молоді» – Київ: ДУТ, 2016 – С.134-136.

20. **Платоненко А.В.** Средства защиты современных мобильных устройств в сетях нового поколения / А. В. Платоненко, А. А. Аносов. // Региональная конференция «Перспективы предоставления услуг на основе сетей пост-NGN, 4G и 5G. Организационные и технические решения по их построению и защите» – Київ: ДУТ, 2017.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВСТУП

Розділ 1. Аналіз загроз та уразливостей для систем бездротового зв'язку

- 1.1. Загрози для мобільних пристроїв
- 1.2. Вразливості бездротових мереж Wi-Fi
- 1.3. Важливість питання стійкого паролю для користувачів
- 1.4. Атаки та статистика втрат від них
- 1.5. Модель перехоплення та захисту інформації в бездротових мережах

Висновки до першого розділу

Список використаних джерел у першому розділі

Розділ 2. Розробка способу обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку

- 2.1. Проблеми сучасних політик безпеки
- 2.2. Способи генерування паролів
- 2.3. Аналіз критеріїв для вибору необхідного способу генерування
- 2.4. Вибір найбільш доцільного для вдосконалення способу

Висновки до другого розділу

Список використаних джерел у другому розділі

Розділ 3. Вдосконалення способу генерування випадкових паролів

- 3.1. Особливості та вимоги до формування паролів у мережах Wi-Fi
- 3.2. Послідовність вдосконалення способу генерування паролів
- 3.3. Додаткове ускладнення при генеруванні способу

Висновки до третього розділу

Список використаних джерел у третьому розділі

Розділ 4. Дослідження запропонованих способів захисту бездротових мереж

- 4.1. Алгоритм генерування стійкого паролю зі змінним правилом ускладнення
- 4.2. Порівняння стійкості парольних множин
- 4.3. Програмна реалізація способу генерування паролів
- 4.4. Практична реалізація та опис використаного технічного обладнання

4.5. Вплив зовнішніх факторів на роботу бездротової мережі

4.6. Аналіз нового стандарту WPA3

Висновки до четвертого розділу

Список використаних джерел у четвертому розділі

ВИСНОВКИ

Додаток А. Акти впровадження

Додаток Б. Список опублікованих праць за темою дисертації

Додаток В. Відомості про апробацію результатів дисертації

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

НСД	– несанкціонований доступ
ПЗ	– програмне забезпечення
AES	– Advanced Encryption Standard (розширений стандарт шифрування)
SKIP	– Cisco Key Integrity Protocol (протокол ключової цілісності Cisco)
IEEE	– Institute of Electrical and Electronics Engineers (Інститут інженерів з електротехніки та електроніки)
GSM	– Global Mobile System for Mobile communications (глобальна мобільна система мобільного зв'язку)
3G	– третє покоління мобільних мереж
4G	– четверте покоління мобільних мереж
IoT	– Internet of Things (інтернет речей)
IP	– Internet Protocol (міжмережевий протокол)
MAC	– Media Access Control (контроль доступу до медіа)
SSID	– Service Set Identifier (ідентифікатор набору послуг)
TKIP	– Temporal Key Integrity Protocol (протокол тимчасової ключової цілісності)
WDS	– Wireless Distribution System (бездротова розподілена система)
WEP	– Wired Equivalent Privacy (Провідні еквівалентні конфіденційності)
Wi-Fi	– Wireless Fidelity (бездротова якість)
WPA	– Wi - Fi Protected Access (захищений доступ до Wi-Fi)
WPS	– Wi-Fi Protected Setup (захищенне налаштування Wi-Fi)

ВСТУП

Актуальність теми. Сучасні мобільні пристрої стали невід'ємною частиною нашого життя, але окрім зручності та багатьох технічних можливостей вони несуть за собою все більшу небезпеку для інформації, яка в них зберігається та передається.

З використанням високошвидкісних мобільних мереж, загрози інформаційної безпеки для державних та приватних установ дедалі збільшуються, оскільки працівники все частіше використовують мобільні пристрої для віддаленої роботи. Отже для зломисників відкриваються більші технічні можливості для здійснення атак, що потребує впровадження засобів захисту інформації.

Зважаючи, на таке, питання щодо забезпечення функціональної безпеки (доступності та цілісності) систем бездротового зв'язку є надзвичайно актуальними. Дослідженню проблеми захищеності бездротових мереж присвячені роботи Н. І. Битюцької, В. Л. Бурячка, О. Л. Весельської, В. І. Ніконова, С. В. Толюпи, Л.А. В. О. Хорошка, Шувалової, О. К. Юдіна, А.В. Чунарьової, L. Badman, R. Bartz, J. Doherty, F. Garzia та багатьох інших.

За їх висновками встановлено, що основними проблемами захищеності систем бездротового зв'язку є: вразливість паролів до підбору, відсутність обізнаності користувачів в налаштуванні та неефективне використання технічних засобів, велика кількість зломисного програмного забезпечення, що використовує збільшення технічних можливостей мобільного обладнання. Дані вразливості несуть небезпеку, як для користувачів особисто, так і для організацій де вони працюють.

Способи, які використовувались для вирішення даної проблеми (парольні політики користувачів з обмеженням по кількості символів; генерування паролів на основі поєднанні декількох слів, або заміни слів іншою мовою; генерування випадкових чисел для вибору слів за таблицею, генератори випадкових значень паролів з певної множини символів і т.п.), не повною мірою відповідають викликам сьогодення.

З огляду на це, розробка технології забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик за рахунок генерування паролів з використанням інтегрованого підходу, є **актуальною науковою задачею**, що має теоретичне і практичне значення.

Зв'язок роботи з науковими програмами, планами, темами.

Тематика дисертаційної роботи та одержані результати безпосередньо пов'язані з «Основними науковими напрямками та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014-2018 роки», а також Стратегією кібербезпеки України від 15 березня 2016 року №96/2016.

Результати роботи відображені у звітах з науково-дослідної роботи «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем (ІКС) в умовах впливу кібернетичних атак» (номер державної реєстрації 0114U000391), яка виконувалась в Державному університеті телекомунікацій й у якій здобувач брав участь у якості виконавця.

Мета і завдання дослідження. *Метою дисертаційної роботи є забезпечення відмовостійкості систем бездротового зв'язку за рахунок підвищення стійкості парольних політик до спроб несанкціонованого доступу.*

Досягнення поставленої мети вимагає вирішення таких **завдань**:

1) проведення аналізу множини існуючих актуальних загроз та уразливостей системам бездротового зв'язку, а також варіантів формування та застосування парольних політик для забезпечення функціональної безпеки таких систем в умовах кібернетичних атак;

2) розроблення методу обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, для забезпечення їх надійності і живучості в умовах кібернетичних атак, за рахунок вибору раціонального способу генерування паролів серед множини існуючих;

3) удосконалення способу або інакше методу генерування ускладнених паролів за показниками довжини та набору символів, з метою формування більш стійких паролів, у порівнянні з відомими способами-аналогами.

Зважаючи на таке **об'єктом дослідження** в роботі є процес забезпечення функціональної безпеки систем бездротового зв'язку. **Предметом дослідження** – інформаційна технологія забезпечення функціональної безпеки систем бездротового зв'язку в умовах загроз і обмежень, визначених специфічними умовами функціонування таких систем.

Методи дослідження. Проведені дослідження базуються на методах теорії множин (для формалізації процесів формування вимог до парольних політик, а також ідентифікації і визначення повноти їх забезпечення), теорії ймовірностей і математичної статистики (для розробки й дослідження алгоритмів генерування парольних множин), експертного оцінювання (для визначення коефіцієнтів стійкості, а також встановлення зв'язків між базовим способом генерування паролю та відповідними способами-аналогами), математичного моделювання (для оцінювання повноти виконання множини вимог), порівняння (для визначення оптимального способу генерування паролів), графічний (для відображення моделей атак та парольних множин), формалізації (для опису розробленого способу ускладнення паролів).

Наукова новизна отриманих результатів полягає в подальшому розвитку теоретичних і практичних методів та моделей забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик. Новими результатами, отриманими в дисертаційній роботі, є:

- вперше розроблений метод обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, **впровадження якого** за рахунок проведення процедури оцінки ступеня близькості між базовим способом генерування паролів і кожним способом-аналогом **дозволило**, на відміну від подібних, серед множини існуючих способів генерування паролів обрати спосіб, найбільш раціональний з точки зору його вдосконалення та забезпечити функціональну безпеку систем бездротового зв'язку в умовах впливу кібернетичних атак;

- удосконалений спосіб генерування випадкових паролів для систем бездротового зв'язку, **впровадження якого** завдяки урахуванню можливості співпадіння з паролями системи словників та використанню інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів (обраних за правилом комбінації з введенням певного ускладнення), **забезпечило** порівняно з аналогами підвищення рівня захищеності систем бездротового зв'язку стандарту IEEE 802.11 від можливого злому (спроб несанкціонованого доступу) в $3,73 \cdot 10^4$ разів.

Практичне значення отриманих результатів у сукупності складає підґрунтя для реалізації програмних засобів, для захисту систем бездротового зв'язку, що застосовуються на об'єктах інформаційної діяльності.

Практична цінність отриманих результатів полягає в програмній реалізації:

по-перше, методу формування паролівних політик, що дозволяє раціонально обрати спосіб генерування паролів серед множини існуючих;

по-друге, способу генерування ускладнених паролів в системах бездротового зв'язку, що дозволяє сформувати стійкий до підбору пароль.

Отримані результати забезпечують зменшення: витрат часу на створення паролю приблизно на 20%, а також ймовірності злому паролю шляхом збільшення часу для його можливого підбору в $3,73 \cdot 10^4$ разів.

Результати дисертаційного дослідження впроваджено у навчальний процес Київського університету імені Бориса Грінченка (акт впровадження від 15.04.2019), а також в практику розроблення політик інформаційної безпеки ТОВ "НТК"ТЕХНОЛОГІЇ БЕЗПЕКИ (акт впровадження від 20.03.2019) та ТОВ «Квадрокоптер» (акт впровадження від 19.04.2019).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належить: в [1,12] – дослідження видів атак на бездротові мережі та види їх захисту, [2] – аналіз підходів до оцінки захищеності мережі; в [3] – оптимізація алгоритму синтезу систем захисту інформації; в [4] – перелік можливих наслідків для засобів інформатизації та

аналіз можливих наслідків електромагнітного впливу в залежності від галузі використання інформаційних систем; в [5] – розгляд топології та видів розподілу, що використовуються; в [7,10] – аналіз вразливості бездротових мереж, описання та графічне зображення моделі перехоплення та захисту інформації в бездротових мережах; в [9, 11] – аналіз систем для підбору, розрахунки та графічне зображення способу.

Апробація результатів дисертації. Основні положення і результати досліджень доповідалися та обговорювалися на: Науково-технічній конференції «Актуальні проблеми забезпечення інформаційної безпеки держави» (м. Київ, 2014 р.); Студентській науково-технічній конференції молодих вчених присвячена Дню науки «Світ телекомунікації та інформатизації» (м. Київ, 2015 р.); Міжнародній науково-технічній конференції «Актуальні проблеми розвитку науки і техніки» (м. Київ, 2015 р.); Міжнародній науково-технічній конференції «Сучасні інформаційно-телекомунікаційні технології» (м. Київ, 2015 р.), Міжнародній науково-технічній конференції студентства та молоді «Світ телекомунікації та інформатизації» (м. Київ, 2015 р.); II Міжнародній науково-практичній конференції «Тенденції розвитку конвергентних мереж: рішення пост - NGN, 4G та 5G» (м. Київ, 2016 р.); III Міжнародній науково-технічній конференції студентства та молоді» (м. Київ, 2016 р.); Міжнародній конференції «Перспективы предоставления услуг на основе сетей пост-NGN, 4G и 5G. Организационные и технические решения по их построению и защите» (м. Київ, 2017 р.), Міжнародна науково-практична конференція «Проблеми інфокомунікаційних наук та технологій» (Problems of Infocommunications Science and Technology, м. Київ, 2019 р.).

Публікації. За результатами дисертаційної роботи опубліковано 20 наукових праць (11 статей, з них 9 – у співавторстві), серед яких: 9 наукових статей, написаних у співавторстві й опублікованих у наукових спеціалізованих фахових виданнях України та країн СНД, які включені до міжнародних наукометричних баз, 2 статті без співавторів. Разом з тим основні наукові результати додатково відображені у 8 тезах доповідей на науково-технічних конференціях, а також

видана за кордоном колективна монографія. Із праць, що опубліковано в співавторстві, у дисертаційній роботі використано виключно ті результати, які одержано здобувачем особисто.

Обсяг і структура дисертації. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, чотирьох розділів, загальних висновків, списків використаних джерел (в кінці кожного розділу основної частини дисертації) і має 120 сторінок основного тексту, 25 рисунків, 10 таблиць. Список використаних джерел містить 95 найменувань і займає 8 сторінок. Загальний обсяг дисертаційної роботи – 138 сторінок.

Розділ 1

АНАЛІЗ ЗАГРОЗ ТА УРАЗЛИВОСТЕЙ ДЛЯ СИСТЕМ БЕЗДРОТОВОГО ЗВ'ЯЗКУ

Інформаційна безпека не несе за собою можливості заробітку, оскільки потребує певних додаткових витрат, але завдяки цим витратам можливо захистити установи від значних майбутніх збитків.

Загрози інформаційної безпеки несуть за собою великі ризики, які можуть обернутись на значні збитки не тільки для організацій, що не впровадили систему захисту інформації, а і для цілої країни.

В наш час загрози інформаційної безпеки нажаль реалізуються дуже часто, адже кожного дня зловмисники знаходять нові вразливості, завдяки яким можуть нанести шкоду як для державних установ, так і для приватних організацій.

1.1. Загрози для мобільних пристроїв

Мобільними пристроями щоденно користується мільйони людей, але коли за безпекою своїх особистих даних мало хто слідкує, то у корпоративних мережах важливим фактором є збереження інформації, що в ній передається.

Нажаль шахраї знову й знову знаходять нові можливості для звершення несанкціонованого доступу до інформації (в компанії «Palo Alto Networks» щоденно звітують про знаходження більше ніж 25 тисяч нових зловмисних програм для мобільних пристроїв).

Постає питання захисту мобільних пристроїв, які можуть використовуватись за межами офісу компанії та створювати нові загрози для витоку інформації.

Завдяки спеціальним технічним рішенням, які стають частиною корпоративної мережі та програмному забезпеченню на пристроях користувачів мобільних пристроїв з'являється змога запобігти небажаним втратам важливої для них інформації.

Для ефективного захисту мобільних пристроїв замало тільки встановленого на них програмного забезпечення.

Важливими з точки зору безпеки є правила роботи в мережі, перелік дозволених програм та формату файлів, що в них можна використовувати, адже дуже велика кількість зловмисних програм приховується за розповсюдженими форматами документів (зокрема *.pdf).

Саме тому краще віддавати перевагу хмарним сервісам, які оцінюють поведінку файлів та допомагають швидше визначити можливу загрозу, ніж після оновлення бази сигнатур антивірусу.

Окрім цього, ніколи не потрібно забувати про людей, які користуються мобільними пристроями, адже саме вони через свою неуважність можуть випадково встановити зловмисне програмне забезпечення, що заблокує їх пристрій та буде вимагати кошти за розшифрування інформації, або ще гірше, розповсюдиться на весь список контактів.

Наприклад відома атака в кінці 2014 року «Привіт! Тобі фото...», що заразила мільйони мобільних телефонів українців, залишаючи їх без грошей на рахунку та змоги навіть отримати повідомлення чи прийняти дзвінок від інших абонентів, на декілька місяців стала проблемою для мобільних операторів і вповноважених фахівців спецслужб.

Нажаль, Україна зайняла п'яте місце у світовому рейтингу з ризику зіткнення з веб-загрозами. За третій квартал 2015 року третина (33,7%) користувачів антивірусних продуктів зіткнулась із загрозами, які розповсюджується через мережу Інтернет.

Проблемою є відсутність оновлення програмного забезпечення та використання піратських програм. Біля 17% заражень було здійснено на користувачів застарілої Windows XP.

Також небезпечними є шифрувальні програми, що вимагають гроші після шифрування файлів, доступ до яких не можливий без спеціального ключа.

На рис. 1.1 зображена структурна схема захищеної корпоративної мережі з використанням мобільних пристроїв.

Інформація з мережі Інтернет та корпоративної мережі передається через мережевий екран, до якого підключений прилад управління мобільними пристроями, який в свою чергу керує мобільними підключеннями до мережі та має доступ до хмарного сервісу, за допомогою якого можна отримати захист від вірусів «нульового дня».

Завдяки такому приладу управління можна отримати: статистику загроз, засоби захисту від зловмисного коду в програмах для мобільних пристроїв, створення та управління правилами безпеки для мобільних пристроїв у мережі [2].

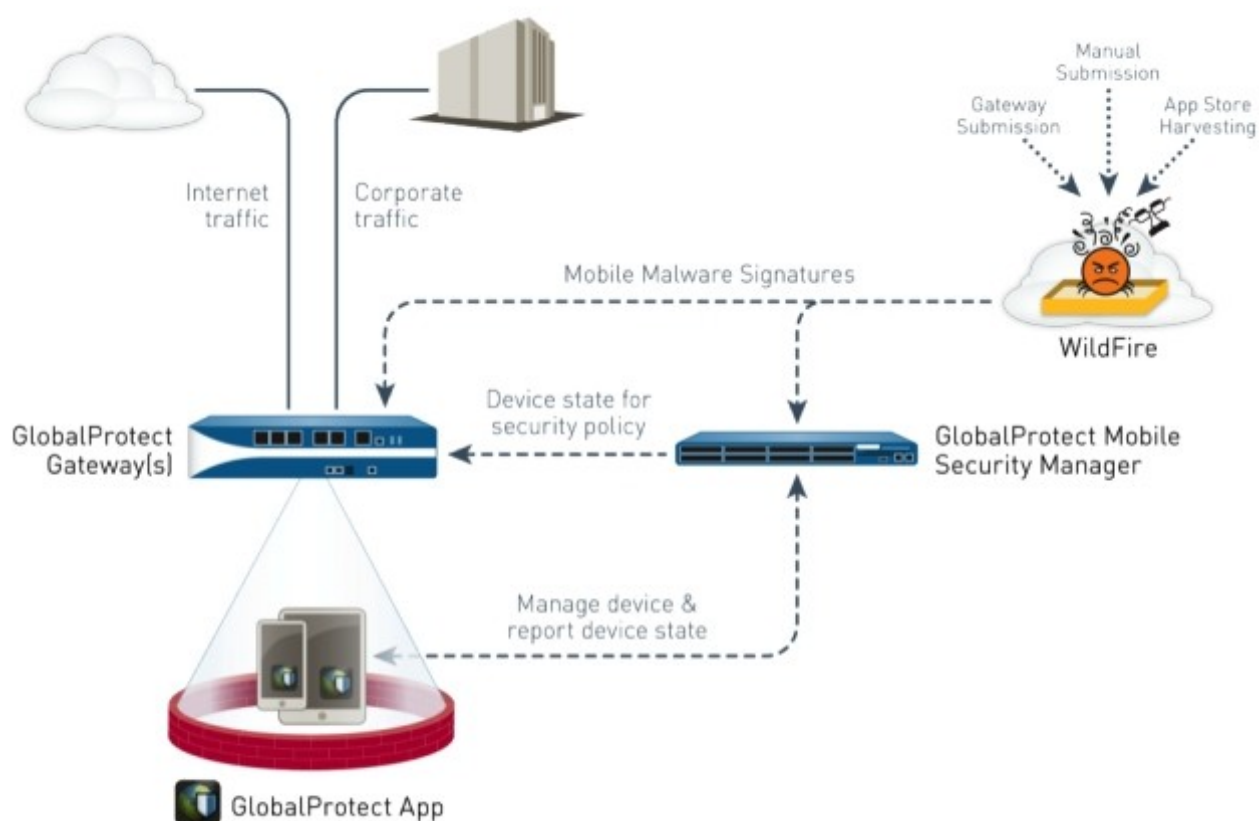


Рис. 1.1. Структурна схема захищеної корпоративної мережі з використанням мобільних пристроїв

Практично кожен другий мешканець нашої держави (45%) має смартфон з сенсорним екраном. Порівняно з 2015 роком простежується зростання користувачів з 26% до 45%, у випадку загального населення (рис. 1.2), та з 59% до 85% – у випадку осіб до 30 років.

При цьому, якщо серед молоді 85% користуються смартфонами, то серед осіб літнього віку цей показник становить всього 6%.

В останні два роки частка застосування смартфонів мешканцями України виросла на 26%. За прогнозами світових лідерів до 2020 року вона досягне більш ніж 70%. Нині понад 68% користувачів смартфонів мають досвід встановлення додатків.

Недосвідчені користувачі мобільних пристроїв випадково встановлюють зловмисне програмне забезпечення, яке може нанести особисту шкоду, чи принести збитки організації, в якій вони працюють.

Кількість мобільних підключень в Україні вже становить більш ніж 58,2 млн, з яких 26% становлять 3G-підключення. Оскільки через 5 років більших обсягів наберуть мережі 4G кількість мобільних підключень в Україні зросте майже на 6 млн.

Загалом же по усьому світу до мереж мобільної передачі даних в цей період приєднається понад 2,6 млрд нових абонентів.

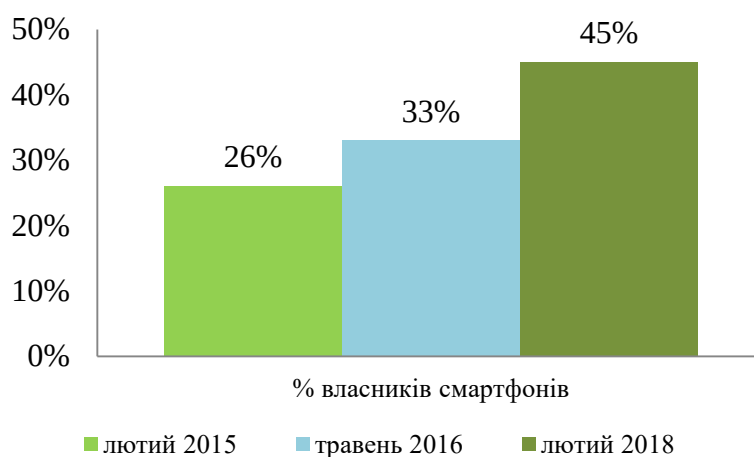


Рис. 1.2. Кількість власників смартфонів в Україні

Підробні зарядні пристрої. Коли на мобільному пристрої закінчується заряд, особливо, якщо смартфон потрібен, щоб переглядати карти, маршрути і довідкову інформацію, власник шукає змоги його зарядити якнайшвидше, нехай навіть на кілька хвилин.

Сучасні смартфони та планшети - це високотехнологічні пристрої, які використовують LTE-з'єднання або звичайний Wi-Fi, і, відповідно, вони витрачають багато енергії.

Ось чому багато мандрівників шукають будь-яку можливість зарядити свій мобільний пристрій хоч де-небудь, нехай навіть на автобусній зупинці, в залі очікування або в будь-якому громадському місці.

При цьому вони забувають про одне дуже важливу обставину: не можна бути впевненим, що зарядний пристрій, який вони готові використовувати є безпечним.

Підробний зарядний пристрій цілком здатний зарядити Ваш пристрій, але при цьому ще непомітно скопіює інформацію з вашого смартфона, коли зарядка відбувається через порт USB.

В деяких випадках таке місце зарядки може ще й встановити шкідливе ПЗ на ваш смартфон, щоб відстежувати, де Ви знаходитесь, і буде це робити навіть коли ви поїдете; він також може скопіювати ваші замітки, список контактів, фотографії, SMS-повідомлення (і повідомлення інших систем обміну повідомленнями), журнали дзвінків, паролі, збережені на пристрої, і навіть cookie-файли браузера [4].

1.2. Вразливості бездротових мереж Wi-Fi

Небезпеку для інформації несуть також і відкриті Wi-Fi мережі, адже кожен має змогу підключитись до них та виконувати певні зловмисні дії.

Небезпечними також можна вважати і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись, наприклад, дізнавшись пароль у працівника [3].

Розповсюдженою проблемою залишаються бездротові мережі, якими щоденно користуються мільйони людей.

У американського оператора стільникового зв'язку «AT & T» є послуга, що надається всім покупцям смартфонів на базі iOS і Android: кожен придбаний телефон, містить список фірмових довірених бездротових мереж, до яких власник телефону може підключатися без будь-яких побоювань .

Більш того, до присутніх у списку точок доступу пристрої будуть підключатися автоматично, як тільки виявляться в зоні покриття сигналу. Але є важливий нюанс: одного разу підключившись до певної бездротової мережі, смартфон або планшет в майбутньому теж буде підключатися, але вже до будь-якої іншої точки доступу, що має ту ж назву мережі і SSID.

Звичайно, це зручно: не потрібно кожного разу ініціювати з'єднання вручну, досить просто опинитися в зоні дії сигналу. Однак є не всім очевидна проблема: підключаючись до такої мережі, не можна бути впевненим в тому, що вона безпечна.

З однаковою ймовірністю точка доступу, до якого тільки що підключився мобільний пристрій, може виявитися як абсолютно недоступним для злоумисників, так і з відкритими вразливостями.

Навіть якщо дана бездротова точка доступу фігурує в списку довірених оператора або інтернет-провайдера, сказати напевно, що вона належить саме їм, Ви не зможете.

Оскільки ніхто не заважає шахраям створити свою бездротову мережу, назвавши її в точності так само, як і фірмову точку доступу стільникового оператора, і організувати атаку типу «людина посередині», збираючи з нічого не підозрюючих користувачів дані облікових записів і заражаючи їх пристрою злоумисним ПЗ [5].

Частою помилкою користувачів є довіра до відкритих мереж, тобто мереж які не використовують пароль для підключення до неї, а отже й не дають змогу шифрування інформації, що передається.

Для захисту інформації, яка передається бездротовими мережами можна виділяють такий перелік рекомендацій:

- зміна параметрів доступу адміністратора до налаштувань;
- обмеження доступу з фільтрації MAC-адрес (англ. Media Access Control);
- режим прихованого ідентифікатора SSID (англ. Service Set Identifier);
- використання стандарту WPA2, 801.11i (WI - FI Protected Access2);

- відключення стандарту WPS (англ. Wi-Fi Protected Setup);
- створення віртуальних персональних мереж (VPN).

Часто вважають, що приховані мережі дуже складно виявити чи підключитися до них. Однак, «прихована» мережа - не що інше, як мережа, що не передає дані про своє існування 10 разів на секунду, або передає їх, але з порожнім ESSID та іншими полями.

Як тільки до такої мережі підключається клієнт, він передає її ESSID і пароль, і якщо така мережа існує в радіусі дії - точка доступу відповідає на запит і проводить всі звичайні процедури по авторизації і передачі даних.

А якщо клієнт вже був підключений раніше - його можна побачити в списку активних підключень та відключити.

Кожен підключений клієнт спілкується з базовою станцією через її BSSID - і це саме те, що зловмисник може бачити у відповідних таблицях при скануванні мереж.

Є змога просто «відключити» клієнта від мережі, після чого він повинен буде підключитися знову - і в цей момент зловмисне ПЗ перехопить «рукоштовування» з усіма ідентифікаторами і ключами.

Також можливо просто залишити ноутбук включеним на пару годин зі зловмисним ПЗ на потрібному каналі і почекати.

При успішному «взломі» мережі з'являється повідомлення з BSSID точки доступу, конспірацію якої вже розкрито [6].

Нажаль, зловмисники завдяки спеціалізованому програмному забезпеченню, досить легко зможуть підмінити MAC-адресу, визначити прихований ідентифікатор, а також підібрати PIN-код підключення до точки безпроводного доступу, але підібрати пароль стандарту WPA2, який може досягати до 63 символів, буде досить тяжко, якщо він не сформований зі звичних слів, що є у базі словників з паролями, які часто використовуються.

Ще більш надійним є варіант використання спеціалізованих серверів авторизації, які періодично генерують нові паролі, а також віртуальних персональних мереж, які додатково будуть шифрувати інформацію, що передається через загальну мережу.

Основні фрагменти неприємної головоломки під назвою «Незахищеність мобільних» - це погано захищені мережі Wi-Fi і неякісна реалізація заходів безпеки в мобільних додатках.

Стільниковий доступ в Інтернет залишається досить дорогим у багатьох випадках, особливо якщо ви подорожуєте за кордоном. Тому майже всі регулярно використовують Wi-Fi в аеропортах, кафе і готелях, не звертаючи особливої уваги на захищеність цих мереж. А вона, на жаль, не така висока, як хотілося б.

Дослідження експертами мереж в Сан-Паулу і виявили, що кожна четверта мережа працює в «відкритому» режимі, тобто не шифрує дані при обміні ними з підключеними пристроями.

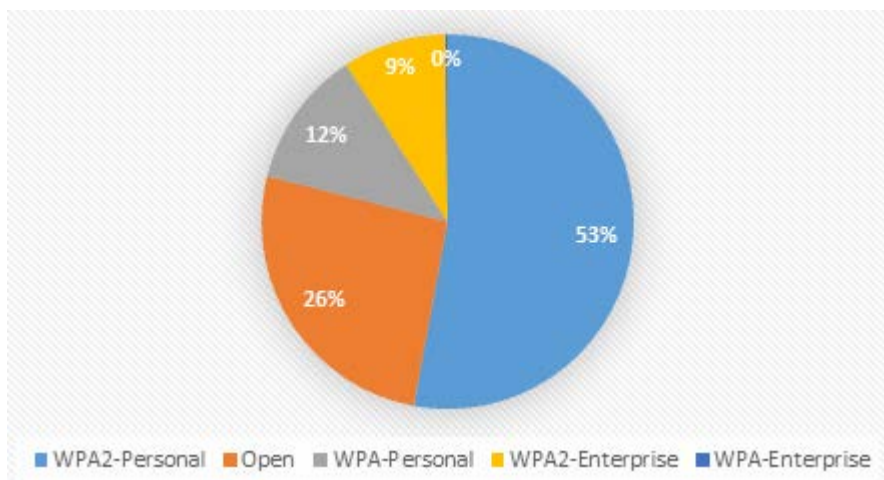


Рис. 1.3. Захищені мережі в Сан-Паулу

Безліч мереж по всьому світу може бути зламано за лічені секунди. Необхідно підключатися тільки до мереж, які використовують захист WPA2. Проаналізувавши більше п'яти тисяч різних точок доступу, фахівцями було виявлено, що не менше 53% з них мають WPA2-аутентифікацію.

Однак викликає тривогу той факт, що 26% всіх мереж є повністю відкритими і ніяк не шифруються. На жаль, часто доводиться підключатися до єдиної наявної мережі.

На смартфонах і планшетах зазвичай немає ніякого контролю за тим, що передається в мережу. Якщо в мобільному браузері можна хоча б побачити в рядку адреси замок, який показує, що використовується захист протоколу HTTPS, то з мобільними додатками зовсім інша історія.

Важко уявити собі, як багато мобільних додатків створені з помилками, якщо навіть компанії першого ешелону їх допускають.

На жаль, серед уразливих додатків є навіть банківські. Мобільні додатки майже ніколи не попереджають користувача про проблеми з SSL-сертифікатами, тому виявити атаку методом «людини посередині» практично неможливо [7].

Крім небезпеки підключитися до мережі, створеної шахраями, у ввімкненого весь час Wi-Fi є ще один недолік - він дозволяє стороннім організаціям стежити за вами. Наприклад, коли Ви заходите в торговий центр з включеним Wi-Fi, Ваш телефон починає шукати точку для підключення до мережі. При цьому він транслює свою власну унікальну MAC-адресу.

Кожен Wi-Fi-приймач, який отримав запит про підключення від Вашого пристрою, може заносити дані про таких запитах в журнал. На базі цих записів маркетингологи часто будують карту пересувань клієнтів, щоб подивитися, хто і скільки часу проводить в якому відділі [8].

Найпопулярнішим в Сан-Паулу виробником Wi-Fi обладнання є CISCO, на другому місці D-Link (рис.1.4).

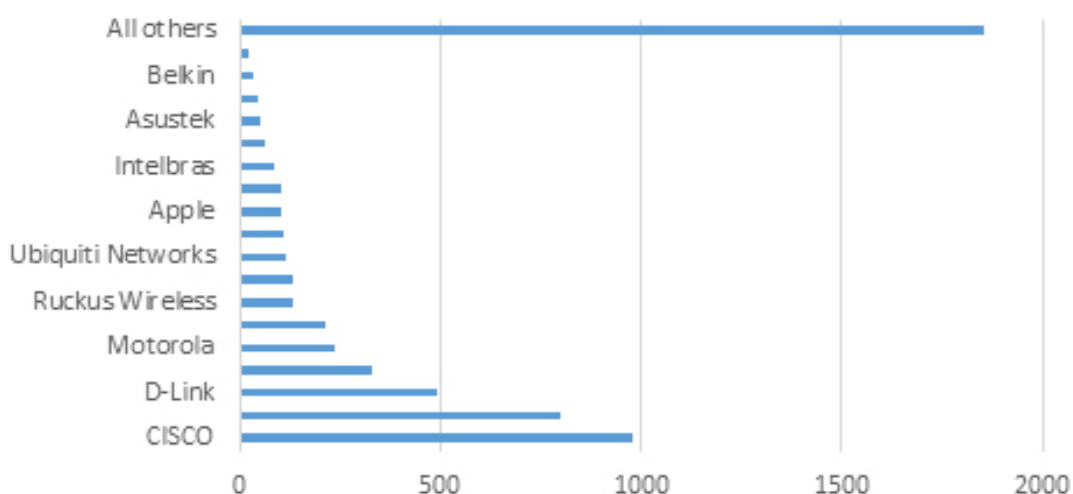


Рис. 1.4. Виробники точок доступу Wi-Fi у Сан-Паулу

У більшості виробників точок доступу, налаштування безпеки (і особливо оновлення прошивок) встановлюються «за вимогою» - таким чином, що залежать від цілеспрямованих дій самого користувача.

Це означає, що навіть якщо існує відома уразливість, за допомогою якої зловмисники можуть віддалено отримати повний доступ до пристрою з правами адміністратора, то така вразливість не може бути автоматично усунена.

Для цього потрібно, щоб користувач (власник точки доступу) зайшов на сайт виробника завантажив оновлення для вбудованого програмного забезпечення, потім підключив свій пристрій Ethernet-кабелем до модему і завантажив нову версію прошивки.

Для власників Wi-Fi пристроїв цей процес в цілому досить складний - вони часто навіть не знають, як перевірити пристрій на наявність вразливостей.

Таким чином, багато точок доступу не отримують оновлень безпеки і залишаються уразливими для віддалених атак.

1.3. Важливість питання стійкого паролю для користувачів

Нестійкі паролі зазвичай стають причиною кібератак. Після того як зловмисник підключиться до мережі, він отримує доступ до всіх підключених пристроїв. Крім того, якщо нестійкий або стандартний пароль використовується для панелі налаштувань, то всі пристрої піддаються ризику кібернетичної атаки, яка може здійснюватися віддалено.

Застосування таких розповсюджених паролів як «1q2w3e4r» і «123qwe» показує, що деякі користувачі намагаються використовувати поєднання символів для створення захищених паролів, проте їх зусилля є недостатніми, оскільки програми для злому паролів, засновані на словниках, в першу чергу аналізують такі поширені варіанти.

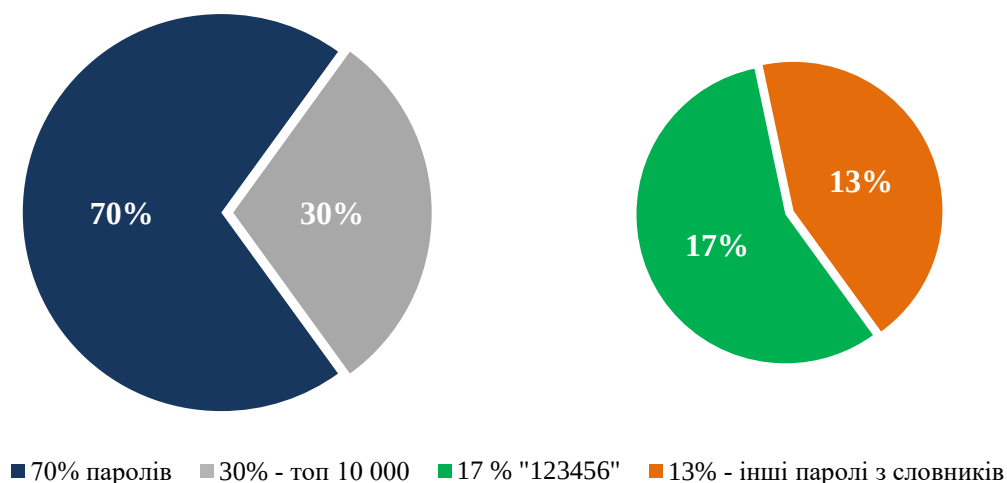


Рис. 1.5. Розподіл паролів користувачів

При цьому, наприклад, 30% користувачів використовують в якості пароля слово з топ - 10 000 паролів. З них майже 17% облікових записів банально захищені відомим паролем «123456» (рис. 1.5), або йому подібним [3].

За даними аналітиків інформаційної безпеки в найближчі роки інформаційна безпека матиме найбільший вплив на ІТ-стратегію компаній.

Підтвердженням цього є масові приклади глобальних атак, як на користувачів так і на локальні та міжнародні компанії, на протязі декількох останніх років, що стали проблемою для багатьох країн світу (зокрема відомі в Україні BlackEnergy, WannaCrypt, Petya.A, а також атаки на облікові записи користувачів міжнародних компаній: Apple, Sony, Gmail, Yahoo, Steam, та ін.), що показує актуальність та необхідність використання надійних засобів захисту інформації.

1.4. Атаки та статистика втрат від них

Основні загрози інформаційній безпеці організацій (рис. 1.6) несуть забезпечення мобільності співробітників (51%) та Інтернет речей (21%).

Основні загрози інформаційної безпеки для організації



Рис. 1.6. Основні загрози інформаційної безпеки для організацій

Одна з наймасовіших вірусних атак була проведена в середині травня 2017 г. Це стало можливо завдяки використанню шкідливого ПО.

Вірус WannaCrypt (також відомий як WCry і WanaCrypt0r 2.0) 12 травня 2017 року вразив велику кількість комп'ютерів під управлінням операційної системи Microsoft Windows.

Від вірусу постраждали комп'ютери приватних осіб, комерційних організацій, урядових установ. WannaCrypt завдав збитків більш ніж на \$ 1 млрд. і приніс творцям дохід у сумі \$ 116,5 тис, заразивши більше 200 000 комп'ютерів в більш ніж 150 країнах світу.

Це не просто атака на домашні або мобільні комп'ютери, а вже загроза для життя і здоров'я громадян.

Від вірусу постраждало близько 48 лікарень і клінік Британської національної служби охорони здоров'я.

Деякі госпіталі навіть призупинили прийом нових пацієнтів, а весь персонал був відправлений додому [x1].

На рис. 1.7 схематично відображено пристрої, які використовують бездротові мережі для передачі даних в сучасних містах.

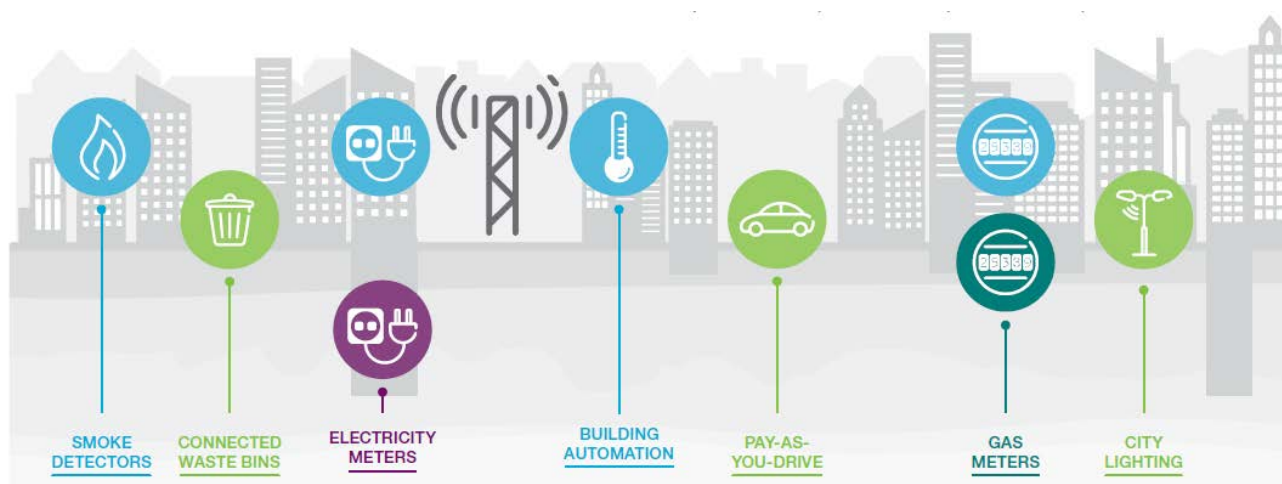


Рис. 1.7. Використання пристроїв, що використовують бездротові мережі в містах

80% власників мереж взагалі не змінюють паролі доступу. В їх число входять і мережі компаній [8+].

Команді китайських дослідників з Keen Security Lab, підрозділ китайського інтернет-гіганта Tencent, вдалося віддалено отримати несанкціонований доступ до електромобіля Tesla Model S, використовуючи уразливість в його мультимедійній системі.

Дослідники, зокрема, підключивши автомобіль до зловмисної точки доступу Wi-Fi, успішно змогли змінити положення водійського сидіння, відкрити люк, активувати двірники, скористатися GPS і навіть задіяти гальма, коли автомобіль був у русі на відстані близько 20 км від них.

Крім того, вони повністю контролювали інформаційно-розважальну систему автомобіля і панель приладів [9].

Захист периметра корпоративної мережі є одним з найбільш поширених способів захисту даних організації. Його використовують для безпечного підключення корпоративної мережі до Інтернету і для забезпечення доступу до неї віддалених користувачів. Однак сьогодні рівень значимості периметра безпеки знижується. Часто це відбувається завдяки поширенню мобільних і хмарних технологій, що дозволяють співробітникам працювати за межами корпоративної мережі.

Разом з зручністю з'являється і необхідність додатково стежити за потенційними загрозами незахищених підключень. Це підштовхує організації або до адаптації захисту периметра до цих змін, або використання принципово нових рішень.

Більшість компаній поки дотримуються модернізації периметра, але розширення способів доступу і постійно зростаючі обсяги даних роблять даний спосіб менш ефективним.

Мобільні пристрої виходять в Інтернет, минаючи його, а використання сторонніх додатків збільшує шанс витоку даних. Все зводиться до того, що на периферійних пристроях занадто багато прогалин, щоб цей підхід був життєздатним.

Великою проблемою є соціальна інженерія. Зловмисники завдяки соціальним мережам, фішинговим та зловмисним сайтам розповсюджують свої програми.

Таким чином може постраждати не тільки користувач особисто, а і компанія, працівником якої він є.

Нажаль ця проблема стала дуже розповсюдженою ще і завдяки використанню USB-накопичувачів, на яких встановлено зловмисне програмне забезпечення. Зловмисники залишають їх у загальних місцях, де працівники проводять вільний час.

Після підключення знайдених носіїв інформації до комп'ютерів, злочинці вже можуть віддалено отримати доступ і нанести шкоду для всієї організації.

Лише за 8 місяців 2015 року правоохоронними органами України вже було зафіксовано понад 20 тис. незаконних операцій з платіжними картками фізичних осіб, які спричинили збитки на суму близько 500 млн. грн.

Це лише ті факти, які вдалося зафіксувати і встановити. В окремих випадках заяви від банків до МВС не надходять.

Банківські працівники намагаються своїми силами встановити зловмисників. Для отримання інформації про банківські рахунки злочинці йдуть на дуже дорогі та витратні заходи.

Вони наймають фахівців, розробляють спеціальні програми для викрадення баз даних з комерційних структур, які накопичують таку інформацію.

Саме тому вдвічі більше фахівців різних компаній першочергову увагу приділяють питанню інформаційної безпеки.

Сучасні механізми забезпечення безпеки слід перемістити максимально близько до даних, щоб навіть у разі проникнення всередину периметра атакуючі не могли ними скористатися.

Незважаючи на це, згідно з результатами опитування Gemalto, 86% організацій збільшили свої інвестиції в забезпечення периметра і понад дві третини (68%) планують підвищити їх.

При цьому 69% з них не впевнені, що їх дані залишаться в безпеці в разі порушення його захисту, а більше половини вважають, що неавторизовані користувачі можуть мати доступ до їх мережі.

З кожним роком невпевненість зростає, так в 2014 р число таких респондентів становила 59%, а в 2015-му вже 66% [10].

За перші шість місяців 2016 року кількість витоків даних збільшилась на 15%. На глобальному рівні в першій половині 2016 року було зафіксовано 974 витоків, в результаті яких в небезпечними виявилися більш 554 мільйонів записів даних, в порівнянні з 844 витоками і 424 мільйонами скомпрометовані записами за попередні шість місяців.

Варто зазначити що:

- в 52% випадків витоків із зафіксованих в першому півріччі 2016, не уточнювалася інформація про кількість записів, які опинилися в руках зловмисників.
- на частку організацій сфери охорони здоров'я довелося 27% всіх витоків даних, і їх кількість збільшилась в порівнянні з 25% за попередні шість місяців.
- при цьому на підприємства галузі охорони здоров'я довелося лише 5% всіх скомпрометованих записів даних, в порівнянні з 12% за попередні шість місяців.

- частку державного сектора довелося 14% всіх витоків даних, що практично відповідає їх кількості за останні 6 місяців 2015 року, при цьому на їх частку припало 57% всіх скомпрометованих записів.
- на компанії сектора фінансових послуг припало 12% всіх витоків, що на 4% нижче в порівнянні із значенням за попередні шість місяців, при цьому на їх частку припало лише 2% всіх скомпрометованих записів.
- на частку підприємств роздрібно́ї торгівлі довелося 11% витоків, що на 6% нижче минулого значення, при цьому всього підприємствами роздрібно́ї торгівлі було скомпрометовано 3% записів даних.
- на частку організацій освітньої сфери припало 11% витоків даних, і менше одного відсотка всіх скомпрометованих записів даних.
- на інші галузі припало 16% витоків і 16% викрадених записів.

З точки зору географії трьома основними регіонами, в яких відбувалися зареєстровані витоків даних, стали:

- Північна Америка (79%),
- Європа (9%),
- Азіатсько-тихоокеанський регіон (8%) [11].

Технологія RFID використовується в найрізноманітніших галузях. Зокрема, одним із найпоширеніших способів використання технології є системи фізичного контролю доступу, в яких вимірювання спектру використовуються для ідентифікації користувачів, розташованих у певній місцевості [10+].

Технологія NFC дозволяє передавати дані на відстані до 10 см по радіо сигнал. Сучасні мобільні телефони на базі Android підтримують технологію HCE, що дозволяє запрограмувати обробник служби для вхідних команд NFC, перебуваючи на рівні ОС, гарантується, що дані, отримані від контролера, будуть отримані виключно за даною заявкою.

Практична швидкість роботи NFC (близько 400 кбіт/с) не дозволяє передавати великі обсяги даних, і, таким чином, цей канал може використовувати для початкового обміну ключами для встановлення альтернативного зашифрованого каналу для прямої передачі даних.

Підключення через Bluetooth, Wi-Fi тощо можна використовувати як приклади альтернативного каналу.

Крім того, використання технології NFC дозволяє використання мобільного телефону як ключового та для відстеження того, чи знаходиться він у полі зчитувач NFC.

Як тільки телефон вийме з поля, можна очистити синхронізований профіль з комп'ютера.

Це вирішує питання тимчасово розгортання профілю користувача, включаючи логіни, паролі, налаштування браузера та інші дані на робочому місці.

Для передачі по захищеному каналу профіль користувача архівується в ZIP архів для зменшення обсягу переданих даних та використання вбудованої ZIP перевірки цілісності.

Після передачі на мобільний пристрій файл негайно зберігається у внутрішньому пам'яті пристрою.

Інші програми не зможуть отримати доступ до внутрішньої пам'яті нашого додатку, оскільки ОС Android використовує для кожного окремі середовища програма, що працює в системі.

Для забезпечення додаткової безпеки дані також шифруються на ключ, який не можна безпосередньо вимагати від самої програми. Ключовий механізм використовується для зберігання ключа.

Через цей механізм ключ може бути тільки отримується, якщо користувач вводить правильний код доступу. Такий підхід дозволяє уникнути ризиків, пов'язаних з втратою телефону та нешифрованим аналізом файлової системи.

Метод заснований на використанні технології NFC, як каналу налаштування ключа сеансу є зручним для користувачів, дозволяє аутентифікацію користувача через смартфон та дані профілю, що копіюється в цільова система, створюється як тимчасові файли, таким чином, з правильним закриттям Java, всі дані будуть видалені.

Окрім того, можна стверджувати, що атака «людина по середині» проти протоколу NFC практично неможливо виконати, і тому вона є можливістю

використовувати розроблений метод як додатковий захід під час двофакторного аутентифікації [11+].

Один із варіантів атаки на безпроводову мережу реалізували співробітники компанії iTrust, дослідницького центру по кібербезпеці при Сінгапурському університеті технологій і дизайну. Вони придумали досить оригінальний спосіб перехоплення сигналів бездротового принтера за допомогою закріпленого смартфона на безпілотному літаючому засобі.

На рис. 1.8 зображена структурна схема даної атаки. Спочатку система розроблялася для підприємств? як недорогий спосіб перевірки безпеки Wi-Fi мереж, але в процесі роботи над проектом дослідники виявили, що їх розробка може також використовуватися в зловмисних цілях.

Потенційними жертвами системи є бездротові принтери, які зазвичай являються найслабшою ланкою в бездротовій мережі компанії.

Як правило, вони поставляються з відкритим Wi-Fi з'єднанням і багато компаній просто забувають змінити налаштування при підключенні пристрою до мережі, залишаючи стандартні налаштування.

Це відкрите з'єднання потенційно може бути використане сторонніми в якості точки доступу для підключення до мережі та крадіжки важливої інформації.

Розроблена дослідниками система сканує незахищені бездротові принтери і попереджає користувача у разі виявлення вразливого пристрою. Також можливо виконувати аналогічну операцію, але не зупинятись на виявленні пристрою, а проникнути у безпроводову мережу.

Для цього створюється підробна точка доступу, яка видає себе за бездротовий принтер. У разі успішного втілення зловмисного плану в реальність можна вільно перехоплювати усі документи, що відправляються співробітниками компанії на друк, і за декілька секунд перенаправити їх в хмарне середовище, використовуючи підключення мобільного телефону, який знаходиться на безпілотному літаючому засобі.

В даному випадку існують певні особливості та труднощі, наприклад

безпілотний літаючий засіб із смартфоном повинен знаходитись в радіусі 25 метрів від мережі.

Тобто, використовуючи подібний метод існує великий ризик викриття. Але даний вид атаки є досить цікавим та заслуговує на увагу, враховуючи стрімкий розвиток використання безпілотних літаючих засобів по всьому світу [2].



Рис. 1.8. Структурна схема злому бездротових принтерів з використанням мобільного телефону, що закріплений на безпілотному літаючому засобі

Компанія Fortinet спільно з партнерами розробила безкоштовну програму оцінки загроз для організацій.

В ході підготовки до проведення процедури оцінки в мережі клієнта встановлюється високопродуктивний брандмауер нового покоління FortiGate, який перевіряє внутрішньо-мережевий трафік додатків на наявність порушень, шкідливого ПЗ і додатків, за допомогою яких зловмисники можуть отримати доступ до файлів конфіденційних даних і нанести компанії-клієнта значної шкоди. Після закінчення періоду збору даних за допомогою засобу FortiAnalyzer створюється докладний звіт про загрози, що містить детальні відомості про трафік додатків, продуктивності користувачів, використання

бездротової мережі, загальну схильність мережі до ризику втрати даних і супутні ділові ризики.

В результаті реалізації програми ретельного аналізу існуючих і потенційних загроз клієнти отримують достовірну уяву про ризики, що загрожують їх мережам, а компанія Fortinet і її партнери рекомендують заходи щодо зниження цих ризиків.

Таким чином, тепер компанії-клієнти можуть бути спокійні за збереження найважливіших ресурсів.

Незалежно від розміру і організаційної форми, компанії стикаються з величезною кількістю серйозних загроз: число атак, яким піддалися мережі, перевищує 32,14 мільйона.

В свою чергу трафік соціальних мереж і мультимедійних потоків становить 25,65% всього мережевого трафіку.

Це підвищує ризик ураження корпоративних мереж і конфіденційних даних за допомогою прихованих завантажень, соціальної інженерії і шкідливої реклами.

Найбільший обсяг трафіку припадає на частку соціальної мережі Facebook - 47,27% трафіку соціальних мереж.

У той же час 42,29% трафіку потокового вмісту проходить через сервіс YouTube.

Так як розкрадання фінансових даних в результаті проникнення в бездротові мережі державних установ, банків і фінансових організацій приносить зловмисникам найбільш значний дохід, саме ці організації найчастіше стають об'єктами атак: на їх частку припадає понад 44,6% акцій кіберзлочинців [12].

Широко зустрічаються терміни WPA і WPA2 визначають, фактично, алгоритм шифрування (TKIP або AES). В силу того, що вже досить давно клієнтські адаптери підтримують WPA2 (AES), застосовувати шифрування за алгоритмом TKIP немає сенсу.

Різниця між WPA2 Personal і WPA2 Enterprise полягає в тому, звідки беруться ключі шифрування, які використовуються в механіці алгоритму AES. Для приватного (домашнього) застосування використовується статичний ключ (пароль, кодове слово, PSK) мінімальною довжиною 8 символів, яке задається в налаштуваннях точки доступу, і у всіх клієнтів даної бездротової мережі однаковим.

Компрометація такого ключа (поділились з сусідом, звільнився співробітник, вкрали ноутбук) вимагає негайної зміни пароля у всіх, хто лишився користувачів, що реалістично тільки в разі невеликого їх числа.

Для корпоративного використання, застосовується динамічний ключ, індивідуальний для кожного працюючого клієнта в даний момент.

Цей ключ може періодично оновлюватися по ходу роботи без розриву з'єднання, і за його генерацію відповідає додатковий компонент - сервер авторизації, і майже завжди це RADIUS-сервер.

Оскільки велика кількість компаній дозволяє використовувати мобільні пристрої для віддаленої роботи, а завдяки соціальним мережам спілкуються зі своїми клієнтами, то необхідно забезпечити певний рівень захисту користувачів від можливих загроз.

Організації постійно піддаються кібератакам. Кількість напрямків атак різко збільшилася, використовувані зловмисниками екосистеми стали більш просунутими.

Щоб захистити ІТ-ресурси в цих умовах, компанії повинні проявляти особливу пильність.

На рис. 1.9 жирні лінії показують пакети, які перехоплюються в різних режимах, а переривчасті лінії - це пакети, що приймаються антеною, але відкидаються драйвером, через обраний режим.

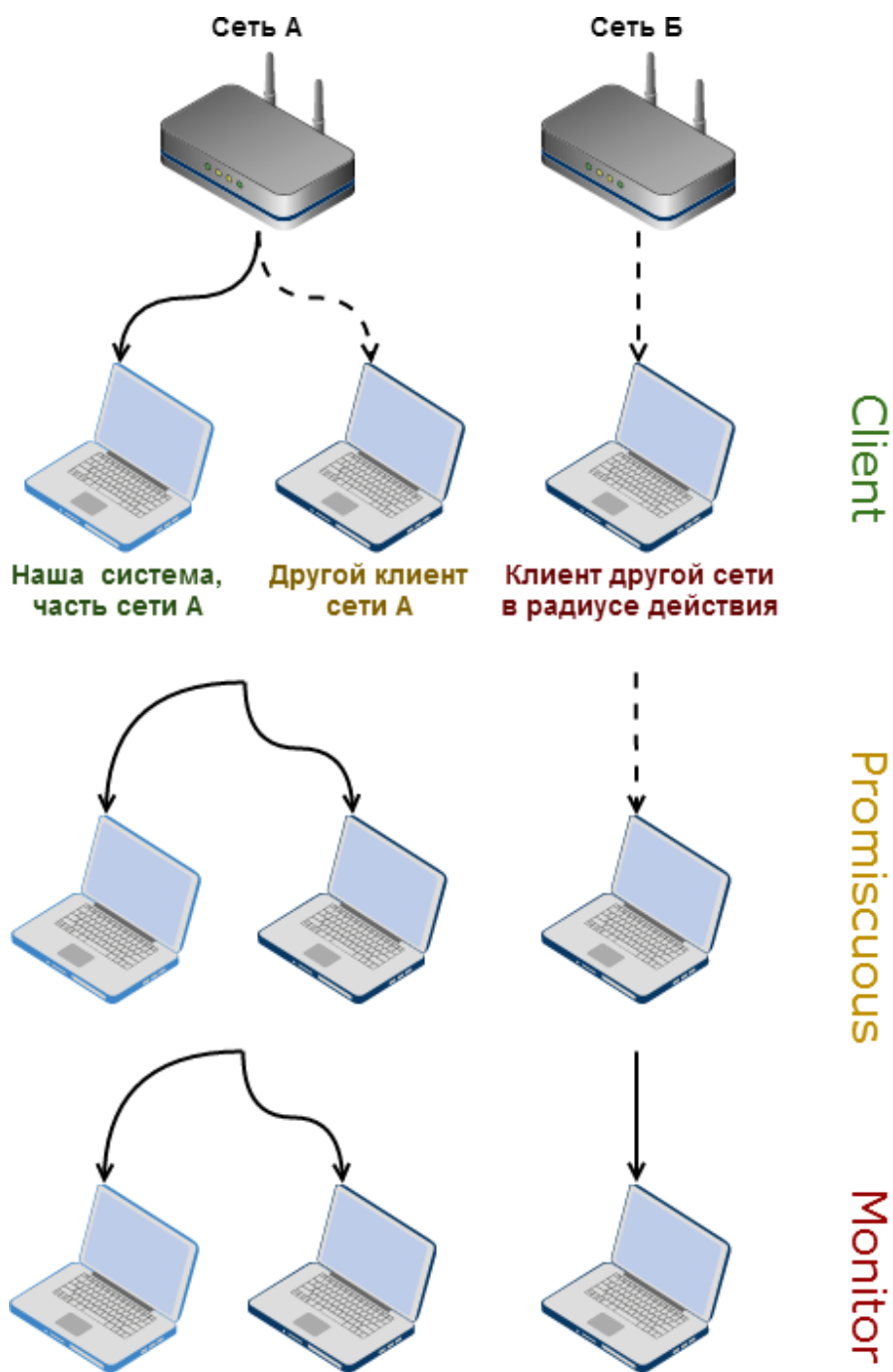


Рис. 1.9. Режимы сканивания беспроводной сети

Програма оцінки кіберзагроз Fortinet призначена для ретельного аналізу трафіку в корпоративних мережах і пошуку індикаторів порушень.

В результаті реалізації програми клієнт отримує рекомендації щодо зниження ризику і підвищення ефективності роботи мережі.

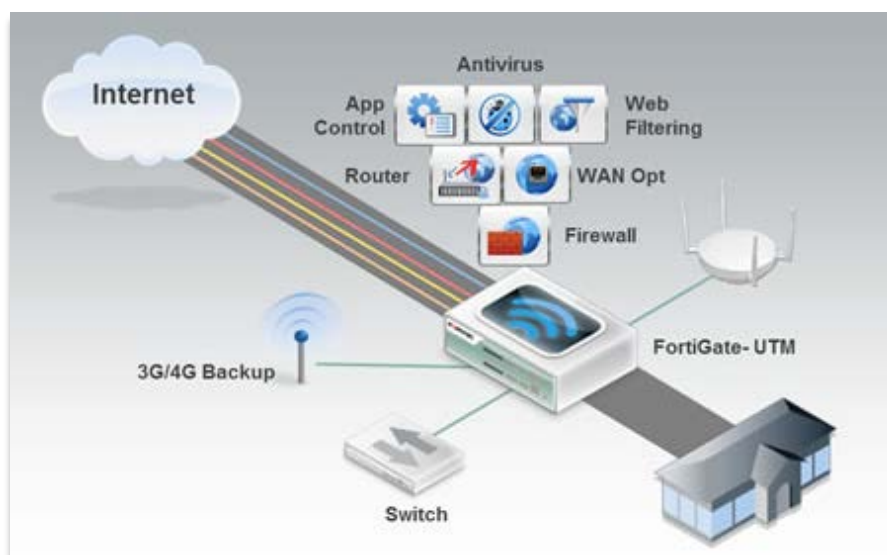


Рис. 1.10. Структурна схема NGFW (Next Generation Firewall)

Якщо раніше просто блокувались певні сайти, щоб працівники не відволікались від роботи, то зараз їх використання є необхідністю.

Таким чином, одним із варіантів вирішення проблеми захисту мереж є NGFW (Next Generation Firewall – мережеві екрани нового покоління, структурна схема показана на рис. 1.10), завдяки яким можливо обмежити трафік по категоріям та відслідковувати поведінку користувачів, надати доступ необхідним пристроям до певних сайтів, та файлів, а також програм та оцінити можливі ризики від них.

Використовуючи такого роду програмно-апаратне забезпечення є можливість захистити корпоративну мережу від зловмисних дій, які могли б понести за собою значні збитки.

Первинне проникнення найчастіше відбувається через розсилки на електронну пошту співробітників.

Однак сам підхід кіберзлочинців тут змінився: якщо раніше вони в основному вдавалися до масових спам-розсилок і фішингу, в надії, що хтось із користувачів кліне на приманку, то сьогодні, як правило, застосовується цільової спам і фішинг.

При цьому під час атаки активно використовуються методи соціальної інженерії. Часто детальний шлях атаки залишався невідомим.

Більшість постраждалих організацій не мало інших засобів захисту і моніторингу, крім антивіруса і брандмауера. Притому, що зараз зловмисники успішно атакують точкові рішення безпеки.

Виявлення атак займало більше місяця, при цьому більшість зломів відбуваються за лічені години. Поточне значення часу виявлення зломів в індустрії складає близько 200 днів. Про справедливості подібних висновків говорить і аналіз атаки Blackenergy [13].

Враховуючи розвиток та поширення сучасних мобільних пристроїв, зростання їх апаратних можливостей, а також швидкості передачі даних в мережах мобільного зв'язку, для більш ефективного захисту треба бути уважнішим, використовувати перевірене програмне забезпечення, різні паролі для облікових записів, блокування пристрою (пін-код, пароль, тощо), віддалене управління на випадок втрати.

Необізнаність користувачів та адміністраторів мереж, що призводить до великої ймовірності перехоплення інформації, може вирішуватись навчанням правилам інформаційної безпеки та створенням відповідних політик безпеки.

Ймовірність перехоплення інформації можна зменшити шляхом використання засобів захисту в повному обсязі, але проблема відсутності коректного налаштування може залишатись, через використання нестійких паролів.

Використовуючи спеціалізоване програмно-апаратне забезпечення є можливість підвищити рівень захисту мереж від зловмисних дій, а правильне налаштування та відповідальне використання особистої техніки допоможе ефективно та безпечно використовувати можливості сучасних мобільних пристроїв.

1.5 Модель перехоплення та захисту інформації в бездротових мережах

Загальну модель перехоплення та захисту інформації в бездротових мережах зображено на рис. 1.11 та описано в таблиці 1.1.

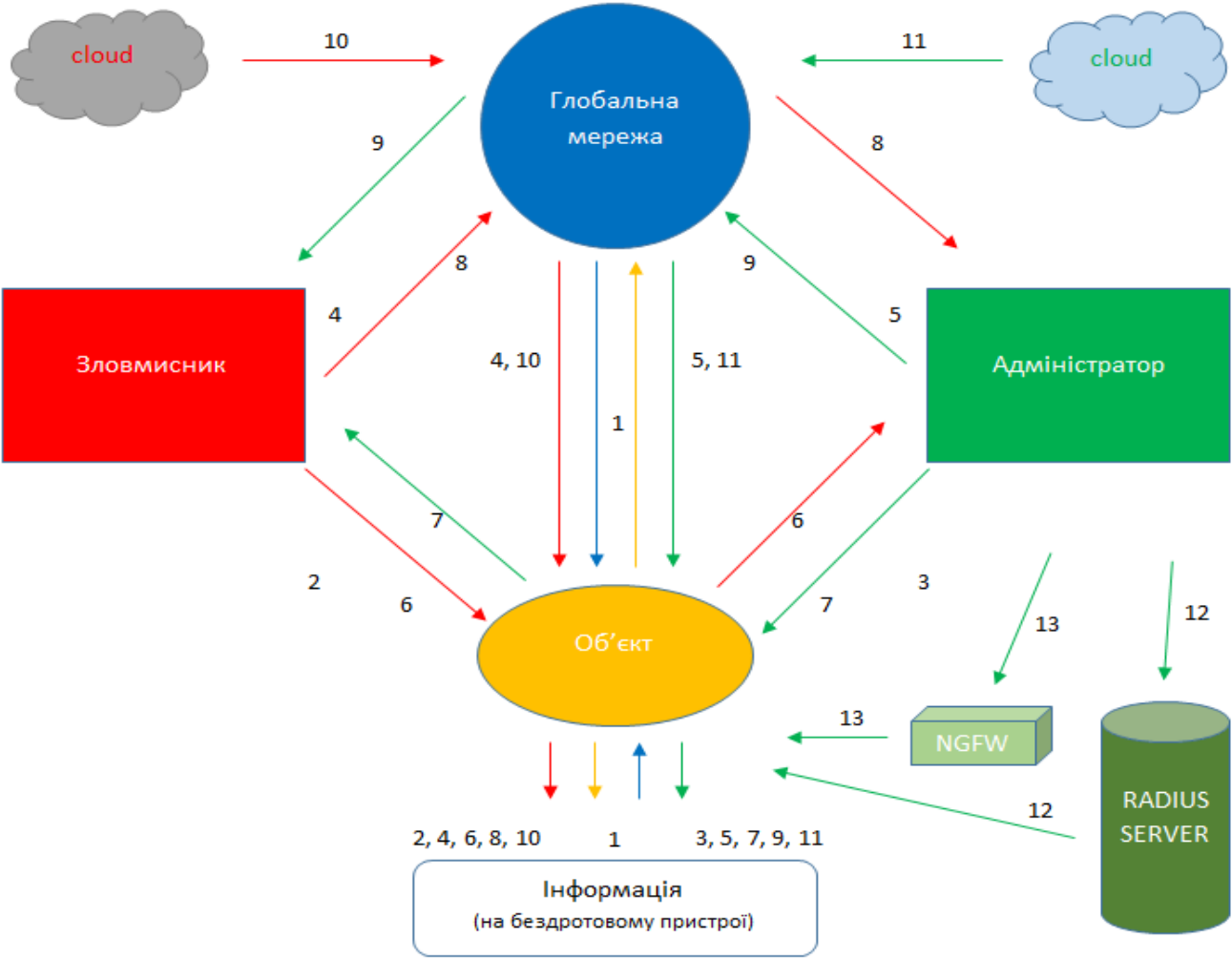


Рис. 1.11. Загальна модель перехоплення та захисту інформації в бездротових мережах

Таблиця 1.1

Опис дій та засобів, що використовуються зловмисниками/адміністраторами при перехопленні/захисті інформації в бездротових мережах

Зловмисник	Адміністратор
1. Стандартна взаємодія пристрою з глобальною мережею через точку доступу (нормальний стан).	
2. Вплив на бездротову мережу з метою перехоплення інформації з пристрою.	3. Засоби захисту адміністратора для бездротової мережі.
4. Вплив на інформацію через глобальну мережу та вразливості зв'язку між нею та точкою доступу.	5. Засоби захисту для каналу зв'язку між глобальною мережею та точкою доступу.
6. Прямий вплив на адміністратора через бездротову мережу.	7. Засоби протидії від прямого впливу зловмисника на бездротову мережу.
8. Прямий вплив на адміністратора через глобальну мережу.	9. Засоби протидії від прямого впливу зловмисника на глобальну мережу.
10. Вплив на бездротову мережу через глобальну з використанням хмарних технологій.	11. Захист бездротової мережі через глобальну з використанням хмарних технологій.
	12. Захист бездротової мережі з використанням RADIUS-SERVER.
	13. Захист бездротової мережі із застосуванням NGFW.

1. Стандартна взаємодія пристрою з глобальною мережею через роутер (нормальний стан). Модель описує нормальний стан роботи мережі, інформація з мобільного пристрою передається через бездротову мережу, без втручання зловмисника.

2. Вплив зловмисника на бездротову мережу з метою перехоплення інформації з пристрою. В даному випадку бездротова мережа піддається впливу зловмисника. Розглядається вплив на об'єкт з використанням локальної бездротової мережі.

Зловмисник з використанням спеціального програмного та апаратного забезпечення намагається проникнути в мережу.

Метою таких дій є бажання отримати доступ до мережі, що може дати йому змогу перехоплювати інформацію з пристроїв підключених до мережі.

Також зловмисник може змінювати параметри об'єкта таким чином, що клієнт мережі може нічого не помітити, але буде передавати зловмиснику свої дані, чи відвідувати саме ті ресурси, в яких зацікавлений зловмисник.

3. Засоби захисту адміністратора для бездротової мережі. При взаємодії клієнта мережі через об'єкт можливі декілька сценаріїв роботи, а саме:

- без використання шифрування, відкрита мережа, до якої може підключитись кожен;
- з використання шифрування (WEP, WPA/WPA2 – Personal, WPA/WPA2 – Enterprise).

Окрім даних інструментів адміністратор може використовувати ще додаткові програмні (антивірусне програмне забезпечення, сканер мережі, брандмауер) та програмно-апаратні засоби (NGFW, Radius-server, хмарні сервіси).

Дані інструменти захисту можуть працювати окремо, або взаємодіяти між собою, окрім цього більшість з них має можливість захистити від впливу з глобальної мережі (п.5, 11).

4. Вплив зловмисника на інформацію через глобальну мережу та вразливості зв'язку між нею та роутером.

Якщо адміністратор мережі лишив налаштування об'єкту «за умовчуванням», або не встановив захищені налаштування, то вплив на локальну бездротову мережу можливий віддалено, з використанням глобальної мережі та вразливості в налаштуваннях.

Таким чином зловмисник може впливати на конфігурацію та налаштування бездротової мережі перебуваючи навіть в іншій країні.

5. Засоби захисту адміністратора для каналу зв'язку між глобальною мережею та роутером.

Завдяки використанню стійкого пароля та зміни логіна для доступу до налаштувань, обмеження кількості спроб авторизації та забороні доступу до налаштувань локальної мережі з використанням глобальної, адміністратор може мінімізувати можливості зловмисника.

Для додаткового захисту необхідно використовувати програмно-апаратні засоби.

6. Прямий вплив зловмисника на адміністратора через бездротову мережу.

Завдяки використанню спеціальних програмних та програмно-апаратних засобів, зловмисник може видавати себе за адміністратора мережі та виконувати зловмисні дії від його лиця, окрім цього можливе блокування або створення перешкод для захисту.

7. Засоби протидії адміністратора від прямого впливу зловмисника на бездротову мережу.

Завдяки програмним та програмно-апаратним засобам адміністратор може не тільки захистити мережу від проникнення, а і обмежити доступ та захистити себе від нападу зловмисника.

8. Прямий вплив зловмисника на адміністратора через глобальну мережу.

Використовуючи зловмисне програмне забезпечення та вразливості в налаштуваннях зловмисник може задіяти глобальну мережу та виконувати дії аналогічні п.6.

9. Засоби протидії адміністратора від прямого впливу зловмисника на глобальну мережу.

Аналогічно до п.7, адміністратор повинен захищати мережу від впливу через глобальну мережу.

10. Вплив зловмисника на бездротову мережу через глобальну з використанням хмарних технологій.

З використанням сучасних хмарних технологій зловмисник може виконувати необхідні йому обчислення для злому на віддалених, але високопродуктивних програмно-апаратних засобах, що дозволить йому значно зберегти час.

11. Захист бездротової мережі адміністратором через глобальну з використанням хмарних технологій.

Завдяки використанню сучасних хмарних технологій адміністратор також має програмно-апаратні засоби, які дозволяють йому аналізувати та відслідковувати спроби несанкціонованого доступу завдяки спеціальним хмарним сервісам.

12. Захист бездротової мережі адміністратором з використанням RADIUS-SERVER.

Для конфігурації локальної мережі підприємства використовується дана модель захисту, яка робить практично не можливим перехоплення інформації в захищеній мережі.

13. Захист бездротової мережі адміністратором з використанням NGFW.

З використанням даного програмно-апаратного засобу можна захистити мережу як локально, так і від впливу з глобальної мережі, а також з використанням хмарних сервісів, що дає змогу поєднати в собі інструменти описані в п. 3, 5, 7, 9, 11, що робить його універсальним засобом моніторингу та захисту мережі, як локальної, так і глобальної.

Таким чином важливо поєднувати зусилля в підвищенні обізнаності користувачів фахівцями у галузі інформаційної безпеки, виробниками мобільних пристроїв, провайдерами послуг та технічного забезпечення, адже більшість користувачів, нажаль навіть не замислюється над можливістю того, що їх пристрої можуть піддаватись загрозам, а їх паролі – атакам на підбір.

Проведення тестів на проникнення, оновлення програмного та апаратного забезпечення є важливим питанням.

Необхідно проводити періодичне навчання працівників компанії та фахівців з інформаційної безпеки, адже не дивлячись на розвиток технологій, саме людина лишається найвразливішою ланкою в інформаційній безпеці.

Це все призводить до того, що:

- зловмисник (атакуючий), використовуючи для проникнення в мережу зламані облікові записи користувачів, що не були захищені стійким паролем (76% вдалих атак на мережу), може знаходитись в мережі компанії в середньому 243 дні, перш ніж його несанкціоноване підключення буде виявлено;

- основні загрози інформаційній безпеці організацій приносить застосування співробітниками мобільних пристроїв (51%) та Інтернет речей (21%);

- збиток, нанесений зловмисником (атакуючим) в результаті кібератаки, буде виражатись переважно у збоях систем (58,4%), втраті даних (25,2%) і несанкціонованому доступі (14,9%) та може привести до репутаційних втрат компаній, обумовлених невинуватими втратами часу на відновлення режиму нормального функціонування системи.

Висновки до першого розділу

Таким чином, за результатами проведеного аналізу множини актуальних загроз та уразливостей для систем бездротового зв'язку в умовах кібернетичних атак можна зробити наступні висновки:

по-перше, знання звичайних користувачів в області інформаційної безпеки дуже обмежені й тому, значна кількість з них не приділяє часу для захисту своїх даних;

по-друге, третина всіх паролів, що використовуються, зламуються шляхом простого перебору варіантів зі словника;

по-третьє, саме цим обумовлюється нагальна потреба застосування ускладнених паролів для забезпечення відмовостійкості систем бездротового зв'язку в умовах кібернетичних атак.

Список використаних джерел у першому розділі

1. Вебінар на тему: «Огляд засобів інформаційної безпеки для мобільних пристроїв» компанії «Palo Alto Networks» (25.03.2015).
2. **Платоненко А. В.** Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко. // Сучасний захист інформації. – 2015. – №4. – С. 86–90.
3. **Платоненко А. В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту / А. В. Платоненко. // Сучасний захист інформації. – 2017. – №1. – С. 128–132.
4. ЧМ 2014 в Бразилії_ Wi-Fi сети и поддельные зарядные устройства. URL: <https://securelist.ru/blog/issledovaniya/20137/chm-2014-v-brazilii-wi-fi-seti-i-poddelnye-zaryadnye-ustrojstva/> (дата звернення: 11.03.2018).
5. Публичные Wi-Fi как угроза вашей безопасности. URL: <https://blog.kaspersky.ru/fake-hotspots/4665/> (дата звернення: 12.03.2018).
6. Wi-Fi сети_ проникновение и защита. 2) Kali. Скрытие SSID. MAC-фльтрация. URL: <https://habr.com/ru/post/225483/> (дата звернення: 12.03.2018).

7. Сколько сетей Wi-Fi не защищены и как защитить от них смартфон. URL: <https://blog.kaspersky.ru/wi-fi-sao-paulo/4351/> (дата звернення: 12.03.2018).
8. Правила безопасности при использовании общественным Wi-Fi. URL: <https://blog.kaspersky.ru/dangerous-public-wi-fi/10107/> (дата звернення: 12.03.2018).
9. Wifi Network Security Statistics_Graph. URL: <https://graphs.net/wifi-stats.html> (дата звернення: 12.03.2018).
10. Хакеры удаленно захватили контроль над движущимся электромобилем Tesla Model S.html URL: <https://itc.ua/news/hakeryi-udalенno-zahvatili-kontrol-nad-dvizhushhimsya-elektromobilem-tesla-model-s/> (дата звернення: 13.03.2018).
11. Безопасность периметра сети — устаревший. URL: <https://www.pcweek.ua/themes/detail.php?ID=152852> (дата звернення: 13.03.2018).
12. Gemalto опубликовала индекс утечек данных за первое полугодие 2016 года. URL: <https://www.pcweek.ua/themes/detail.php?ID=152843> (дата звернення: 15.03.2018).
13. Fortinet запускает глобальную программу оценки киберугроз. URL: <http://www.pcweek.ua/themes/detail.php?ID=151378> (дата звернення: 15.03.2018).
14. Кибербезопасность как основа 4-й промышленной революции. Подход Cisco. URL: <https://www.pcweek.ua/themes/detail.php?ID=152022> (дата звернення: 15.03.2018).
15. Vladymyrenko Maksym. Analysis of implementation results of the distributed access control system. / Maksym Vladymyrenko, Sokolov Volodymyr, Buriachok Volodymyr, **Platonenko Artem**. // Preprint. PIC S&T`2019 IEEE conference, Kyiv
16. Opirsky Ivan. Use of near field communication technology for automated profile replication/ Opirsky Ivan, Ivanchenko Ihor, **Platonenko Artem**, Skladannyi Pavlo, Roshchuk Mariia. // Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, Bielsko-Biala, Poland
17. **Платоненко А.В.** Захист інформації у безпроводових мережах WI-FI./ Платоненко А.В. // Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави» – Київ: ДУТ, 2014 – С.40-41.

18. **Платоненко А.В.** Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах. / Платоненко А.В. // Науково-технічна конференція «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.34-35.

19. **Платоненко А.В.** Сучасні загрози інформаційної безпеки для пристроїв у корпоративних мережах. Матеріали Міжнародної науково-технічної конференції «Актуальні проблеми розвитку науки і техніки» – Київ: ДУТ, 2015 – С.128.

20. **Платоненко А.В.** Сучасні загрози інформаційної безпеки для державних та приватних установ України. / Платоненко А.В. // II Міжнародна науково-технічна конференція «Актуальні проблеми розвитку науки і техніки» – Київ: ДУТ, 2015 – С.137-138.

21. **Платоненко А.В.** Сучасні загрози інформаційної безпеки та засоби захисту від них. / Платоненко А.В. // Міжнародна науково-технічна конференція студентства та молоді «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.159-160.

22. **Платоненко А.В.** Актуальні загрози інформаційної безпеки сучасних мобільних пристроїв у мережах нового покоління. / Платоненко А.В. // II Міжнародна науково-практична конференція «Тенденції розвитку конвергентних мереж: рішення пост - NGN, 4G та 5G» – Київ: ДУТ, 2016 – С.182-183.

23. **Платоненко А.В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв в Україні. / Платоненко А.В. // III Міжнародна науково-технічна конференція студентства та молоді» – Київ: ДУТ, 2016 – С.134-136.

24. **Платоненко А.В.** Средства защиты современных мобильных устройств в сетях нового поколения / А. В. Платоненко, А. А. Аносов. // Региональная конференция «Перспективы предоставления услуг на основе сетей пост-NGN, 4G и 5G. Организационные и технические решения по их построению и защите» – Київ: ДУТ, 2017.

Розділ 2

РОЗРОБКА СПОСОБУ ОБҐРУНТУВАННЯ РІШЕННЯ НА ВДОСКОНАЛЕННЯ ПАРОЛЬНИХ ПОЛІТИК В СИСТЕМАХ БЕЗДРОТОВОГО ЗВ'ЯЗКУ

Під парольною політикою в цьому сенсі будемо розуміти перелік вимог для створення паролю. Основними умовами щодо обґрунтованого вибору найбільш доцільного для вдосконалення способу генерування паролів, серед сукупності можливих, є:

по-перше, дослідження однієї із важливих якостей парольних політик, а саме стійкості до підбору та з'ясування можливості щодо її підвищення в результаті проведення вдосконалення;

по-друге, проведення раціонального вибору "базового способу" серед сукупності можливих способів, що досліджуються.

Розроблено метод обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, для забезпечення їх надійності функціональної безпеки і живучості в умовах кібернетичних атак, за рахунок вибору раціонального способу генерування паролів серед множини існуючих.

2.1. Проблеми сучасних політик безпеки

У прагненні поліпшити прибутковість і масштаб бізнесу власники і топ-менеджери часто залишають поза фокусом своєї уваги інформаційну безпеку підприємства. Однак саме цей сегмент загальної структури компанії є найбільш вразливим і критичним для іміджу.

Останнім часом відзначається вкрай негативний вплив кібератак на фінансове становище підприємств.

У 22% атакованих організацій зменшилася кількість замовників, при цьому у 40% з них клієнтська база скоротилася більш ніж на 20%; крім того, у 29% зменшилися доходи, з них у 38% доходи скоротилися більш ніж на 20%.

Але іноді трапляються і більш драматичні ситуації: в кінці 2016 корпорація Yahoo визнала, що в серпні 2013 року відбулося дуже серйозний злом в її інформаційних системах, в результаті якого були викрадені дані більш ніж одного млрд користувачів. Через це компанії Verizon і Yahoo відклали заплановану багатомільярдну операцію зі злиття на три місяці.

Відсутність зацікавленості у керівництва до інформаційної безпеки - одна з найбільш критичних проблем бізнесу, відповідно і для політик інформаційної безпеки, які мають затверджуватись керівництвом, це є основною проблемою.

Адже саме від твердої волі і передбачливості директора або власника компанії багато в чому залежить, наскільки надійно інформація підприємства буде захищена від посягань, а імідж залишиться чистим і незаплямованим.

Ніхто крім власника, інвестора або акціонера не може бути більше зацікавлений в довгостроковій цінності своїх активів.

Типові помилки і помилки топ-менеджерів або власників бізнесу, які хочуть захистити свої активи, але при цьому відсувають питання інформаційної безпеки в кінець списку важливих і невідкладних справ викладені нище.

1. В компанії все добре, ніхто ніколи не втрачав дані, про подібні факти нікому з працівників невідомо.

Якщо в інформаційних системах на перший погляд не відбувається нічого підозрілого, це не означає, що все дійсно добре. Особливість сучасних кібератак в тому, що вони протікають вкрай приховано.

Так, в лютому дослідники з CyberX розкрили деталі нової широкомасштабної кібератаки, що охопила безліч об'єктів в Україні.

Зловмисники атакували критично важливі інфраструктурні підприємства, наукові центри і медіаресурси. В Україні хакери націлилися на міжнародні організації з контролю за правами людини, антитерористичні центри та об'єкти критичної інфраструктури.

В результаті атаки кіберзлочинцям вдалося викрасти великі обсяги конфіденційної інформації, включаючи записи розмов користувачів через вбудовані мікрофони ноутбуків, скріншоти документів, різні файли і паролі.

Варто відзначити, що якщо камеру в смартфоні або ноутбучі досить легко деактивувати, просто заклеївши її непрозорою стрічкою, то заблокувати роботу мікрофона практично неможливо, хіба що розібрати пристрій і фізично його відключити. Оскільки хакери використовували Dropbox для зберігання викрадених даних, в CyberX назвали операцію - BugDrop.

Слід підкреслити, що вищезгадана серія атак - далеко не єдина. Так, експерти однієї з найбільших антивірусних виробників нещодавно виявили, що близько 140 організацій в 40 країнах світу стали жертвами «непомітних» цільових атак: для проникнення в корпоративні мережі зловмисники використовували виключно легітимне ПЗ, а будь-які шкідливі файли зберігали в пам'яті системи, не залишаючи ніяких слідів на жорстких дисках.

Розслідування інциденту дозволило встановити, що подібні атаки здійснювалися по всьому світу.

Атака через легітимні програмні додатки дає можливість атакуючим уникати виявлення і блокування методом «білих списків» (коли в системі можна запускати тільки офіційні програми перевірених виробників).

Присутність шкідливого коду лише в оперативній пам'яті системи залишає дослідників без будь-яких доказів і артефактів, на основі яких можна провести розслідування.

2. Для рішень задачі з інформаційної безпеки є IT-фахівці - вони впораються.

Власник або директор компанії помиляється, якщо наймає в службу інформаційної безпеки одного або двох високопрофесійних і високооплачуваних співробітників в надії, що цим він закrije всі питання з кіберзахисту.

Звичайно, кваліфікований персонал - це важливий фактор при побудові системи інформаційної безпеки. Однак трудові ресурси - лише одна ланка системи, хоча і досить важливе.

Необхідно враховувати, що експерти в області інформаційної безпеки зазвичай мають дуже вузькою спеціалізацією.

Тому при наймі співробітників треба розуміти, який сектор в сфері інформаційної безпеки він зможе покрити своїми знаннями.

Наприклад, фахівець з впровадження DLP-систем навряд чи буде компетентний при розгортанні систем відеоспостереження, а експерт із захисту мережевого периметра не буде розбиратися в технологіях віртуалізації.

З іншого боку, містити занадто великий штат ІТ-фахівців з вузькою кваліфікацією, які займаються інформаційною безпекою - занадто дорого і не оптимально.

Набагато вигідніше при впровадженні нових рішень звертатися до системних інтеграторів, які вже впровадили безліч проектів і мають багатий досвід по роботі в компаніях різного масштабу.

Якщо планується впровадити комплексну систему безпеки, то не уникнути інвестування в модернізацію мережевого і серверного устаткування, придбання систем моніторингу, аналітики, засобів пасивного та активного захисту інформації. Саме тут досвід і кваліфікація системного інтегратора (або інтеграторів) важлива та корисна.

3. Є міжмережевий екран і антивірус - цього достатньо для захисту.

Власне, це твердження є хибним лише частково: дійсно, побудова базової системи інформаційної безпеки саме починається з розгортання антивірусних засобів на робочих станціях і серверах, а також установки брандмауера на кордоні периметра локальної мережі для захисту внутрішніх хостів від атак ззовні.

Однак таких коштів зараз абсолютно недостатньо. Адже якщо атака почнеться з внутрішніх вузлів, то в цьому випадку брандмауер буде безсилий.

До того ж, деякі зі зловмисних програм для проникнення можуть використовувати уразливості «нульового дня» і не будуть визначатись класичним антивірусом.

Фінансові втрати від шахрайства з використанням корпоративної електронної пошти тільки в 2016 році глобально досягли 3 млрд доларів США, а число вразливостей в різних продуктах склало близько 500.

Варто також відзначити, що через масове використання мобільних пристроїв і хмарних сервісів мережевий периметр в компаніях все більше розмивається. Тому сьогодні потрібні зовсім інші системи захисту, більш різнопланові і просунуті.

4. Немає критичної інформації, яку необхідно захищати.

Можливо у компанії дійсно немає інформації, яка може бути цікавою для конкурентів або інших суб'єктів.

Але, без сумніву, дані дуже важливі для бізнесу: облік з продажу, список контрагентів, контакти найбільш активних клієнтів, бухгалтерський облік і т. д.

Все це може бути в один момент знищено зловмисним ПЗ або зашифровано програмами-вимагачами типу Ransomware.

Слід зауважити, що Ransomware є найбільш суттєвою з кіберзагроз на сьогоднішній день: згідно з даними Cisco, число різновидів «шифрувальників» збільшилася майже вдвічі, до того ж їх кількість продовжує зростати.

Окремі різновиди програм-вимагачів здатні атакувати всі рівні мережі. Щоб не платити потім викуп за розшифровку власних даних, краще завчасно потурбуватися про їх захист.

5. Вже були проблеми в ІБ, їх вирішили, більше нічого робити не планується.

Необхідно розуміти, що технології, які застосовуються кіберзлочинцями постійно еволюціонують, зловмисники вигадують все нові і нові способи проникнення і злому інформаційних систем.

Відділ інформаційної безпеки, так само як і власник бізнесу, повинні постійно відслідковувати актуальну інформацію в галузі, інакше атака може повторитися.

Непорушне правило, якого слід дотримуватися, говорить, що «інформаційна безпека - це не проект, а процес».

Згідно зі статистикою, лише кожна друга компанія розслідує попередження про порушення захисту, при цьому необхідні попереджувальні заходи вживаються менш ніж для 50% сигналів про реальні загрози.

Для своєчасного виявлення та запобігання наслідків атак саме забезпечення інформаційної безпеки має стати одним з бізнес-пріоритетів для топ-менеджерів компанії.

6. Користувачів не потрібно навчати - їх завдання працювати, а не думати про безпеку.

Це одне з найбільш поширених і небезпечних помилок, адже саме поінформовані і пильні співробітники є першою лінією оборони в боротьбі з кіберзагрозами.

Навчання співробітників того, як протистояти різним хитрощів шахраїв, соціальної інженерії, як безпечно працювати в будь-якому місці і з будь-якого пристрою, є одним із запорук успіху.

І навпаки, неправильне і безграмотне поведінку співробітників може стати причиною порушення інформаційної безпеки.

Досвід багатьох компаній показує, що кінцеві користувачі є основним фактором, що визначає успіх або провал проектів з кібербезпеки.

Якщо співробітники нехтують прийнятими в компанії правилами безпеки, намагаються отримати доступ до корпоративних даних в будь-який місці і з будь-якого пристрою, то це ставить під загрозу інформаційні ресурси будь-якого рівня.

Необхідно врахувати, що навчання користувачів вимагає особливого підходу. Просто розповідь загальними словами про передові технології кібербезпеки навряд чи справить потрібний ефект.

Набагато краще пояснити стандарти корпоративного захисту, використовуючи життєві приклади, які актуально діяльності співробітника. Тоді буде змога швидко зрозуміти вимоги компанії в області інформаційної безпеки та дотримуватися їх у своїй роботі.

7. Політики безпеки будуть заважати роботі бізнес-підрозділів. Можна обійтися і без них.

Відсутність правил, які визначаються політиками безпеки, веде до ослаблення рівня кіберзахисту.

З іншого боку, надмірно суворі політики інформаційної безпеки можуть викликати дискомфорт і невдоволення користувачів.

Тут необхідно дотримуватися такої стратегії: будь-який набір правил в області інформаційної безпеки повинен бути єдиним як для рядового співробітника, так і для топ-менеджера, включаючи власника бізнесу.

Так, якщо в компанії введена заборона на використання особистих мобільних пристроїв, то це повинно стати загальним заборонаю для всіх.

Відповідно керівникові компанії слід обмежувати себе у використанні інформаційних систем рівно стільки, наскільки він обмежує своїх співробітників.

Політики безпеки можуть втратити свою актуальність, якщо користувачі вважатимуть, що їх порушення не призведе до будь-яких проблем в інформаційному захисті, або якщо вони будуть думати, що обхід політик поліпшить продуктивність роботи.

Тому корпоративні стандарти інформаційної безпеки повинні бути в актуальному стані і відповідати вимогам бізнесу та державним стандартам [1].

Отже тільки спільне та відповідальне відношення працівників, керівників кожного з відділів й вищого керівництва допоможе підтримувати політики безпеки в актуальному стані, що в свою чергу знизить рівень ризиків втрати важливих даних та підвищить рівень обізнаності користувачів в питаннях інформаційної безпеки не тільки в рамках роботи, але і в повсякденному житті.

В мережі Інтернет досить велика кількість програмного забезпечення для відновлення паролів, які застосовуються для комп'ютерної криміналістики, відновлення даних та аудитів інформаційної безпеки [4].

На жаль, спробам виправлення і усунення недоліків застарілих пристроїв і програмного забезпечення приділяється надмірна увага, що негативно відбивається на протидії сучасним атакам, провідниками яких є цифрові пристрої.

86% організацій зафіксували атаки, які використовують уразливості, існуючі вже більше десятиліття. Майже в 40% випадків цілями ставали ще більш старі уразливості. В середньому на одну організацію доводиться 10,7 унікальних вразливих додатків. У 9 з 10 компаній були виявлені модифіковане ПЗ, що представляє собою серйозну небезпеку.

В цілому при порівнянні середніх показників чисельності виявлених у кожному регіоні світу унікальних варіантів шкідливого ПЗ і сімейств ботнетів найбільшу кількість, та різноманітність загроз в кожній категорії спостерігається в Африці, на Близькому Сході, та в Латинській Америці. Найбільш виразно ця тенденція проявляється в категорії ботнетів [5].

Зростання інвестицій в кіберзахист має вагомі підстави: в останні кілька років кількість загроз для фінансової індустрії неухильно зростає, вони стають все більш складними і можуть мати серйозні наслідки.

Так, 70% банків повідомили про те, що за рік вони понесли грошові втрати в результаті кібершахрайства.

Найбільше побоювань викликають ризики, пов'язані з мобільним банкінгом: 42% респондентів вважають, що в найближчі три роки їм буде користуватися переважна кількість клієнтів, в той час як рівень кіберграмотності користувачів залишиться низьким.

Це загрожує збільшенням кількості інцидентів, пов'язаних з крадіжкою грошей через мобільні пристрої.

Серед інших актуальних загроз для користувачів банки виділили фішинг: з ним в 2016 році стикалися клієнти 46% компаній.

Ще одна сфера підвищеного ризику - банкомати. Причому лише 19% банків стурбовані загрозою атак на них, в той час як в 2016 році обсяг шкідливого програмного забезпечення для банкоматів виріс на 20% в порівнянні з 2015 роком.

Необережність користувачів і зростаюча кількість атак змушують банки переглянути пріоритети щодо забезпечення безпеки: 61% учасників вважають поліпшення захисту додатків і сайтів одним з головних пріоритетів. На другому місці (52%) виявилось впровадження більш надійних систем авторизації [6].

Якщо Ви хочете, щоб Ваш пароль і дані, які він зберігає, були захищені від хакерів настільки, наскільки це можливо, то обов'язково ознайомтеся з методами, використовуваними для зломів паролів.

У разі якщо Ви думаєте, що такі злочинні обійдуть Вас своєю увагою, або думаєте, що вони ніколи не зможуть вгадати Ваш пароль, може бути, Вам буде цікаво дізнатися, наскільки Ви не праві.

Десять найбільш поширених методів злому паролів виглядають так:

1. Атака з використанням словників.

При цьому використовується простий файл, який містить слова, які можна, сюрприз-сюрприз, знайти в словнику. Іншими словами, атаки такого типу перебирають саме слова, які багато людей використовують в якості пароля.

Така "хитрість", як вміло згруповані разом слова, наприклад, "сімсімоткройся" або "ясуперадміністратор", не врятують пароль від злому - можливо, хакери всього лише витратять кілька зайвих секунд.

2. Атака методом повного перебору (грубої сили).

Цей метод схожий на атаку по словнику, але з додатковим бонусом - звичайно, для хакера, який дозволяє виявити слова, що не містяться в словнику, перебираючи всі можливі букви і цифри комбінації від aaa1 до zzz10.

Це не швидкий спосіб, особливо, якщо ваш пароль складається з декількох символів, але, в кінцевому рахунку, пароль буде розкритий. Метод повного перебору може бути спрощений за допомогою використання додаткових обчислювальних потужностей комп'ютера, в тому числі, з використанням можливостей Вашої відеокарти GPU - і, наприклад, використання розподілених обчислювальних моделей і зомбі-ботнетів.

3. Атака з використанням райдужної таблиці.

Райдужна таблиця - це список попередньо обчислених хешей (числових значень зашифрованих паролів), використовуваних більшістю сучасних систем. Таблиця включає в себе хеші всіх можливих комбінацій паролів для будь-якого виду алгоритму хешування. Час, необхідний для злому пароля за допомогою райдужної таблиці, зводиться до того часу, який потрібен, щоб знайти захешірований пароль в списку. Проте, сама таблиця величезна і для перегляду вимагає серйозних обчислювальних потужностей. Також вона буде марна, якщо хеш, який вона намагається знайти був ускладнений додаванням випадкових символів до паролю до застосування алгоритму хешування.

Варто сказати про можливість існування ускладнених райдужних таблиць, але вони були б настільки великі, що їх було б важко використовувати на практиці. Вони, швидше за все, працювали б тільки з набором заздалегідь заданих "випадкових величин", при цьому пароль повинен складатися менш ніж з 12 символів, інакше розмір таблиці буде непомірно великий, навіть для хакерів державного рівня.

4. Фішинг.

Найпростіший спосіб злому - запитати у користувача його / її пароль. Фішингових повідомлень призводить нічого не підозрює читача на підроблені сайти онлайн-банкінгу, платіжних систем або інші сайти, на яких потрібно обов'язково ввести особисті дані, щоб "виправити якусь страшну проблему з безпекою".

Навіщо ускладнювати собі життя зломом пароля, коли користувач з радістю повідомить його сам?

5. Соціальна інженерія.

Соціальна інженерія дотримується тієї ж концепції, що і фішинг - "запитати у користувача пароль", але не за допомогою поштової скриньки, а в реальному світі.

Улюблений трюк соціальної інженерії - зателефонувати в офіс під виглядом співробітника ІТ-безпеки і просто попросити пароль доступу до мережі. Ви

будете здивовані, як часто це працює. Деякі злочинці навіть відчувають потребу - надіти костюм і бейдж перш, ніж прийти в компанію, щоб задати адміністратору в приймальні той же питання лицем до лица.

6. Шкідливе програмне забезпечення.

Програма перехоплення вводиться з клавіатури або виводиться на екран інформації може бути встановлена шкідливим ПЗ, яке фіксує всю інформацію, яку Ви вводите, або створює скріншоти під час процесу авторизації, а потім надсилає копію цього файлу хакерам.

Деякі шкідливі програми шукають існуючий файл з пароллями веб-браузера клієнта, потім копіюють цей файл, який (крім добре зашифрованих) буде містити легкодоступні збережені паролі з історії сторінок, відвіданих користувачем.

7. Офлайн хакінг.

Легко уявити собі, що паролі в безпеці, коли вони захищені системами блокування, які блокують користувачів після трьох-чотирьох невдалих спроб набору пароля, що також дозволяє блокувати програми автоматичного підбору паролів. Це було б правильно, якби не той факт, що більшість зломів паролів відбувається в офлайн, з використанням набору хеш в файлі паролів, які були "отримані" від скомпрометованої системи.

Часто, розглянута жертва виявляється скомпрометована через злом третьої сторони, яка тим самим забезпечує доступ хакерам до системи серверів і всіх важливих файлів користувача з хешірованого пароллями. Зломщик паролів може працювати стільки часу, скільки йому потрібно, щоб спробувати зламати код без оповіщення цільової системи або окремих користувачів.

8. Підглядання через плече.

Найбільш самовпевнені хакери під виглядом кур'єрів, фахівців з технічного обслуговування кондиціонерів або будь-яких інших службовців проникають в офісні будівлі.

Як тільки вони потрапляють в офісну будівлю, уніформа обслуговуючого персоналу надає їм свого роду безкоштовний квиток на безперешкодний доступ в усі куточки офісної будівлі. Це дозволяє їм записувати паролі, що вводяться

реальними співробітниками, а також надає відмінну можливість побачити всі ті паролі, які багато так люблять писати на стікери і клеїти прямо на монітори своїх комп'ютерів.

9. Метод "павуків"

Досвідчені хакери зрозуміли, що багато корпоративних паролі складаються зі слів, які пов'язані з бізнесом. Вивчення корпоративної літератури, матеріалів веб-сайтів, сайтів конкурентів і навіть список клієнтів можуть забезпечити хакерів "боєприпасами" для побудови користувацького списку слів, який потім використовується для злому методом грубої сили.

Дійсно досвідчені хакери автоматизували процес і запускають "павутинні" додатка, аналогічні тим, які застосовуються провідними пошуковими системами, щоб визначити ключові слова, зібрати і обробити списки для злому.

10. Припущення

Кращим другом зломщиків паролів, звичайно, є передбачуваність користувачів. Якщо дійсно випадковий пароль був створений за допомогою програмного забезпечення, призначеного для цього завдання, то для користувача "випадковий" пароль, навряд чи буде нагадувати щось подібне.

Замість цього, завдяки нашій емоційної прихильності до речей, які нам подобаються, швидше за все, ті "випадкові" паролі, які ми створимо, будуть засновані на наших інтересах, хобі, іменах домашніх тварин, сім'ї і так далі. Насправді, паролі, як правило, будуються на основі всіх тих речей, про які ми так хотіли б поговорити в соціальних мережах і навіть включити в наш профіль. Зломщики паролів, цілком ймовірно, подивляться на цю інформацію і зроблять кілька, часто правильних, здогадок при спробі зламати пароль споживчого рівня, не вдаючись до словника або методу грубої сили.

2.2. Способи генерування паролів

Основні ознаки стійкого до злому пароля (перебір по базах хешів, коли алгоритм хешування заздалегідь відомий):

- довжина пароля (чим більше, тим краще), рекомендують використовувати 15-символьний пароль;
- відсутність словникових слів і частин поширених паролів у складі пароля;
- відсутність шаблонів при складанні паролю (логічний алгоритм генерації пароля, наприклад: «sob@k@», або «q1w2e3r4t5»);
- стохастичні послідовності символів з різних груп (рядкові, прописні, цифри, розділові знаки і спец-символи);

Однак в людей є досить обмежені здібності до запам'ятовування незв'язної інформації, тому паролі, які підходять під вищевказані параметри, хоч і будуть досить стійкі до злому з одного боку, але, з іншого боку, їх дуже непросто запам'ятати. Тому, як приклад, розглянемо менш складні варіанти складання і запам'ятовування паролів.

Людині важно скласти абсолютно випадкові послідовності. Тому необхідно використовувати простіший варіант, а саме - складання послідовностей слів, які пов'язані між собою досить, щоб пароль було легко запам'ятати.

Отже, деякі рекомендації для ідей створення паролів:

- використовуйте в паролі антоніми, синоніми і омоніми та ін. в різних комбінаціях з розділовими знаками і цифрами;
- формули і вирази;
- несправжні адреси електронної пошти;
- рими в паролі;
- повторення;
- візуалізація;
- перебільшення.

Один з найбільш надійних способів запам'ятати пароль - багаторазово набрати його на клавіатурі [7].

На підставі проаналізованих атак та їх статистичних даних, розглянуто методи і множини формування паролів, сформульована постановка задачі у вигляді визначення критерію оцінки стійкого паролю, для захисту інформації в бездротових мережах.

Оскільки паролі є ключами підключення до бездротових мереж, то питання їх стійкості є дуже значиним та важливим, з точки зору захищеності користувачів.

При генеруванні паролів є різні способи їх створення. Необхідно їх розглянути та порівняти.

«Через 20 років постійних зусиль ми, нарешті, досягли успіху в тому, що навчили людей придумувати складні для запам'ятовування паролі, які легко підбираються комп'ютером» (рис. 2.1) [2].

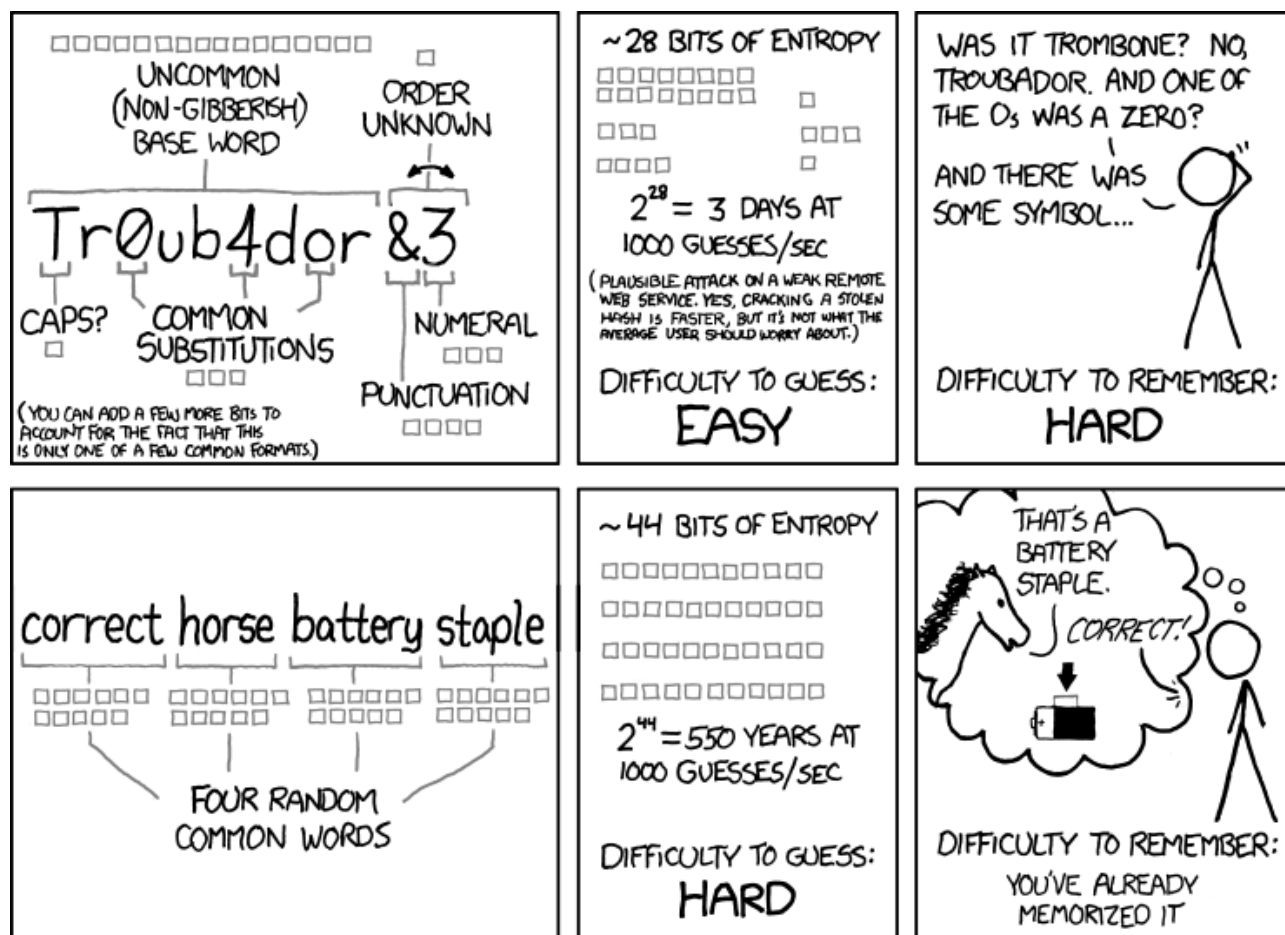


Рис. 2.1. Складність паролю, що складається з декількох не пов'язаних між собою слів

Стенфордський університет, оновив вимоги до паролів для доступу студентів і викладачів до внутрішніх ресурсів своєї мережі.

Тепер жорсткі вимоги використання букв в різних регістрах, цифр і спецсимволів діють тільки для коротких паролів, і чим довшим є пароль, тим ці вимоги м'якші.

При довжині пароля:

- від 8 до 11 символів використання спецсимволів обов'язково,
- від 12 до 15 можна обійтися тільки буквами в різних регістрах і цифрами,
- від 16 до 19 вже можна відмовитися від цифр,
- від 20 символів немає взагалі ніяких обмежень.

Будь-який пароль, який легко запам'ятати, швидше за все легко і зламати.

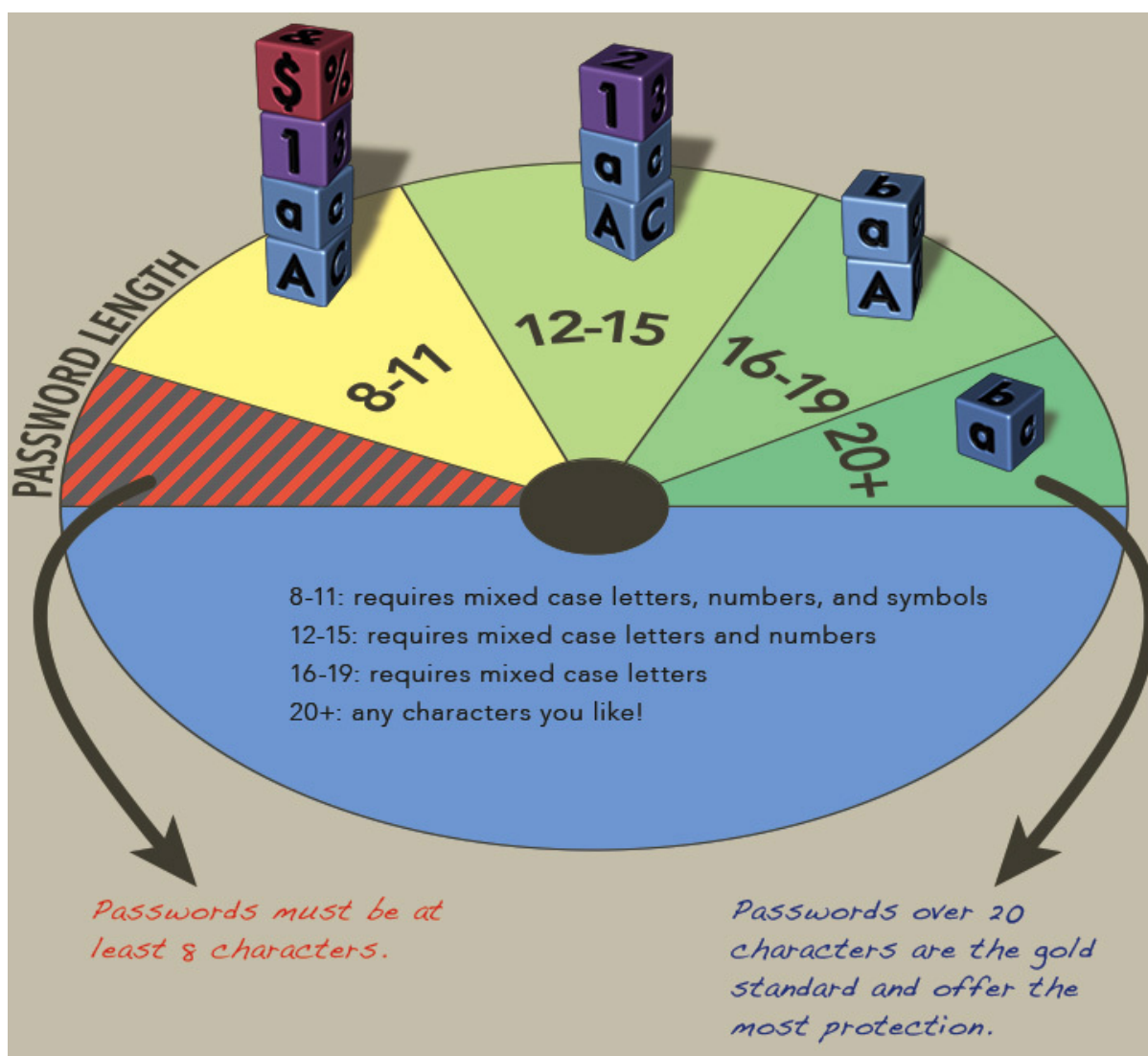


Рис. 2.2. Складність паролю, що складається з різної кількості символів

При обмеженій довжині пароля для збереження стійкості він повинен більше бути схожим на криптографічний ключ у вигляді набору випадкових символів, ніж на секретне слово. І зберігати такі ключі зручно в менеджері паролів, а не у власній пам'яті.

Якщо ж необхідно поєднувати запам'ятовування - краще використовувати пароліні фрази з кількох слів. Саме до цього і підштовхує користувачів нова політика, і, мабуть, багатьом її треба брати в приклад, адже часто довжина пароля обмежується і використовувати довгу фразу в якості пароля неможливо.

В принципі, в нових вимогах Стенфордського університету немає нічого революційного, але це дуже хороший приклад того, як можна поєднувати турботу про безпеку і зручність користувачів, приклавши зовсім небагато зусиль.

Для наочності було опубліковано невелику інфографіку з поясненням нової політики і рекомендаціями щодо використання паролів (рис. 2.2) [3].

Спосіб заміни слів шляхом написання їх на іншій розкладці клавіатури.

Даний спосіб не можна вважати надійним, оскільки більшість часто вживаних слів на певній мові використовуються для створення словників паролів, які в разі пришвидшують результат підбору. Зловмисник може швидко підібрати пароль такого роду, що не дає змоги довіряти даному способу генерування.

Спосіб випадкового натискання клавіш.

Даний спосіб також не можна вважати ефективним, оскільки словники із «змієподібними» комбінаціями паролів (введеними затиснутим пальцем за певним маршрутом на клавіатурі) також існують, що в свою чергу не можна вважати надійним варіантом генерування.

Спосіб «обчислюваних людиною» паролів.

В основі даного способу лежить формування матриці з символами, наприклад назви ресурсу, та відповідної заміни обраних символів, за певним правилом. Воно може бути зручним для використання захисту онлайн-ресурсів, але генерування паролю для бездротової мережі з 63 символів таким методом не дасть необхідної надійності та займе багато часу.

Спосіб генерування паролів завдяки асоціаціям та заміні певних букв символами.

Цей спосіб може бути легшим для запам'ятовування, але також не несе за собою необхідної надійності та потребує значного часу на генерування, крім того словники з такого роду словами також існують, оскільки символи для заміни в основному використовують ті ж самі (наприклад літеру О замінюють цифрою 0).

Спосіб створення паролів з декількох слів, з логічним поєднанням, та із зміною певних символів.

Даний спосіб генерування паролів вже може дати більш складний результат, але його стійкість, також не можна вважати високою. Час на генерування може бути ще більшим, хоча в багатьох випадках саме такі рекомендації є популярними.

Спосіб створення паролів завдяки генеруванні випадкових чисел з використанням гральних кубиків та подальшого вибору слів за таблицею.

Цей спосіб може займати менше часу для генерування паролю, але надійність створеного паролю важко вважати високою, оскільки використання словників для підбору також можливе.

Генерування випадкових паролів завдяки спеціальним командам та додаткам в операційній системі вже може дати складніший результат та потребує набагато меншу часу для створення, але питання випадкового генерування такого ж самого паролю зловмисником, хоча й малоімовірне, але все ж таки можливе. Отже об'єднаємо способи генерування паролів у таблиці 2.1 [3].

Таблиця 2.1

Способи генерування паролів

Назва способу	Стисла характеристика	Рівень стійкості
Спосіб заміни слів	базується на написанні паролю літерами з іншої розкладки клавіатури	<u>нестійкий</u> , оскільки більшість часто вживаних слів на певній мові використовуються для створення словників паролів
Спосіб випадкового натискання клавіш	базується на натисканні клавіш у певному порядку, не відриваючи руки	<u>нестійкий</u> , оскільки словники із «змієподібними» комбінаціями паролів (введеними затиснутим пальцем за певним маршрутом на клавіатурі) також існують
Спосіб «обчислюваних людиною» паролів	базується на формуванні матриці з символами, наприклад назви ресурсу, та подальшої заміни обраних символів, за певним правилом	може бути зручним для використання захисту онлайн-ресурсів, але генерування паролю для бездротової мережі з 63 символів таким способом не дасть необхідної стійкості та займе багато часу
Спосіб генерування паролів завдяки асоціаціям	базується на застосуванні технології асоціацій та заміни певних літер символами	може бути легшим для запам'ятовування, але також не несе за собою необхідної стійкості та потребує значного часу на генерування
Спосіб створення паролів з декількох слів	базується на логічному поєднанні слів із зміною певних символів	може дати більш складний пароль, але його стійкість, також не можна вважати високою, а час на генерування може бути ще більшим
Спосіб створення паролів завдяки генеруванню випадкових чисел	базується на використанні гральних кубиків для генеруванні випадкових чисел та подальшого вибору слів за таблицею	може займати менше часу для генерування паролю, але стійкість створеного паролю важко вважати високою, оскільки можливе використання словників для підбору
Спосіб генерування випадкових паролів	базується на генеруванні паролів завдяки спеціальним командам та додаткам в операційній системі	може дати складніший результат та потребує набагато меншу часу для створення, але питання випадкового генерування такого ж самого паролю зломисником, хоча й малоімовірне, але все ж таки можливе

Примітка: з проблемами, що відображені в табл. 2.1, можна зіткнутися не тільки при застосуванні онлайн-генераторів, а й при використанні відповідного ПЗ для створення паролів.

2.3. Аналіз критеріїв для вибору необхідного способу генерування

Під стійкістю паролю будемо розуміти мінімальну ймовірність його підбору (чим більша стійкість (надійність) паролю – тим менша ймовірність підбору і навпаки, більша ймовірність підбору – буде означати меншу стійкість паролю), а в якості базового способу обиратимемо той, що відповідатиме вимогам до перспективного (ускладненого) способу генерування паролів у системах бездротового зв'язку.

Вибір найбільш доцільного для вдосконалення способу генерування паролів, серед сукупності можливих, здійснюється на підставі визначення та оцінки ступеня близькості (відстані) між базовим способом та кожним способом-аналогом, що дозволяє генерувати паролі для парольних політик та проводиться, як за загальними вимогами, так і за сукупністю характеристик відповідних способів. Вхідними даними для цього є:

- загальні вимоги до структури базового способу та його аналогів (час генерування, довжина паролю, стійкість до підбору);
- перелік характеристик (показників), що притаманні базовому способу та способам-аналогам (кількість символів та можливість їх повторення, множини символів та необхідність їх поєднання, частота зміни паролю);
- вимоги до ускладненого способу генерування паролів у системах бездротового зв'язку (підвищення стійкості до підбору).

Практика показує, що парні порівняння - найбільш зручна для експертів форма вираження своїх переваг.

Можливі ускладнення, яких експерт зазнає при здійсненні парних порівнянь, зводяться до мінімуму, а надмірність інформації, що утримується в заповнених матрицях, дає можливість в процесі наступної обробки значно зменшити вплив помилок експертів при попарному зіставленні цінностей як окремих функцій і критеріїв, так і порівнюваних об'єктів загалом.

Експертом називають спеціаліста, який має інформацію про розв'язувану задачу, але не несе безпосередньої відповідальності за результат її розв'язання.

Експерт дає оцінки конкуруючим способам з вказаної вибірки, розташовуючи їх у ряд переваг, необхідний для вирішення задачі вибору.

Особа, що приймає рішення, має певну мету, яка служить мотивом щодо постановки задачі та пошуку її розв'язання.

Як правило, особа, що приймає рішення, є компетентним спеціалістом у своїй галузі і має досвід діяльності в ній, наділена необхідними повноваженнями й несе відповідальність за прийняте рішення.

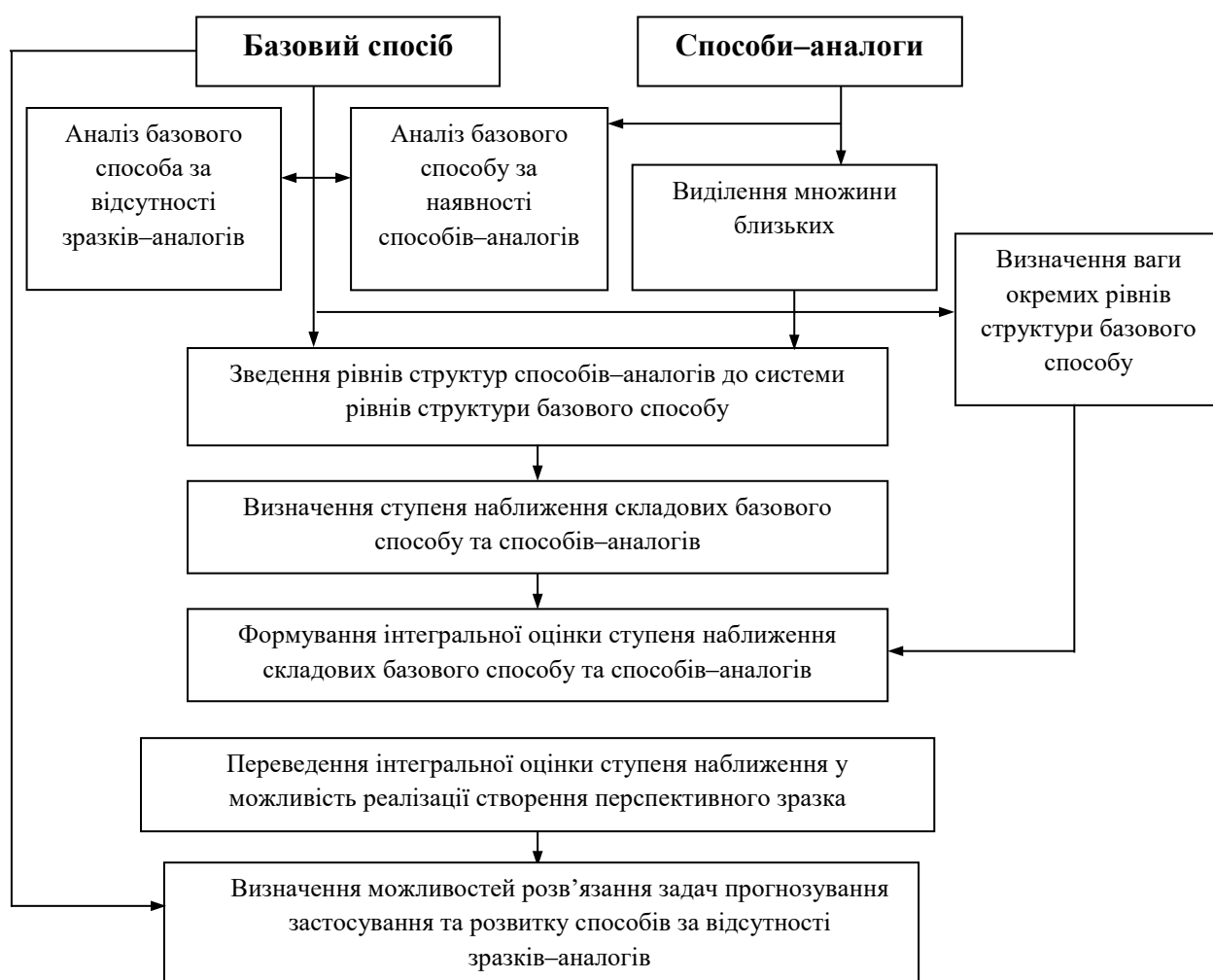


Рис.2.3. Структура методики експертного аналізу у процесі розв'язання задач прогнозування їх застосування та розвитку

2.4. Вибір найбільш доцільного для вдосконалення способу

Процедура вибору найбільш доцільного для вдосконалення способу генерування паролів серед сукупності можливих, ґрунтується на модифікованому методі аналізу ієрархій Сааті та поєднує в собі такі кроки.

Крок 1. Пошук співвідношень між базовим способом генерування паролів і кожним способом-аналогом та розрахунок відстані між ними.

Здійснюється з урахуванням того, що:

- 1) вимоги до базового способу є частиною вимог до способу-аналогу:

$$p_0 = 1 - \frac{1+a_1}{2}, \text{ де } 0.3 < a_1 \leq 1.5; \quad (2.1)$$

- 2) вимоги до способу-аналогу є частиною вимог до базового способу:

$$p_0 = 1 - \frac{1+a_2}{2}, \text{ } 0 \leq a_2 < 0.5; \quad (2.2)$$

- 3) перетинання вимог до способу-аналогу та вимог до базового способу (спосіб-аналог краще базового способу):

$$p_0 = 1 - \frac{b_1}{2}, \text{ } a_1 < b_1 \leq 1; \quad (2.3)$$

- 4) перетинання вимог до базового способу та вимог до способу-аналога (базовий спосіб краще способу-аналога):

$$p_0 = 1 - \frac{b_2}{2}, \text{ } 0 \leq b_2 < a_2, \quad (2.4)$$

де p_0 - відстань між характеристиками (показниками) базового способу та кожного із способів-аналогів за загальними вимогами;

a_1, a_2 - коефіцієнти, що залежать від сумарної кількості подібних співвідношень, яких за основними характеристиками може бути, наприклад, не більше трьох.

За умови, що подібні співвідношення взагалі відсутні - $a_1 = 0.25$ та $a_2 = 0.25$;

b_1, b_2 - коефіцієнти, вибір значень яких здійснюється користувачем, який в даному випадку виконує роль експерта, за правилами: $b_1 \in]a_1, 1[$; $b_2 \in]0, a_2[$.

Крок 2. Оцінка близькості (відстані) між базовим способом генерування паролів та способом-аналогом з урахуванням характеристик.

Способи генерування паролів із сукупності однотипних, обраних для порівняння (табл. 2.1), розташовуються експертами в порядку убутання їх значимості. В даному ряду першим номером буде фігурувати базовий спосіб.

Заповнення матриць парних порівнянь способів генерування паролів із досліджуваної сукупності - $A_j = [a_{11}, \dots, a_{in}, \dots, a_{QQ}]$ за кожним j -м показником (характеристикою): $A_j = |a_{in}^{(j)}|$, $i, n = \overline{1, Q}$, $j = \overline{1, L}$ - відбувається за методом парних порівнянь декількома незалежними експертами (групами експертів) на підставі оцінок їх характеристик, досвіду та інтуїції експертів, з використанням відповідної п'ятибальної шкали (де Q - кількість способів генерування паролів, що підлягають порівнянню).

Причому, в даному випадку елемент $a_{in}^{(j)}$ (2.5) матриці (A_j) визначатиме вагу i -го способу генерування, відносно n -го при порівнянні їх за j -м показником. Пропонується таке правило, згідно з яким відбувається заповнення матриць (A_j) :

$$\alpha_k = \begin{cases} \alpha_1 & - \text{якщо способи за } j\text{-м показником не відрізняються,} \\ & \text{тобто мають однакову важливість;} \\ \alpha_2 & - \text{якщо } i\text{-й спосіб за } j\text{-м показником має} \\ & \text{слабку перевагу над } n\text{-м способом;} \\ \alpha_3 & - \text{якщо перевага помітна;} \\ \alpha_4 & - \text{якщо перевага } i\text{-го способу за } j\text{-м показником суттєва;} \\ \alpha_5 & - \text{якщо } i\text{-й спосіб за } j\text{-м показником має} \\ & \text{абсолютну перевагу над } n\text{-м способом.} \end{cases} \quad (2.5)$$

Якщо $a_{in}^{(j)} = \alpha_k$, де $\alpha_k \neq 0$, $k = \overline{1,5}$ (наприклад, $\alpha_1 = 1$, $\alpha_2 = 3$, $\alpha_3 = 5$, $\alpha_4 = 7$, $\alpha_5 = 9$), то $a_{ni}^{(j)} = \frac{1}{\alpha_k}$. Причому $a_{ii} = 1$.

В результаті, для кожного способу генерування паролів, серед тих, що порівнюються, формуються відповідні квадратні матриці, елементи яких задовольняють умові оберненої симетричності. На підставі знайдених: максимального власного значення $\lambda_{\max A_j}$ кожної з матриць (A_j) та притаманного йому власного вектору відбувається формування набору локальних пріоритетів способів генерування за кожною характеристикою:

$$k_j = \lambda_{\max A_j}^{(j)} x_{B_{lj}}. \quad (2.6)$$

Зі значень $x_{B_{lj}}$ формується узагальнена власна матриця:

$$A_{B_{lij}} = [x_{B_{l1}}, \dots, x_{B_{lj}}, \dots, x_{B_{lL}}], \quad j = \overline{1, L}, \quad (2.7)$$

а потім проводиться нормування елементів кожного з її стовпчиків (вміщують в собі коефіцієнти важливості способу генерування за однією з характеристик):

$$A_{B_{lij}}^{nor} = A_{B_{lij}} / \sum_{i=1}^Q A_{B_{lij}}, \quad i = \overline{1, Q}, \quad j = \overline{1, L}. \quad (2.8)$$

Формування матриці вагових коефіцієнтів важливості кожної характеристики - $B = [b_{11}, b_{jh}, \dots, b_{LH}]$, де $b_{jh} = \beta_k$; $\beta_k \neq 0$; $k = \overline{1,5}$; $h = \overline{1, H}$; $j = \overline{1, L}$, для способу генерування паролів, відбувається за способом безпосередньої оцінки в межах заданої п'ятибальної шкали на підставі врахування значимості даних характеристик під час вирішення однієї й тієї ж задачі, згідно з міркуваннями H експертів-спеціалістів.

Правило, згідно з яким кожній характеристиці надається свій бал, вибираємо таке (при цьому, наприклад: $\beta_1 = 1$, $\beta_2 = 3$, $\beta_3 = 5$, $\beta_4 = 7$, $\beta_5 = 9$):

$$\beta_k = \begin{cases} \beta_1 & - \text{можливо не враховувати} \\ \beta_2 & - \text{бажано враховувати} \\ \beta_3 & - \text{враховувати обов'язково} \\ \beta_4 & - \text{важливий} \\ \beta_5 & - \text{дуже важливий} \end{cases}, \quad (2.9)$$

Нормована вага j -ї характеристики, визначена h -м експертом, при цьому становить: $b_{jh}^{nop} = b_{jh} / \sum_{j=1}^L b_{jh}$, де $h = \overline{1, H}$. Середнє значення вагового коефіцієнта (коефіцієнта значимості) для j -ї характеристики, визначене H експертами, обчислюється за такою формулою:

$$b_j^{середнє} = \sum_{h=1}^H b_{jh}^{nop} / \sum_{h=1}^H \sum_{j=1}^L b_{jh}^{nop}, \quad h = \overline{1, H}, \quad j = \overline{1, L}. \quad (2.10)$$

При цьому, якщо виникає ситуація коли декілька характеристик способу-аналога відповідають одній вимозі базового способу, або ж навпаки - декілька вимог базового способу відповідають одній характеристиці способу-аналога, вирішується задача щодо приведення кількості вимог базового способу, що розглядаються та способу-аналога до однакової кількості.

Це реалізується шляхом підсумовування середніх значень їх вагових коефіцієнтів (коефіцієнтів значимості) - $b_j^{середнє}$:

$$b^p = \sum_{j=1}^p b_j^{середнє}.$$

За умови відсутності даних про вимоги до перспективного (ускладненого) способу генерування паролів, аналогічні характеристики способів-аналогів виключаються з подальшого розгляду.

Значення вектору переваг для способів генерування паролів з досліджуваної сукупності визначаються шляхом перемноження узагальненої власної матриці (кореляційної функції способів генерування за всіма характеристиками) на вектор усереднених коефіцієнтів значимості кожної характеристики:

$$\gamma = A_{Вл_{ij}}^{nop} \cdot b_j^{середнє} = \begin{bmatrix} x_{11} & \dots & x_{1j} & \dots & x_{1L} \\ \dots & \dots & \dots & \dots & \dots \\ x_{i1} & \dots & x_{ij} & \dots & x_{iL} \\ \dots & \dots & \dots & \dots & \dots \\ x_{Q1} & \dots & x_{Qj} & \dots & x_{QL} \end{bmatrix} \cdot \begin{bmatrix} b_1^{середнє} \\ \dots \\ b_j^{середнє} \\ \dots \\ b_L^{середнє} \end{bmatrix} = (\gamma_{cn}^{баз}, \gamma_{an_1}, \dots, \gamma_{an_i}, \dots, \gamma_{an_Q}) \quad (2.11)$$

При цьому, зважаючи на те, що попередньо способи генерування паролів із сукупності однотипних, обраних для порівняння, були розташовані експертами в

порядку убутання їх значимості, отриманий вектор переваг також відповідатиме даній закономірності.

Причому на першому місці буде знаходитись показник, що характеризуватиме базовий (перспективний або ускладнений) спосіб.

Оцінка близькості (відстані) між базовим способом генерування паролів та способом-аналогом з урахуванням характеристик дозволяє отримати оцінку невідповідності опису базового способу й кожного способу-аналога, з погляду збігу переліку їх характеристик.

При аналізі формули (2.11) можливі такі варіанти зіставлення:

– існує однозначна відповідність між способом та його аналогом. Відстань між базовим способом та способами-аналогами за характеристиками (p_T) знаходиться за формулою:

$$p_T = \gamma_{cn}^{баз} - \gamma_{ан}, \quad (2.12)$$

– спосіб-аналог не відповідає базовому способу. У даному випадку робиться висновок про те, що опис способу-аналога обтяжений зайвими характеристиками, які доцільно викреслити з процесу порівняння.

Крок 3. Формування комплексної (узагальненої) оцінки для кожної пари базовий спосіб– спосіб-аналог генерування паролів із досліджуваної сукупності.

В даному випадку можливі такі співвідношення:

а) отримані оцінки відстані близькі за значеннями.

При цьому показник комплексної узагальненої оцінки ступеня близькості базового способу та способів-аналогів (p) знаходимо шляхом усереднення значень оцінок відстані за загальними вимогами характеристиками (показниками):

$$\text{якщо } \left| \frac{p_0 - p_T}{p_{\max}} \right| \leq 0.1 \quad \text{то} \quad p = \frac{p_0 + p_T}{2}; \quad (2.13)$$

б) оцінка відстані за загальними вимогами суттєво менша оцінки відстані за характеристиками (відповідає неповній кореляції між оцінками, що згадувались).

При цьому показник p знаходимо з формули:

$$\text{якщо } \frac{p_T - p_0}{p_{\max}} > 0.1 \quad \text{то} \quad p = p_0 + k_1 p_T, \text{ де } k_1 = \left| \frac{p_T - p_0}{p_{\max}} \right|. \quad (2.14)$$

в) оцінка відстані за характеристиками суттєво менша оцінки відстані за загальними вимогами (відповідає неповній кореляції між згадуваними оцінками).

При цьому показник p знаходимо з формули:

$$\text{якщо } \frac{p_0 - p_T}{p_{\max}} > 0.1 \quad \text{то} \quad p = p_T + k_2 p_0, \text{ де } k_2 = \left| \frac{p_0 - p_T}{p_{\max}} \right|. \quad (2.15)$$

де $p_{\max}$ - максимальне значення коефіцієнта p_T ;

p_T - відстань між базовим способом та способами-аналогами;

p_0 - відстань між характеристиками (показниками) базового способу та кожного із способів-аналогів за загальними вимогами;

k_1, k_2 - коефіцієнти, що відображують невідповідність оцінок та вибираються за допомогою експертного аналізу.

Для проведення заходів з вдосконалення обирається той спосіб генерування паролів із всіх можливих пар «базовий спосіб – спосіб-аналог» із досліджуваної сукупності, для якого коефіцієнт комплексної (узагальненої) оцінки буде найбільшим (табл. 2.2) [4].

Таблиця 2.2

Порівняння способів генерування паролів за загальними вимогами

Назва способу	Час генерування	Довжина паролю	Стійкість паролю
Спосіб генерування випадкових паролів	0.950	0.980	0.935
Спосіб створення паролів завдяки генеруванню випадкових чисел	0.720	0.715	0.750
Спосіб створення паролів з декількох слів	0.318	0.529	0.597
Спосіб генерування паролів завдяки асоціаціям	0.210	0.312	0.389
Спосіб «обчислюваних людиною» паролів	0.152	0.214	0.247
Спосіб випадкового натискання клавіш	0.368	0.390	0.189
Спосіб заміни слів	0.169	0.369	0.125

Висновки до другого розділу

Таким чином, за коефіцієнтом переваг γ та показником комплексної узагальненої оцінки ступеня близькості (відстані) між базовим способом генерування паролів і кожним способом-аналогом (табл. 2.1) найбільш раціональним для забезпечення функціональної безпеки систем бездротового зв'язку, за рахунок вдосконалення парольних політик, є спосіб генерування випадкових паролів (табл. 2.2).

Список використаних джерел у другому розділі

1. Информационная безопасность компании. Семь основных заблуждений руководителя. URL: <https://www.pcweek.ua/themes/detail.php?ID=154197> (дата звернення: 15.04.2018).
2. xkcd_Password Strength URL: <https://xkcd.com/936/> (дата звернення: 15.04.2018).
3. Новые требования к паролям Стэнфордского университета_ баланс между длиной и сложностью. URL: <https://habr.com/ru/post/220949/> (дата звернення: 15.04.2018).
4. ElcomSoft Co.Ltd. Комплексные решения в области восстановления паролей, анализа и обеспечения безопасности компьютера, системы, сервера, локальной сети. URL: <https://www.passwords.ru/download/> (дата звернення: 20.04.2018).
5. Исследование_ киберпреступники пытаются изменить баланс сил в сфере информационной безопасности. URL: https://www.pcweek.ua/themes/detail.php?ID=154298&THEME_ID=13875 (дата звернення: 22.04.2018).
6. Банки вынуждены тратить на инфобезопасность в три раза больше, чем остальные компании. URL: https://www.pcweek.ua/themes/detail.php?ID=154317&THEME_ID=13875 (дата звернення: 22.04.2018).
7. Простой и надежный пароль – коллективное творчество. URL: <https://habr.com/ru/post/118499/> (дата звернення: 25.04.2018).

8. Топ-10 методів взлому паролів - Стаття PCI DSS. URL: <http://pcidss.ru/articles/39.html> (дата звернення: 27.04.2018).

9. Бурячок В.Л. Вибір раціонального способу генерування паролів серед множини існуючих / В.Л. Бурячок, **А.В. Платоненко**, О.В. Семко. // Безпека інформації. – 2019. – Том 25, № 1. – С. 59–64.

10. **Платоненко А.В.** Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах. / Платоненко А.В. // Науково-технічна конференція «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.34-35.

11. **Платоненко А.В.** Сучасні загрози інформаційної безпеки для пристроїв у корпоративних мережах. Матеріали Міжнародної науково-технічної конференції «Актуальні проблеми розвитку науки і техніки» – Київ: ДУТ, 2015 – С.128.

12. **Платоненко А.В.** Сучасні загрози інформаційної безпеки для державних та приватних установ України. / Платоненко А.В. // II Міжнародна науково-технічна конференція «Актуальні проблеми розвитку науки і техніки» – Київ: ДУТ, 2015 – С.137-138.

13. **Платоненко А.В.** Актуальні загрози інформаційної безпеки сучасних мобільних пристроїв у мережах нового покоління. / Платоненко А.В. // II Міжнародна науково-практична конференція «Тенденції розвитку конвергентних мереж: рішення пост - NGN, 4G та 5G» – Київ: ДУТ, 2016 – С.182-183.

14. **Платоненко А.В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв в Україні. / Платоненко А.В. // III Міжнародна науково-технічна конференція студентства та молоді» – Київ: ДУТ, 2016 – С.134-136.

15. **Платоненко А.В.** Средства защиты современных мобильных устройств в сетях нового поколения / А. В. Платоненко, А. А. Аносов. // Региональная конференция «Перспективы предоставления услуг на основе сетей пост-NGN, 4G и 5G. Организационные и технические решения по их построению и защите» – Київ: ДУТ, 2017.

Розділ 3

ВДОСКОНАЛЕННЯ СПОСОБУ ГЕНЕРУВАННЯ ВИПАДКОВИХ ПАРОЛІВ

Даний розділ присвячено вдосконаленню обраного в другому розділі способу генерування випадкових паролів.

Завдання пошуку надійного паролю для захисту інформації в бездротових мережах потребує перевірки на стійкість до підбору.

3.1. Особливості та вимоги до формування паролів у мережах Wi-Fi

Стандарт Wi-Fi використовується для широкосмугових бездротових мереж зв'язку. Спочатку технологія Wi-Fi була орієнтована на організацію точок швидкого доступу в Інтернет для мобільних користувачів.

Переваги бездротового доступу очевидні, а технологія Wi-Fi спочатку стала стандартом, якого дотримуються виробники мобільних пристроїв.

Поступово мережі Wi-Fi стали використовувати малі і великі офіси для організації внутрішніх мереж, а оператори створювати власну інфраструктуру надання бездротового доступу в Інтернет на основі технології Wi-Fi.

Таким чином мережі Wi-Fi поширені майже всюди і часто мають зони покриття, що покривають цілі райони міста.

З точки зору безпеки, слід враховувати не лише загрози, властиві дротовим мережам, але також і середовище передачі сигналу.

У бездротових мережах отримати доступ до інформації, що передається набагато простіше, ніж в проводових мережах, так само як і вплинути на канал передачі даних. Досить помістити відповідний пристрій в зоні дії мережі.

Загрози інформаційної безпеки, що виникають при використанні Wi - Fi мереж, можна умовно розділити на два класи:

прямі – загрози інформаційної безпеки, що виникають при передачі інформації по бездротовому інтерфейсу IEEE 802.11;

непрямі – загрози, пов'язані з наявністю на об'єкті і поряд з об'єктом великої кількості Wi-Fi мереж.

Радіоканал передачі даних, що використовується в Wi-Fi потенційно схильний до втручання з метою порушення конфіденційності, цілісності і доступності інформації.

У Wi-Fi передбачені як аутентифікація, так і шифрування, але ці елементи захисту мають свої недоліки.

Бездротові пристрої можуть міняти точки підключення до мережі в процесі роботи. Наприклад, можуть відбуватися «випадкові асоціації», коли некоректно налаштований бездротовий клієнт автоматично асоціюється і підключає користувача до найближчої бездротової мережі.

Таким чином зловмисник перемикає на себе користувача для подальшого сканування уразливостей, фішингу або атаки «людина посередині».

До того ж багато користувачів, підключених до внутрішньої мережі, невдоволених якістю і політикою роботи мережі, перемикаються на найближчу доступну точку доступу (чи операційна система робить це автоматично при відмові дротової мережі).

Некоректно налаштовані пристрої, пристрої із слабкими і недостатньо довгими ключами шифрування, що використовують уразливі методи аутентифікації, – саме такі пристрої піддаються атакам в першу чергу.

Згідно зі звітами аналітиків, велика частина успішних зломів відбувається саме через неправильні налаштування точок доступу і програмного забезпечення клієнта.

Некоректно налаштовані точки доступу. Досить підключити неправильно налаштовану точку доступу до мережі для злому останньої.

Налаштування «за умовчанням» не включають шифрування і аутентифікацію, або використовують ключі, прописані в керівництві, що усім відомі. Малоймовірно, що користувачі досить серйозно турбуються безпечною конфігурацією пристроїв. Саме такі точки доступу і створюють основні загрози захищеним мережам.

Некоректно налаштовані бездротові клієнти. Техніка клієнтів мережі, яка некоректно налаштована – загроза небезпечніше, ніж некоректно налаштовані точки доступу.

Особисте обладнання користувачів і вони не конфігуруються спеціально в цілях безпеки внутрішньої мережі підприємства.

Крім того, вони знаходяться за периметром контрольованої зони, так і усередині, що дозволяє зловмисникові проводити різні атаки, поширювати небезпечне програмне забезпечення, або просто забезпечувати зручну точку входу в корпоративну мережу.

WEP - перший стандарт захисту Wi-Fi. Розшифровується як Wired Equivalent Privacy («еквівалент захисту дротових мереж»), але він дає набагато менше захисту, ніж ці самі дротові мережі, так як має безліч огріхів і зламуються безліччю різних способів.

Його потрібно уникати майже так само, як і відкритих мереж - безпека він забезпечує тільки на короткий час, через який будь-яку передачу можна повністю розкрити незалежно від складності пароля.

Ситуація ускладнюється тим, що паролі в WEP - це або 40, або 104 біта, що є вкрай короткою комбінацією та підібрати її можна за секунди (це без урахування помилок в самому шифруванні).

Основна проблема WEP - у фундаментальній помилці проектування, бо шифрування потоку робиться за допомогою тимчасового ключа. WEP фактично передає кілька байт цього самого ключа разом з кожним пакетом даних.

Таким чином, незалежно від складності ключа розкрити будь-яку передачу можливо просто маючи достатню кількість перехоплених пакетів (кілька десятків тисяч, що досить мало для мережі, що активно використовується).

WPA - друге покоління, яке прийшло на зміну WEP. Розшифровується як Wi-Fi Protected Access. Якісно інший рівень захисту, завдяки прийняттю до уваги помилок WEP. Довжина пароля - довільна, від 8 до 63 байт, що сильно ускладнює його підбір (порівняйте з 3, 6 і 15 байтами в WEP).

WPA відрізняється від WEP і тим, що шифрує дані кожного клієнта окремо. Після «рукоштовування» генерується тимчасовий ключ, який використовується для кодування передачі цього клієнта, але ніякого іншого. Тому навіть якщо зломисник проникне в мережу, то прочитати пакети інших клієнтів він зможе тільки, коли перехопить їх «рукоштовування» - кожного окремо.

WPS дає змогу клієнту підключитися до точки доступу, завдяки 8-символьного коду, що складається з цифр (PIN). Однак через помилки в стандарті потрібно вгадати лише 4 з них.

Таким чином, достатньо всього-на-всього 10000 спроб підбору і незалежно від складності пароля для доступу до бездротової мережі зломисник автоматично отримує цей доступ, а з ним на додачу - і цей самий пароль яким він є.

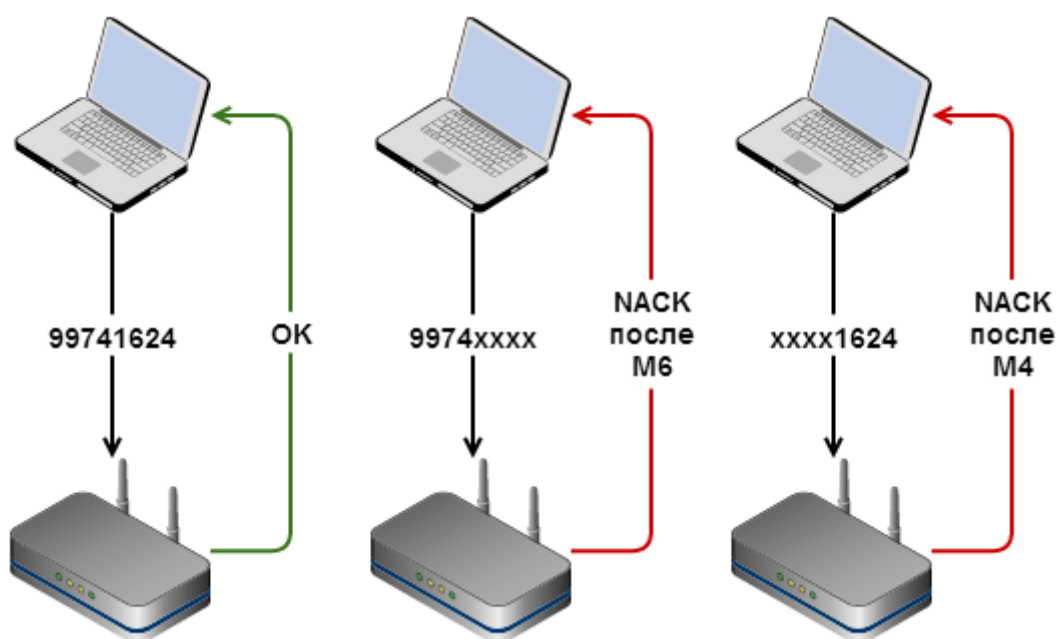


Рис. 3.1. Підключення до мережі через PIN-код

На рис. 3. 1. описано процес підключення клієнта до точки доступу за допомогою PIN-коду. PIN - 8 цифр, які зазвичай нанесені на самому роутері.

Клієнти, що підтримують WPS, можуть підключитися до мережі або за звичайним паролем WEP / WPA, або за допомогою PIN, причому ввівши останній клієнт отримує пароль мережі в чистому вигляді.

Однак ж не все так погано. Більш нові версії ПЗ обмежують можливість підбору, після декількох невдалих спроб авторизації WPS автоматично відключається.

Деякі моделі збільшують час відключення ще більше, якщо за короткий інтервал були зроблені ще невдалі спроби увійти.

PIN змінюється окремо від пароля мережі, тому останній можна оновлювати як завгодно часто, ніяк не ускладнюючи перебір PIN.

Рис. 3.2. відображає процеси, що відбуваються паралельно на обох сторонах (клієнта і точки доступу бездротової мережі), а не те, що передається через радіоканал.

WPA2 або стандарт 801.11i – це фінальний варіант стандарту безпеки бездротових мереж. В якості основного шифру був вибраний стійкий блоковий шифр AES. Система аутентифікації в порівнянні з WPA зазнала мінімальних змін.

Також як і в WPA, в WPA2 є два варіанти аутентифікації WPA2-Enterprise з аутентифікацією на RADIUS сервері і WPA2-PSK з передвстановленим ключем.

Відмови в обслуговуванні (DoS-атака). DoS-атаки спрямовані на порушення якості функціонування мережі або на абсолютне припинення доступу користувачів. У разі Wi-Fi мережі відстежити джерело, що завантажує мережу «сміттєвими» пакетами, вкрай складно – його місце розташування обмежується лише зоною покриття.

До того ж є апаратний варіант цієї атаки – встановлення досить сильного джерела завад в потрібному частотному діапазоні.

Сигнали Wi-Fi пристроїв мають досить складну структуру і широкий спектр, тому ці сигнали, а тим більше, навколишні облаштування Wi-Fi неможливо ідентифікувати звичайними засобами радіомоніторингу.

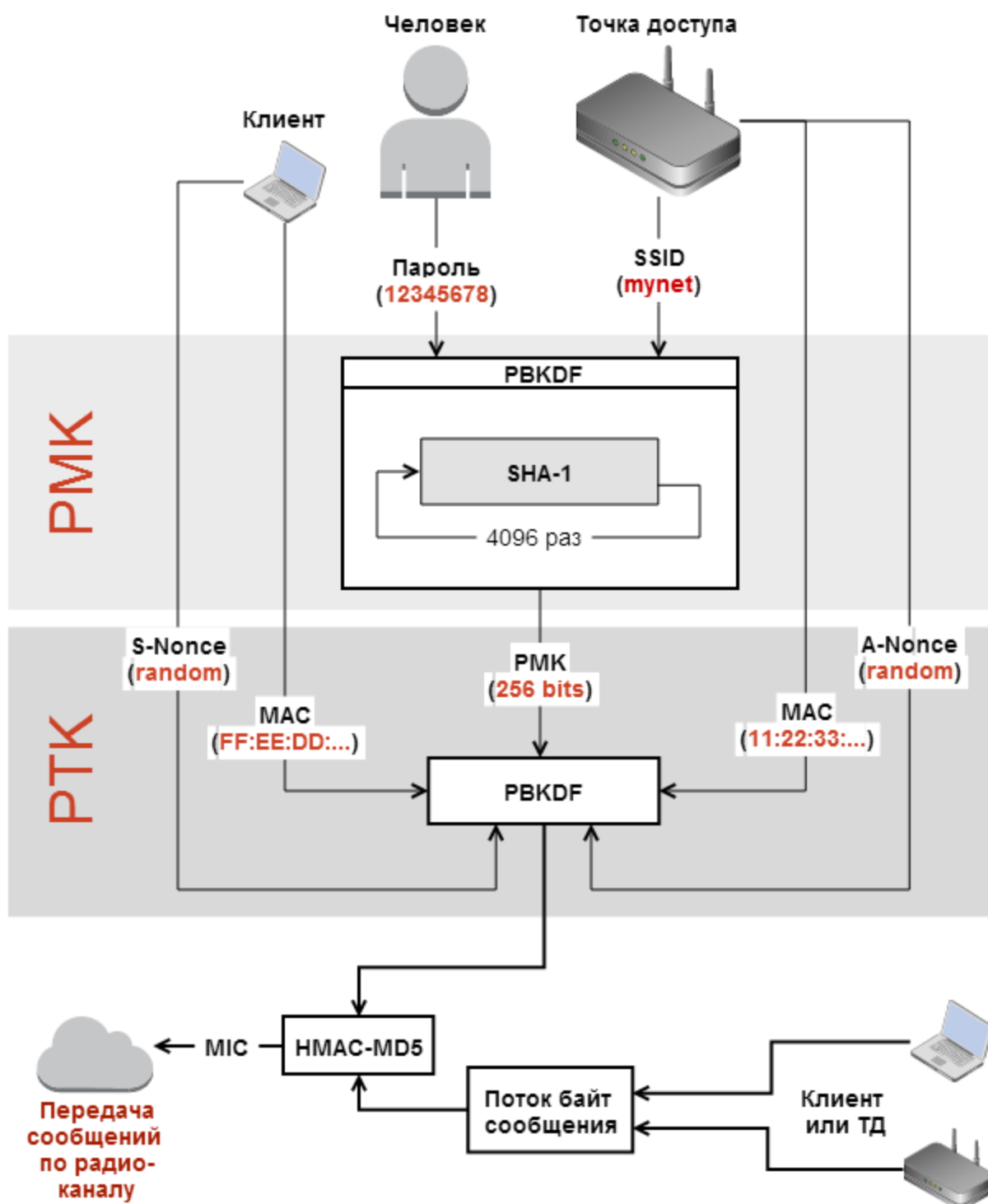


Рис. 3. 2. Взаємодія між клієнтом та точкою доступу

Впевнене виявлення сигналу Wi-Fi сучасними комплексами радіомоніторингу в широкій смузі частот можливо тільки за енергетичною ознакою, за наявності смуг паралельного аналізу шириною декілька десятків МГц на, швидкості не менше 400 МГц/с і лише у ближній зоні.

Сигнали точок доступу, що знаходяться в дальній зоні, виявляються нижче рівня шумів приймача. Виявлення Wi-Fi передавачів, при послідовному скануванні вузькосмуговими приймачами взагалі неможливе.

Виходячи з того, що практично кожен об'єкт оточує безліч Wi-Fi мереж, відрізнити легальних клієнтів своєї мережі та сусідніх мереж від порушників, нажаль вкрай складно, що дозволяє успішно маскувати несанкціоновану передачу інформації серед легальних існуючих Wi-Fi каналів.

У великих містах Wi-Fi мережі загального користування мають досить велику зону покриття, щоб відпала необхідність використати мобільний пункт прийому інформації поряд з об'єктом – несанкціонований пристрій може підключитися до доступної Wi-Fi мережі і використати її для передачі інформації через інтернет у будь-яке необхідне місце.

Якщо на об'єкті обмежено винесення носіїв інформації і вихід в Інтернет обмежений, то одним з варіантів прихованої передачі великого об'єму інформації є Wi-Fi.

Треба підключитися до сусідніх Wi-Fi мереж, залишаючись непоміченим серед легальних користувачів.

Більшість атак розпочинаються з розвідки, в ході якої проводиться сканування мережі, збір і аналіз пакетів (багато службових пакетів в мережі Wi-Fi передаються у відкритому вигляді).

При цьому вкрай проблематично з'ясувати, хто легальний користувач, що намагається підключитися до мережі, а хто збирає інформацію.

Після розвідки приймаються рішення про подальші кроки атаки. Можна зменшити схильність розвідці, розмістивши точку доступу так, щоб вона забезпечувала необхідне покриття, і це покриття мінімально виходило за контрольовану територію.

Треба регулювати потужність точки доступу і використати спеціальні інструменти для контролю поширення сигналу.

Також можна повністю екранувати приміщення з точкою доступу для повної невидимості мережі ззовні.

На сьогодні основними методами злому WPA2 PSK є атака за словником і метод грубої сили.

Атака за словником на WPA/WPA2 PSK. WPA/WPA2 PSK працює таким чином: він витікає з ключа попередньої сесії, яка називається Pairwise Transient Key (PTK).

PTK, у свою чергу використовує Pre-Shared Key і п'ять інших параметрів:

- SSID,
- Authenticator Nounce (ANounce),
- Supplicant Nounce (SNounce),
- Authenticator MAC-address (MAC-адрес точки доступу),
- Supplicant MAC-address (MAC-адреса Wi-Fi клієнта).

Цей ключ надалі використовує шифрування між точкою доступу та Wi-Fi клієнтом. Зловмисник, який у цей момент часу прослуховує ефір, може перехопити усі п'ять параметрів. Єдиною річчю, якою не володіє лиходій це Pre-Shared key.

Pre-Shared key виходить завдяки використанню парольної фрази WPA-PSK, яку відправляє користувач, разом з SSID.

Комбінація цих двох параметрів пересилається через Password Based Key Derivation Function, яка виводить 256-бітовий загальний ключ.

У звичайній WPA/WPA2 PSK атаці по словнику, зловмисник використовуватиме програмне забезпечення, яке виводить 256-бітовий ключ для кожної парольної фрази і буде використовувати її з іншими параметрами, які були описані в створенні PTK.

PTK використовуватиметься для перевірки Message Integrity Check (MIC) в одному з пакетів.

Якщо вони співпадуть, то парольна фраза в словнику буде вірною. При цьому використовуються уразливості протоколу аутентифікації користувачів це відкрита передача ANounce, SNounce, MAC-адреса точки доступу і MAC-адреси Wi-Fi клієнта.

Якщо при відтворенні алгоритму аутентифікації станеться «успішна авторизація користувача», означає, що вибраний зі словника пароль є істинним і атака призводить до успішного злому мережі. [2]

Відповідно до світового аналізу бездротових точок доступу серед 32 мільйонів точок доступу Wi-Fi, більше 20% пристроїв використовують відкриті бездротові мережі. 68 % використовують WPA2 (рис. 3.3) [3].

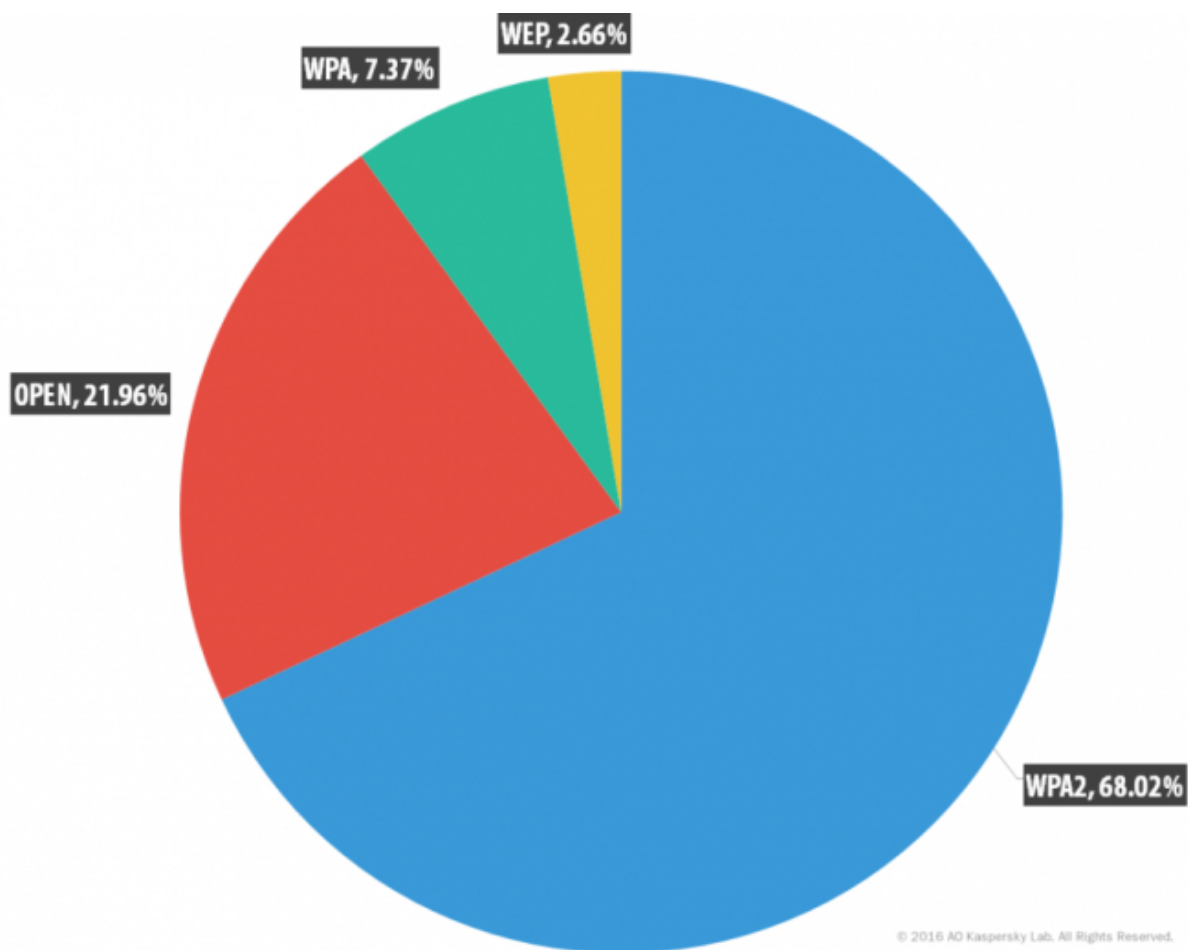


Рис. 3. 3. Розподілення мереж за типами захисту

Саме тому, враховуючи поширеність бездротових мереж Wi-Fi та алгоритму їх захисту WPA2, присвячується спосіб вдосконалення для паролей, які максимально йому відповідають.

3.2. Послідовність вдосконалення способу генерування паролів

Процедура (послідовність) вдосконалення полягає в такому.

Етап 1. Визначення швидкості підбору паролів та обґрунтування їх стійкості.

Для сучасного комп'ютера домашнього користувача при стандартних режимах його роботи з використанням центральних процесорів (CPU), швидкість підбору може становити 6000-7000 паролів за секунду. Залежно від моделі та режиму роботи, вона може відрізнятись.

Для зручності обчислення кількості можливих варіантів підбору паролю за певний проміжок часу в роботі було зроблено припущення, що за одну секунду роботи CPU може перебрати біля 10 000 паролів із обраних сукупностей.

Збільшити швидкість підбору паролів у сотні й тисячі разів можливо завдяки використанню графічних процесорів у відео-картах (GPU) та GPU-ферм (наприклад 12 відео-карт, об'єднаних для спільної роботи).

За таких умов швидкість підбору паролів становитиме від 15 млрд. до 180 млрд. за секунду й більше.

Ймовірні значення кількості підбору паролів для випадків підбору з використанням CPU, GPU та GPU-ферми (з 12 GPU) в межах від одної секунди до одного року наведено в таблиці 3.1.

Таблиця 3.1

Кількість можливих варіантів підбору паролю за певний проміжок часу

Кількість паролів			
CPU	GPU	GPU-ферма (з 12 GPU)	Час
10^4	$1,5 \cdot 10^{10}$	$1,8 \cdot 10^{11}$	1 секунда
$6 \cdot 10^5$	$9 \cdot 10^{11}$	$1,08 \cdot 10^{13}$	1 хвилина
$3,6 \cdot 10^7$	$5,4 \cdot 10^{13}$	$6,48 \cdot 10^{14}$	1 година
$8,64 \cdot 10^8$	$1,3 \cdot 10^{15}$	$1,56 \cdot 10^{16}$	1 доба
$3,15 \cdot 10^{11}$	$4,73 \cdot 10^{17}$	$5,68 \cdot 10^{18}$	1 рік

Якщо в якості певної сукупності паролів взяти множину можливих мобільних телефонів, у форматі + 380 YY XXX XX XX (YY код регіону або мобільного оператора, де є 16 кодів оператора, або 48 кодів регіонів та операторів України, XXX XX XX номер телефону).

Для перебору з використанням CPU, наприклад, мобільних номерів потрібно 4 години 26 хвилин, а для перебору кодів регіонів та операторів України приблизно 13 годин 18 хвилин. ____

З використанням для перебору паролів GPU-ферм тривалість відповідних операцій можна зменшити, як мінімум, у 18 млн. разів.

Як результат, логічним, хоча і доволі тривіальним, є висновок: чим більша тривалість підбору – тим пароль буде більш стійким до підбору і навпаки.

Оскільки множини паролів можуть здаватися стійкими до підбору на CPU, а швидкості GPU та GPU-ферм по підбору паролів є значно більшими, то постає необхідність у пошуку множин паролів для формування парольних політик.

Етап 2. Визначення множин паролів для парольних політик.

Математично парольні множини для парольних політик можна описати, як вибірку з певних символів:

- *сполучення з символів для паролів* (комбінація), коли з n елементів (кількості можливих символів) вибирають k (довжина обраного паролю), порядок не має значення;
- *розміщення з символів для паролів*, коли з n елементів вибирають k в певному порядку;
- *розміщення з повтореннями з символів для паролів*, коли число всіх розміщень з n елементів вибирають k , з повтореннями.

Статистичною (емпіричною) функцією розподілу вибірки множини паролів є закон зміни частоти події підбору пароля, при $X < x$:

$$F^*(x) = \frac{a(x)}{a}, \quad (3.1)$$

де $a(x)$ – число значень варіантів паролю, для яких $x \leq X$,

X – випадкова величина множини паролів, розподіл якої невідомий;

a – об'єм вибірки множини паролів.

Аналогом теоретичної диференціальної функції (густини) розподілу є щільність відносної частоти:

$$f_i = \frac{W_i}{h} \quad (3.2)$$

де W_i – відносна частота, h – інтервал підбору.

На відміну від емпіричної функції розподілу вибірки множини паролів функція розподілу $F(x)$ генеральної сукупності їх множини є теоретичною функцією розподілу.

Різниця між ними полягає в тому, що теоретична функція $F(x)$ визначає ймовірність підбору $X < x$, а емпірична функція $F^*(x)$ визначає відносну частоту цього ж підбору.

Емпірична (статистична) функція розподілу вибірки множини паролів є оцінкою теоретичної функції розподілу генеральної сукупності їх множини.

Математичне сподівання характеризує середнє значення, біля якого групуються можливі значення випадкової величини підбору, а дисперсія характеризує степінь розсіювання цих значень відносно середнього.

Середнє арифметичне спостережуваних значень випадкової величини множини паролів:

$$M^*[X] = \frac{\sum_{i=1}^k x_i n_i}{n} = x_e \quad (3.3)$$

де x_i – значення випадкової величини паролю,

$n = \sum_{i=1}^k n_i$ – число випробувань можливого підбору (об'єм вибірки).

Статистичні початкові та центральні моменти вибірки довільних порядків m :

$$M[(X - x_r)^m] = \frac{\sum_{i=1}^k (x_i - x_r)^m N_i}{N} \quad (3.4)$$

При збільшенні числа спостережень вибірки множини паролів всі статистичні характеристики будуть збігатись за ймовірністю до відповідних числових характеристик генеральної сукупності їх множини.

$$\text{При } M \rightarrow \text{Max}, P_z \rightarrow 0$$

Для даних паролів можливі деякі відмінності, за кількістю множини.

Сполучення множини паролів (комбінація). З n елементів вибирають k , порядок не має значення.

$$C_n^k = \frac{n!}{(n-k)! \cdot k!} \quad (3.5)$$

де n - кількість можливих символів;

k - довжина обраного паролю.

В даному випадку:

$n=88$ - ASCII: 26 прописних літер, 26 заголовних літер, 10 цифр, 26 спеціальних символів;

$k=63$ - кількість символів у паролі для WPA/WPA2.

Розміщення множини паролів. З n елементів вибирають k в певному порядку.

$$A_n^k = \frac{n!}{(n-k)!} \quad (3.6)$$

де n - кількість можливих символів;

k - довжина обраного паролю.

Розміщення з повтореннями множини паролів. Число всіх розміщень з n по k з повтореннями.

$$A'_n{}^k = n^k \quad (3.7)$$

де n - кількість можливих символів;

k - довжина обраного паролю [4].

Залежно від обраного типу захисту мережі та варіанту обмеження у виборі символів, можливі різні значення кількості паролів.

В таблиці 3.2 розглянуто можливі множини паролів для парольних політик, залежно від варіанту захисту бездротових мереж Wi-Fi з використанням WPA/WPA2.

Таблиця 3.2

Кількість паролів, що використовуються для захисту
бездротових мереж Wi-Fi

Варіанти захисту	Кількість символів в паролі	Кількість отриманих паролів для парольних політик		
		Сполучення	Розміщення	Розміщення з повтореннями
WPA/WPA2	64 шістнадцяткових символи	0	$1.12 \cdot 10^{21}$	$8.22 \cdot 10^{85}$
WPA/WPA2 (TKIP 128 біт)	63 символи ASCII	$6.03 \cdot 10^{21}$	$1.19 \cdot 10^{109}$	$3.18 \cdot 10^{122}$
+WPS(QSS) Налаштування швидкого підключення, що несе уразливість	8 цифр, одна з яких відповідає за контрольну суму, тому підбирається 7, через помилку підбирається 4 перших, або 4 останніх з 7	$6.05 \cdot 10^5$	$10^4 + 10^3$	10^7

Примітка: $n=88$ - ASCII: 26 прописних літер, 26 заголовних літер, 10 цифр, 26 спеціальних символів; $k=63$ - кількість символів у паролі для WPA/WPA2.

Як видно з таблиці 3.2, знання зловмисником технологій формування парольних політик (наприклад, шляхом сполучення множини паролів або розміщення з повтореннями множини паролів) надасть йому перевагу в часі на підбір паролю без повторень приблизно у $5.27 \cdot 10^{100}$ разів.

Разом з тим, слід зазначити, що кількість паролів для певної множини дозволяє оцінити лише саму множину паролів за її величиною, але не дає можливості оцінити власне стійкість паролю, оскільки вона залежить від способу, за яким створюється пароль (табл. 2.1) та від можливої швидкості його підбору.

Частковий збіг з паролями в існуючих словниках може зменшити час, що необхідний для його підбору.

Існує можливість збільшити значення швидкості підбору в тисячі разів, завдяки використанню графічних процесорів у відео-картах (GPU).

На прикладі однієї із відео-карт, що використовується для перебору хешів паролів, швидкість підбору може становити до 15 млрд. за секунду, а з використанням GPU-ферм може досягати 200 млрд. за секунду.

Спеціалізовані ферми можуть досягати значення в 350 млрд. переборів за секунду, та не обмежуються цим значенням.

Тому постає задача з вибору множин і підмножин паролів для ускладнення, а також формування відповідних змінних правил, які б дозволили зменшити ймовірність підбору ускладнених паролів.

Етап 3. Формування змінних правил ускладнення для сполучення множини паролів.

Із сполучення множини паролів U_p відбирається множина U_z (рис. 3.4), що складається з паролів, які мають в собі 2 або 3 числа від двох до восьми цифр.

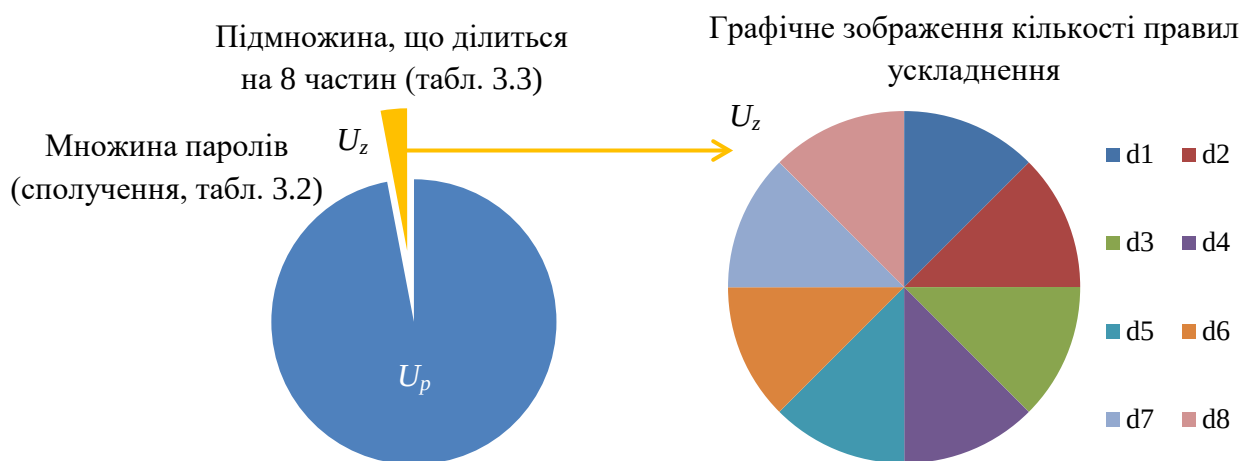


Рис.3. 4. Кількість чисел, що можуть бути частиною паролю

До U_z потрапляють паролі, які містять 2 або 3 числа, довжиною від 2 до 8 цифр, або комбінацій набору символів, що можуть бути в словниках.

В свою чергу із множини U_z за певним правилом d ($d1\dots d8$), що визначається кількістю та довжиною чисел, виділяються 8 підмножин $U_{l(d)}$, (від 2 до 8 цифр), що прописуються в кожному рядку таблиці 3.3.

Таблиця 3.3

Кількість чисел, що можуть бути частиною паролю

$U_{l(d)}$	Кількість чисел у паролі	Кількість цифр у числі				Кількість комбінацій
$d1$	3	3	3	3	1	$U_{l(d1)}$
$d2$	3	4	3	2	1	$U_{l(d2)}$
$d3$	3	4	3	3		$U_{l(d3)}$
$d4$	3	4	4	2		$U_{l(d4)}$
$d5$	2	5	5			$U_{l(d5)}$
$d6$	2	6	4			$U_{l(d6)}$
$d7$	2	7	3			$U_{l(d7)}$
$d8$	2	8	2			$U_{l(d8)}$

З підмножини $U_{l(d)}$ відповідно до обраного номеру правила d обираються паролі, які додаються до множини ($U_p - U_z$).

Це, в свою чергу, створює множину U_k . Графічно умовні множини символів для паролів можна зобразити так, як показано на рис.3.4.

Даний підхід забезпечує трирівневе ускладнення паролю, оскільки:

по-перше, при додаванні паролів обираються лише ті, що складаються з певної кількості цифр (відповідно до певного правила d);

по-друге, при виборі правила d для множини ускладнених паролів, воно може бути як змінним (тобто не мати залежності/порядку), так і сталим (наприклад: всі паролі за одним правилом);

по-третьє, при використанні змінного порядку правил ускладнення d під час генерування паролів (наприклад, кожен пароль по черзі за певним правилом, або будь-яка кількість паролів за кожним із правил у хаотичному порядку і т.д.), унеможлиблюється створення такої ж процедури генерування паролів зловмисником.

Етап 4. Розрахунок кількості паролів для можливих парольних множин.

Формула розрахунку кількості можливих комбінацій паролів матиме вигляд:

$$U_{l(d)} = C_l^m \cdot C_{l-m}^m \cdot C_{l-2m}^m \cdot \dots \cdot C_{l-(r-1)m}^m \cdot C_{l-rm}^m \quad (3.8)$$

де l – кількість літер алфавіту;

m – кількість літер в слові (3...6);

$r = 1 \dots m$, при умові: $m < rm < l$.

В даному випадку добуток комбінацій означає поєднання значень паролів, кількість цифр у яких, сумарно дорівнює 10.

Для кожної довжини чиста та поєднання отримаємо певне значення комбінацій, що може бути використане для розрахунку.

Отже, для кожного $U_{l(d)}$ в таблиці 6 буде обчислене певне значення за формулою (3.8). Загальна кількість паролів для парольної множини U_z буде сумою значень підмножин $U_{l(d)}$, розрахованих за формулою (3.9):

$$U_z = U_{l(d1)} + \dots + U_{l(d16)} \quad (3.9)$$

Враховуючи, що при формуванні ускладненої парольної множини можливе використання $(U_p - U_z)$ та $d1$ або $(U_p - U_z)$ та $d2$ або $(U_p - U_z)$ та $d3$ і т.д., - кінцеве значення ускладненої множини буде розраховуватись за формулою (3.10):

$$U_k = (U_p - U_z) \cdot U_z \quad (3.10)$$

де U_k – кількість паролів для кінцевої, ускладненої, множини паролів;

U_p – початкове значення кількості паролів (сполучення з таблиці 3.2);

U_z – значення кількості комбінацій чисел, з різної кількості цифр, формула (3.9).

Формула (18) отримана з суми добутків початкової комбінації U_p без множини U_z та значень d , що в результаті дає кінцеве, ускладнене, значення.

Для окремого розрахунку ускладненої множини паролів, за одним із можливих правил d , використовується формула (3.11):

$$U_{k(d)} = (U_p - U_z) \cdot U_{l(d)} \quad (3.11)$$

де $U_{k(d)}$ – ускладнена комбінація за обраним правилом d ,

U_p – початкове значення кількості паролів (сполучення з таблиці 3.2),

U_z – значення комбінацій чисел, з різної кількості цифр з формули (3.9),

$U_{l(d)}$ – кількість комбінацій чисел, з кількості цифр за правилом, формула (3.8).

3.3. Додаткове ускладнення при генеруванні способу

На етапі 3 можливо обрати не числа, а наприклад, букви. Із сполучення множини паролів U_p відбирається множина U_z (рис. 3.5), що складається з паролів, які мають в собі малі літери англійського алфавіту.

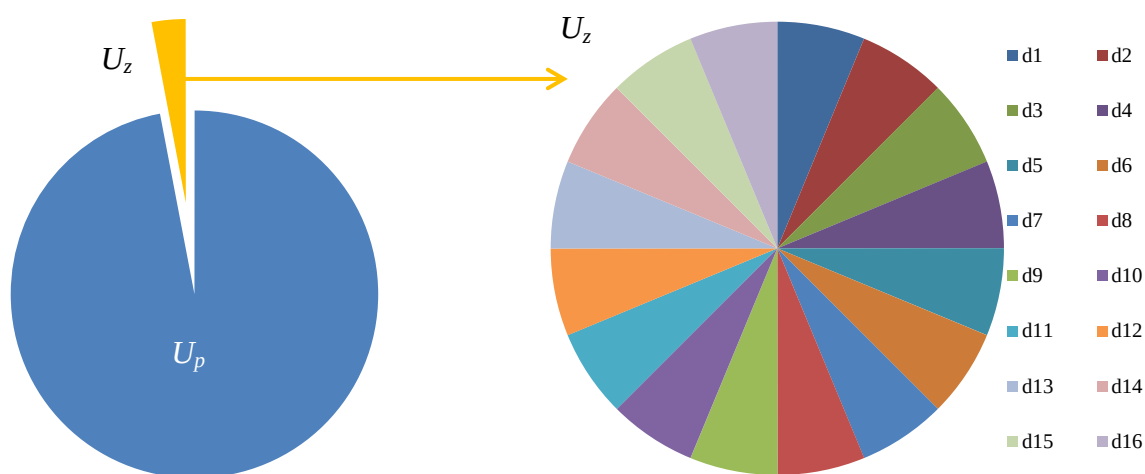


Рис. 3.5. Кількість слів, або набору символів, що може бути частиною паролю

До U_z потрапляють паролі, які містять 3 або більше простих слів англійською мовою (з 26 прописних літер ASCII, $l=26$) довжиною до 6 символів, або комбінацій набору символів, що можуть бути в словниках.

Із множини U_z за певним правилом d ($d1\dots d16$), що визначається кількістю та довжиною слів (набору символів), виділяються 16 підмножин $U_{l(d)}$, (від 3 до 6 літер), що прописуються в кожному рядку таблиці 3.4.

Таблиця 3.4

Кількість слів, або набору символів, що може бути частиною паролю

$U_{l(d)}$	Кількість слів у паролі	Кількість літер у слові										Кількість комбінацій
$d1$	4	6	6	6	6	2						$U_{l(d1)}$
$d2$	5	6	6	6	5	3						$U_{l(d2)}$
$d3$	5	6	6	5	5	4						$U_{l(d3)}$
$d4$	5	6	5	5	5	5						$U_{l(d4)}$
$d5$	5	5	5	5	5	5	1					$U_{l(d5)}$
$d6$	5	5	5	5	5	4	2					$U_{l(d6)}$
$d7$	6	5	5	5	4	4	3					$U_{l(d7)}$
$d8$	6	5	5	4	4	4	4					$U_{l(d8)}$
$d9$	6	5	4	4	4	4	4	1				$U_{l(d9)}$
$d10$	6	4	4	4	4	4	4	2				$U_{l(d10)}$
$d11$	7	4	4	4	4	4	3	3				$U_{l(d11)}$
$d12$	7	4	4	4	4	3	3	3	1			$U_{l(d12)}$
$d13$	7	4	4	4	3	3	3	3	2			$U_{l(d13)}$
$d14$	7	4	4	3	3	3	3	3	3			$U_{l(d14)}$
$d15$	8	4	3	3	3	3	3	3	3	1		$U_{l(d15)}$
$d16$	8	3	3	3	3	3	3	3	3	2		$U_{l(d16)}$

З підмножини $U_{l(d)}$ відповідно до обраного номеру правила d обираються паролі, які додаються до множини $(U_p - U_z)$. Це, в свою чергу, створює множину U_k . Графічно умовні множини символів для паролів можна зобразити так, як показано на рис.3.5.

Кожне значення правила d розраховується для кожного варіанту за формулою комбінацій де:

- довжина паролю становить 26 символів,
- пароль може складатись з декількох слів (від 4 до 8 слів довжиною від 3 до 6 букв).

Оскільки можливе поєднання різних слів з різною кількістю букв у слові, то для розрахунку довелося використовувати добуток та додавання комбінацій, відповідно до правил комбінаторики для «і» та «або».

Таким чином добуток комбінацій означає поєднання кількості значень паролів, кількість букв у яких, сумарно складають довжину алфавіту.

Для кожної довжини слова та поєднання слів різної довжини отримаємо певне значення комбінацій, що можна буде використати для розрахунку [5].

Висновки до третього розділу

Таким чином, зазначена процедура (послідовність) вдосконалення випадкового паролю завдяки використанню інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів (використовуючи змінний вибір правила ускладнення d), а також урахуванню можливостей співпадіння з паролями системи словників та розширення множини U_z (за рахунок використання набору букв/символів, або слів іншою мовою) дозволяє:

по-перше, створити пароль, ймовірність підбору якого серед певної множини паролів U_k буде мінімальною;

по-друге, збільшити кількість варіантів правила ускладнення d та кількість можливих комбінацій підбору, а також рівень невизначеності для злоумисника.

Список використаних джерел у третьому розділі

1. Защита в сетях Wi-Fi. URL: https://ru.wikipedia.org/wiki/Защита_в_сетях_Wi-Fi (дата звернення: 22.05.2017).
2. Новые требования к паролям Стэнфордского университета_ баланс между длиной и сложностью. URL: <https://habr.com/ru/post/220949/> (дата звернення: 23.06.2017).
3. Research on unsecured Wi-Fi networks across the world. URL: <https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/> (дата звернення: 25.06.2018).
4. Аносов А. О. Модель перехоплення та захист інформації в бездротових мережах / А. О. Аносов, А. В. Платоненко. // Сучасний захист інформації. – 2017. – №2. – С. 90–94.
5. Бурячок В.Л. Генерування паролю для бездротових мереж з використанням змінного правила ускладнення/ В.Л. Бурячок, А. О. Аносов,
6. Атаки на беспроводные сети. Часть 1. 2004. URL: <https://www.securitylab.ru/analytics/216360.php> (дата звернення: 27.06.2018).
7. Wi-Fi сети_ проникновение и защита. 2) Kali. Скрытие SSID. MAC-фильтрация. URL: <https://habr.com/ru/post/225483/> (дата звернення: 12.03.2018).
8. Wifi Network Security Statistics_Graph. URL: <https://graphs.net/wifi-stats.html> (дата звернення: 12.03.2018).
9. **Платоненко А.В.** Захист інформації у безпроводових мережах WI-FI./ Платоненко А.В. // Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави» – Київ: ДУТ, 2014 – С.40-41.
10. **Платоненко А.В.** Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах. / Платоненко А.В. // Науково-технічна конференція «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.34-35.
11. **Платоненко А.В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв в Україні. / Платоненко А.В. // III Міжнародна науково-технічна конференція студентства та молоді» – Київ: ДУТ, 2016 – С.134-136.

Розділ 4

ДОСЛІДЖЕННЯ ЗАПРОПОНОВАНИХ СПОСОБІВ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

4.1. Алгоритм генерування стійкого паролю зі змінним правилом ускладнення

При проектуванні систем захисту інформації розробник повинен вирішувати складні завдання, пов'язані зі створенням відповідного математичного та апаратного забезпечення, реалізацією необхідного рівня захищеності об'єкта. Крім того, він повинен враховувати особливості апаратури, що використовується та елементної бази, виходячи з архітектури системи і в умовах різних ускладнюючих ситуацій.

Розглянемо методику синтезу оптимальної структури систем захисту інформації. Можливі два підходи до вирішення завдання синтезу структури систем захисту інформації, засновані на конфігурації системи виду:

- універсальна система - спеціалізована система;
- уніфіковані блоки - спеціалізована система.

Перший варіант прийнятний, коли система проектується на стандартних елементах, тобто використовуються серійно випускається апаратура. В цьому випадку оптимізація структури, полягає у відповідному усунення надмірності апаратних коштів. Такий синтез системи найменш трудомісткий і до його переваг можна віднести:

- використання всього математичного забезпечення, що є в розпорядженні керуючого комп'ютера;
- можливість налагодження алгоритмів і програм на комп'ютері в реальному масштабі часу;
- скорочення термінів розробки.

Недоліком даного варіанту синтезу є обмежена мінімізація системи, складність і високі вимоги до архітектури і обсягом пам'яті. Однак синтез системи за цією методикою забезпечує програмну сумісність.

Синтез системи на основі другого підходу передбачає створення повністю самостійної структури системи, яка реалізується на уніфікованих функціональних блоках і комплексах програмного забезпечення в ній, що дозволяють найкращим чином реалізувати алгоритми вирішення заданих завдань.

Цей підхід передбачає мінімальну надмірність програмного забезпечення, завдяки компромісу між застосуванням і вибором програмних і апаратних засобів в системі. При цьому системи, що мають кілька рівнів обробки інформації та що розробляються на базі уніфікованих функціональних блоків, дозволяють забезпечити:

- високий ступінь автоматизації процесів обробки інформації;
- простоту вибору та зміни режимів роботи;
- різноманіття форм і форматів даних, що вводяться і параметрів контролю,
- виведених даних, отриманих після обробки інформації;
- простоту сполучення системи з зовнішніми пристроями.

Процес проектування та синтезу системи захисту інформації на базі мікропроцесорів можна розділити на два етапи: розробку і вибір апаратних засобів і програмного забезпечення.

При розробці пакетів великих програм раціонально використовувати метод поетапного уточнення з дотриманням принципу модульності, що зменшує ступінь взаємодії і взаємозалежності програмних модулів і тим самим істотно полегшує налагодження програм.

На етапі розробки апаратних засобів основним завданням розробника є вибір оптимальної архітектури системи, оптимальної структури уніфікованих блоків, визначення обсягів оперативної і постійної пам'яті. При цьому побудові системи необхідно передбачати включення, як уніфікованих функціональних блоків, мікрокомп'ютерів, генераторів шуму, приймачів, і т.п.

Блоковий принцип побудови системи забезпечує ефективне використання її ресурсів при використанні уніфікованих функціональних вузлів.

Виконати оптимальний синтез з метою створення системи, що забезпечує одночасне рішення всіх задач заданого класу в силу алгоритмічної різноманітності і

складності окремих завдань досить складно, тому його раціонально проводити в такій послідовності:

- сформулювати вимоги до системи і на їх підставі виробити узагальнений алгоритм;
- синтезувати структуру системи відповідно до узагальненим алгоритмом на базі розроблених уніфікованих функціональних блоків;
- включити додаткові модулі для розширення структури і програмного забезпечення системи, що дозволяє вирішувати більшу кількість завдань [1].

Для впровадження розробленого способу сформовано алгоритм, який описує всі його етапи та дає змогу створити необхідне програмне забезпечення для автоматизованого генерування стійкого паролю в залежності від вимог системи, для якої буде використовуватись розглянутий спосіб.

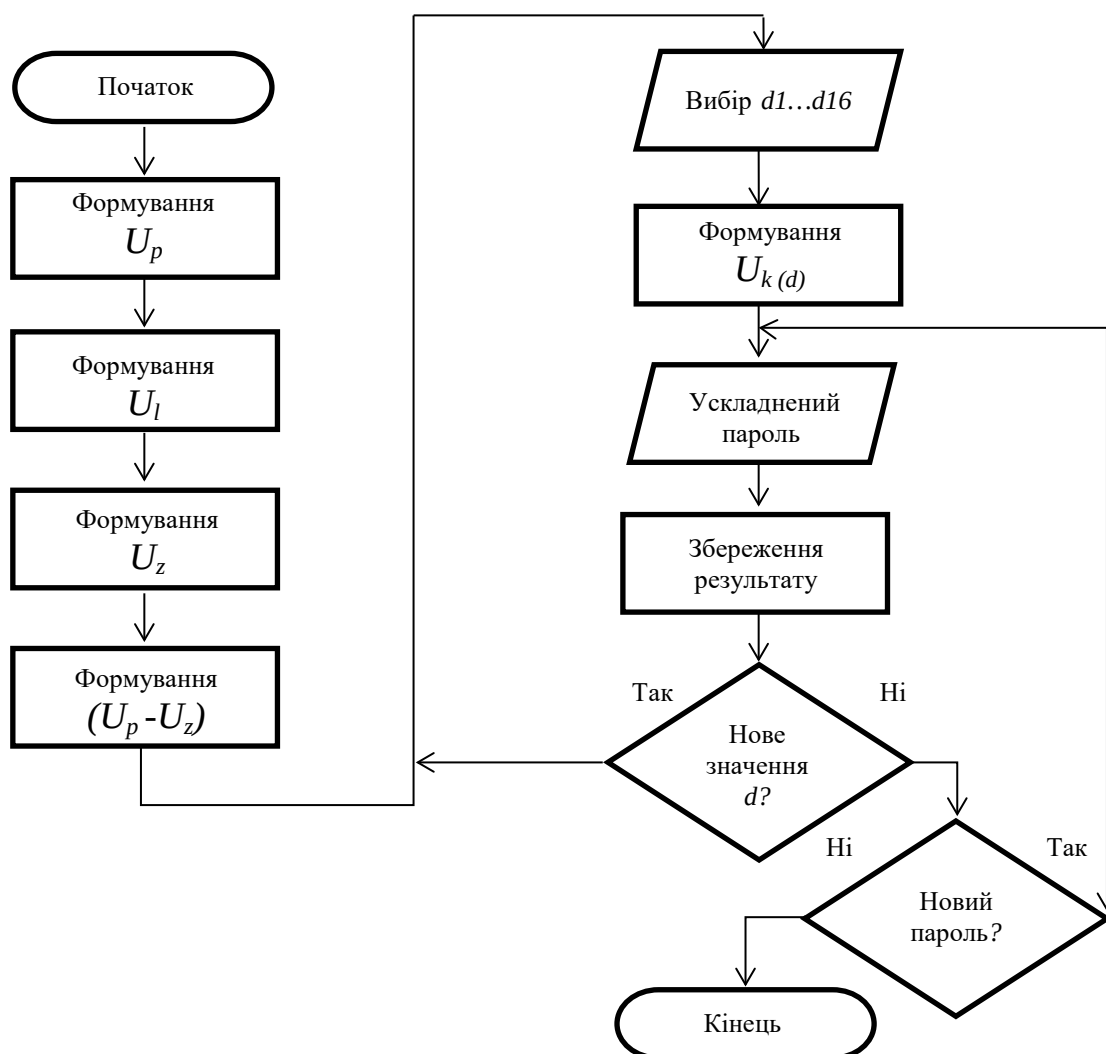


Рис. 4.1. Алгоритм генерування стійкого паролю зі змінним правилом ускладнення

На рис. 4.1 приведено блок-схему алгоритму, що відображає процес генерування паролів для ускладненого паролю.

На початку обирається множина паролів U_p за правилом комбінації, з використанням символів без повторень, в якій кількість можливих паролів становить $6,03 \cdot 10^{21}$.

Відповідно до таблиці 6, залежно від значення d , кожне значення $U_{l(d)}$ розраховується окремо, оскільки кількість можливих слів, або комбінацій символів може бути різної довжини.

Розраховані значення кількості слів, що можуть бути частиною паролю, для кожного $U_{l(d)}$ наведено в таблиці 4.1.

Таблиця 4.1

Розрахунок кількості чисел, що можуть бути частиною паролю

$U_{l(d)}$	Розрахунок	Кількість комбінацій
1	$U_{10(d1)} = C_{10}^3 \cdot C_7^3 \cdot C_4^3$	16 800
2	$U_{10(d2)} = C_{10}^4 \cdot C_6^3 \cdot C_3^2$	12 600
3	$U_{10(d3)} = C_{10}^4 \cdot C_6^3 \cdot C_3^3$	4 200
4	$U_{10(d4)} = C_{10}^4 \cdot C_6^4 \cdot C_3^2$	3 150
5	$U_{10(d5)} = C_{10}^5 \cdot C_5^5$	252
6	$U_{10(d6)} = C_{10}^6 \cdot C_4^4$	210
7	$U_{10(d7)} = C_{10}^7 \cdot C_3^3$	120
8	$U_{10(d8)} = C_{10}^8 \cdot C_2^2$	45
Всього		37 377

Підмножина U_z складається з $3,73 \cdot 10^4$ паролів, що відповідно до формули (17) складається з суми значень $U_{l(d)}$.

Відповідно до обраного d , значення $U_{l(d)}$ приєднується до множини $(U_p - U_z)$, що в свою чергу створює ускладнену, за одним з правил, множину $U_{k(d)}$ з кількості паролів що розраховується за формулою (3.11).

Таким чином, загальна кількість комбінацій можливих слів з 2 або 3 чисел від 2 до 8 цифр складає $3,73 \cdot 10^4$ (U_z), а кількість можливих комбінацій паролів без даних комбінації чисел, практично не зміниться, та становитиме $6,03 \cdot 10^{21}$ ($U_p - U_z$).

За рахунок введення правила ускладнення d та вибіркового додаванню паролів, маємо кінцеве значення $2,25 \cdot 10^{26}$ (U_k).

4.2. Порівняння стійкості паролівних множин

Порівняння стійкості паролівних множин до підбору розглянуті в таблиці 4.2.

Таблиця 4.2

Кількісна оцінка стійкості паролівних множин

Парольна множина	Кількість паролів у парольній множині	Коефіцієнти стійкості			
		1	-	-	-
Мобільний номер 10 цифр (16 кодів оператора)	$1,6 \cdot 10^8$	1	-	-	-
Телефонний номер України 10 цифр (48 кодів регіонів)	$4,8 \cdot 10^8$	3	1	-	-
Випадкова комбінація 8 символів ASCII	$6,43 \cdot 10^{10}$	$4,02 \cdot 10^2$	$1,34 \cdot 10^2$	1	-
Випадкова комбінація 63 символи ASCII	$6,03 \cdot 10^{21}$	$3,77 \cdot 10^{13}$	$1,26 \cdot 10^{13}$	$9,38 \cdot 10^{10}$	1
Ускладнена комбінація 63 символи ASCII	$2,25 \cdot 10^{26}$	$1,40 \cdot 10^{18}$	$4,68 \cdot 10^{17}$	$3,50 \cdot 10^{15}$	$3,73 \cdot 10^4$

Примітка: коефіцієнт стійкості, що дорівнює 1 обирається для парольної множини, з якої починається порівняння.

Як видно з таблиці 4.2, для перебору випадкової комбінації з 63 символів ASCII знадобиться в $3,77 \cdot 10^{13}$ разів більше часу, ніж на підбір мобільного номеру, а для підбору паролю з множини сформованої ускладненим способом необхідно у $3,73 \cdot 10^4$ разів більше часу, ніж обраним у другому розділі базовим способом генерування паролів, що підтверджує правильність його вибору для вдосконалення.

4.3. Програмна реалізація способу генерування паролів

Реалізація практичної складової виглядає, як звичний для багатьох, генератор паролів, але з вказанням змінного правила, яке обирається у третьому розділі відповідно до таблиці 3.3.

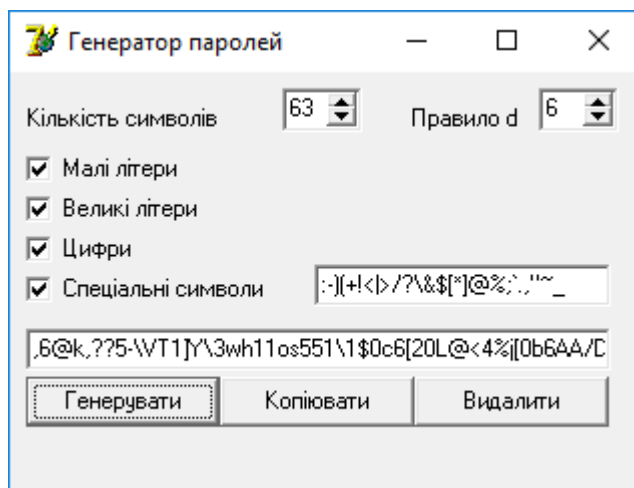


Рис. 4.2. Програмна реалізація генератора паролей

Відповідно до описаних етапів формування паролю в програмному забезпеченні є змога обрати необхідку кількість символів у паролі, символи з яких він буде складатись та правило ускладнення d . Крім кнопки генерування, для зручності є змога зкопіювати пароль та видалити його.

4.4. Практична реалізація та опис технічного обладнання

Окрім налаштувань точок доступу таких моделей як TP-Link, D-Link, Xiaomi, на практичній частині запропонований спосіб використовувався у налаштуваннях безпеки моделей, що застосовують бездротові системи типу Wi-Fi для підключення, а саме:

- DJI Phantom 3 Standard,
- DJI Spark,
- DJI Mavic AIR
- DJI Osmo.

Для підключення між пультом керування та квадрокоптером використовується свій протокол зв'язку, але для підключення мобільного телефону до пульта керування, з метою одержання зображення з камери безпілотної використовуються звичайне Wi-Fi з'єднання.



Рис. 4.3 DJI Phantom 3 Standard з пультом керування та мобільним пристроєм

Для підключення DJI Spark та DJI Mavic AIR можна використовувати тільки мобільний телефон, без необхідності підключення до пульта керування, але в DJI Spark, так само як і в DJI Phantom 3 Standard є змога підключатись до пульта завдяки бездротовому з'єднанню.

Пульт DJI Mavic AIR до мобільного телефону має тільки дротове підключення, що робить передачу зображення з камери більш надійним та

стабільним. З наземних пристроїв тестувалась система DJI Osmo, яка через бездротову мережу Wi-Fi передає зображення на мобільний телефон.



Рис. 4.4 DJI Spark з пультом керування



Рис. 4.5 DJI Mavic AIR з пультом керування



Рис. 4.6. DJI Osmo з підключеним мобільним пристроєм

Всі вищевказані моделі пройшли тестування з паролем для їх захисту, що був згенерований запронованим способом. Формування паролю не вплинуло на продуктивність роботи пристроїв та залишило гарне враження у фахівців.

4.5. Вплив зовнішніх факторів на роботу бездротової мережі.

Дослідження в області дії потужних електромагнітних випромінювань на електронну інфраструктуру і пошук захисту від них активно ведуться в різних країнах. Джерела електромагнітних імпульсів розробляються в ряді країн з метою досягнення якісно нового рівня радіолокації, радіозв'язку, технологій вирішення інших технічних завдань.

Принцип їх роботи допускає генерацію і випромінювання в навколишній простір не лише одиничних електромагнітних сигналів, але і цілих пакетів.

Параметри випромінювання таких пристроїв роблять їх дуже небезпечними при дії на мікроелектронні системи.

Відносна простота виготовлення і доступність придбання таких генераторів, а також компактність цих приладів дозволяють розцінювати їх в якості потенційних засобів навмисного впливу, що дозволяють локально створювати ефекти, подібні до електромагнітних випромінювань ядерного вибуху.

Існує широка номенклатура генераторів, що формують електромагнітні імпульси, які призначені для перевірки стійкості електронного устаткування різних об'єктів до електромагнітного впливу.

Характер порушень в роботі безпосередньо залежить від параметрів і рівня стійкості устаткування до цього впливу.

Порушення в основному носять тимчасовий характер, проявляються під час впливу і зберігаються впродовж деякого періоду після цього впливу, причому виявити факт навмисного електромагнітного впливу, як в цей період, так і надалі – є не можливим.

Електронна інфраструктура, ставши об'єктом електромагнітної атаки, може зазнати ряд деструктивних змін, що, у свою чергу, приведе до збоїв в роботі електронного устаткування і далі – до функціональних порушень видів діяльності, що ним забезпечується.

Систематизований перелік можливих наслідків для засобів інформатизації, використовуваних в основних сферах діяльності, приведений в табл. 4.3.

Таблиця 4.3

**Деструктивні ефекти в електронному устаткуванні
при навмисному електромагнітному впливі (НЕМВ)**

Вид системи	Вид ефекту в результаті дії
Засоби телекомунікації	- зависання і перезавантаження комп'ютерів, - значне зниження інформаційного трафіку, - збільшення кількості помилок.
Засоби зв'язку і навігації	- зменшення ефективної дальності зв'язку (від 2 до 10 разів), - неправдиві свідчення, або збої в засобах навігації.
Засоби безпеки	- збої в системах контролю і управління доступом, - блокування охоронно-пожежної сигналізації, - мимовільне включення устаткування пожежогасіння, - спотворення зображень з камер відео нагляду.

Варто відмітити, що збиток від електромагнітного нападу може бути порівняний з наслідками прямих терористичних атак.

Проблему захисту інформаційних систем від навмисного електромагнітного впливу намагаються розв'язати фахівці різних країн.

Основним напрямом міжнародної діяльності є розробка цільових стандартів по забезпеченню стійкості цивільних об'єктів до впливу потужних електромагнітних випромінювань.

В їхньому числі – методи оцінки стійкості до таких впливів на інформаційні системи телекомунікаційної апаратури і центрів обробки даних, практичні методи захисту комп'ютерних систем, тощо.

Міра ушкодження системи залежить від стійкості як кожного з компонентів пристроїв, так і від енергії потужної завади в цілому, яка може бути поглинена схемою без виявлення дефекту або відмови.

Наприклад, для електромагнітного реле з котушкою на напругу 230 В змінного струму комутаційна завада від індуктивного навантаження з амплітудою 500 В, хоча і є більш ніж двократним перенапруженням, але навряд чи приведе до відмови реле в силу стійкості електромеханіки до такого роду завад, та в свою чергу, малої тривалості такої завади (впродовж мікросекунд).

Інакше виходить з мікросхемою, що живиться від джерела 5 В постійного струму. Імпульсна завада з амплітудою 500 В, у 100 разів перевищує напругу живлення цього електронного компонента і призводить до неминучої відмови і подальшого руйнування пристрою.

Стійкість мікросхем до перенапружень на декілька порядків нижче, ніж стійкість електромагнітного реле.

Оскільки завади, що мають меншу енергію, виникають частіше ніж завади, що мають велику енергію, найбільш частою реакцією електронних систем на дію електромагнітних завад буде не руйнування пристрою, а порушення його роботи або короточасний збій в роботі з наступним відновленням порушеної функції.

Імпульсні перенапруження, що виникають при розрядах блискавок і при комутації в силових електроустановках, здатні пошкодити, або зруйнувати як електронні прилади, так і цілі системи.

Кожну секунду близько 50 блискавок вдаряють по поверхні землі, і в середньому кожен її квадратний кілометр блискавка вражає шість разів за рік. Напруга блискавки може складати до ста мільйонів вольт.

У нормах будівництва громовідводів приймають зазвичай струм блискавки до 200 тисяч ампер при тривалості близько 1 мс, хоча практично струм блискавки рідко перевищує 20-30 кА.

Температура каналу при головному розряді може перевищувати 25000°C . Довжина каналу блискавки може бути від 1 до 10 км, діаметр — декілька сантиметрів.

При ударі блискавки в громовідвід електричний струм (у вигляді імпульсу дзвоноподібної форми) поступає в землю і розтікається в ґрунті на всі боки до декількох десятків і навіть сотень метрів, причому із-за опору ґрунту цей струм створює на ньому падіння напруги.

Оскільки найбільший опір чинять шари ґрунту, що лежать поблизу місця входження струму в землю, то саме тут спостерігається найвища напруга.

В міру видалення від цієї точки опір проходженню струму зменшується, при цьому знижується і напруга.

Для зниження потенціалу, що наводиться при протіканні струму блискавки в ґрунті, опір розтіканню струму в зоні розташування житлових і промислових будівель і споруд зменшують за допомогою металевої сітки досить великої площі, розміщеної в ґрунті під фундаментом будівель.

Проте опір таких заземляючих систем все ще дуже далеко від нуля, і тому навіть залишкові імпульсні потенціали, наведені в заземляючій системі і проникаючі по кабелях на входи електронної апаратури, представляють для неї серйозну небезпеку.

Завади такого роду називаються кондуктивними. Окрім завад такого виду, імпульс сильного струму, що проходить по громовідводу, створює і завади у

вигляді електромагнітних полів, що впливають на усі близько розташовані провідники. Така дія називається індуктивною.

Існують ще і ємнісні наведення, при яких короткі (тобто високочастотні) імпульси перенапруження з високовольтних ліній електропередач потрапляють в низьковольтні ланцюги через ємнісні зв'язки між обмотками трансформаторів.

В процесі поширення завади, має місце багатократне перетворення одного виду на інший, тому таке ділення дуже умовне, особливе коли йдеться про високочастотні процеси. (Імпульс розрядного струму блискавки з досить крутими фронтами – 8 і 20 мкс, можна розглядати саме як такий високочастотний процес.)

Тому аналіз розтікання струму в землі через заземляючі пристрої вимагає обліку обох цих складових.

Більше того, потрапивши в електронну апаратуру за допомогою електромагнітного поля або по дротах, завада зазнає численні перетворення вже всередині цієї апаратури із-за наявності паразитних ємнісних і індуктивних зв'язків між окремими елементами, або між різними вузлами апаратури.

При цьому високочастотна складова завади може проникати углиб апаратури, в обхід встановлених фільтрів і захисних елементів.

Ще один шлях для проникнення завади від розряду блискавки – протікання струмів по заземленому металевому корпусу і заземленим екранам численних кабелів, підключених до нього.

Усе це говорить про те, що забезпечити належний рівень захисту від електромагнітних завад електронної апаратури дуже і дуже непросто.

Особливо складно це зробити на старих підстанціях, системи заземлення яких проектувалися для роботи з електромеханічним захистом, значно стійкішим до електромагнітних дій, чим мікропроцесорна.

Якщо врахувати, що небезпечні підйоми потенціалу в ланцюгах заземлення виникають не лише при ударах блискавки, але і при аварійних коротких замиканнях в електричних мережах, то проблема стане ще складнішою.

В деяких випадках для запобігання такому підйому потенціалу в ланцюгах електронної апаратури контури заземлення силового устаткування і електронної

апаратури роблять роздільними. Проте на реально існуючих підстанціях виконати таке розділення нереально.

Таким чином, тільки комплексне рішення проблеми дозволить уникнути впливу потужних електромагнітних завад. Це рішення повинне включати:

- використання мікропроцесорних реле захисту тільки на підстанціях, спроектованих і побудованих з урахуванням найсучасніших вимог до електромагнітної сумісності і розрахованих на експлуатацію високочутливої електронної апаратури;
- вдосконалення конструкції самих мікропроцесорних реле захисту;
- розміщення мікропроцесорних реле захисту в металевих шафах, спеціально призначених для захисту електронного устаткування і забезпечених фільтрами на усіх кабелях, що входять в шафу.

Зафіксовано електромагнітні атаки на системи безпеки і комп'ютерні мережі банків, автомобільні системи безпеки, військові системи радіозв'язку.

З метою забезпечення безпеки об'єктів інформаційної діяльності, необхідно створювати для них системи захисту інформації від несанкціонованого доступу, знищення, модифікації та блокування інформації. Це передбачає планування і реалізацію комплексу технічних і організаційних заходів, що забезпечують захищеність об'єктів інформаційної діяльності [5].

Канал передачі - це фізичне середовище, яке використовується для передачі сигналу від передавача до приймача. Атмосфера може бути каналом у бездротовому зв'язку.

Телефонні канали зазвичай використовують ряд фізичних носіїв, включаючи дротові лінії, волоконно-оптичні кабелі та бездротові лінії (мікрохвильові радіолінії).

Для будь-якого фізичного середовища важливим є схильність до випадкових викривлень через такі механізми, як аддитивний вплив теплового шуму, який створюється електронними пристроями, вплив зовнішніх джерел, який може створювати як аддитивний, так і мультиплікативний шум.

Вплив шуму можна зменшити за рахунок збільшення потужності переданого сигналу. Однак функціональні та інші практичні вимоги обмежують рівень потужності переданого сигналу.

Також основні обмеження включають доступну частотну смугу частоти передаючого каналу. Обмеження частотної смуги частот обумовлене фізичними обмеженнями середовища та електричних компонентів, що використовуються в передавачі та в приймачі.

Кожна проблема захисту надійності та шумозахисту телекомунікаційної мережі має своє остаточне рішення.

Проблема підвищення шумозахищеності може бути представлена як проблема фільтрації, інакше кажучи, відділення корисної інформації від перешкод (спотворення). Є дві основні проблеми фільтрації:

1. Відокремлення корисної інформації від втручання (шуму) без втрати корисної інформації. Це головне завдання передачі інформації.

Якщо рішення неможливо з якихось причин, то необхідно звести до мінімуму появі спотворень через певний критерій оптимальності.

2. Відокремлення корисної інформації від цілої інформації та від шуму, що означає відстежувану втрату частини корисної інформації.

Це основна проблема керуючого обладнання, і тут дозволені спотворення корисного сигналу. Тим часом інформаційний струм змінюється на функції та значення, які певним чином характеризують вихідний процес.

Вибір методу захисту від шуму залежить від типу корисних сигналів та шумів. Існує три основні типи сигналів та шумів:

1. Сигнали, розділені по частоті. Ці сигнали обмежені відносно вузькою смугою і допускають вибір частоти. Вони включають гармонічні коливання та вузькосмугові процеси.

2. Сигнали, розділені за часом. Вони з'являються (періодично чи неперіодично) у дискретні моменти часу та потребують так званих імпульсних методів поділу. Цей тип сигналів включає імпульсні послідовності, дискретні широкосмугові сигнали.

3. Сигнали шуму. Ці сигнали блокують широку смугу і змінюються в часі постійно. Зазвичай у теоретичних дослідженнях для простоти вважають, що такий розподіл ймовірностей є нормальним.

Тим часом, вибираючи метод, необхідно враховувати попередні та задні дані про характеристики корисного сигналу та шуму. Проблема шумозахисту системи ускладнюється тим, що на задній частині внутрішніх (апаратних) та зовнішніх детермінованих шумів, на неї часто впливає хаотичний імпульсний шум зі спонтанним розподілом ймовірностей. Таким чином, колективний розподіл ймовірності сигналу та шуму також є спонтанним [6].

Потреба в збільшенні пропускної здатності мереж зв'язку подвоюється щороку, і цей темп навряд чи сповільниться найближчим часом.

Крім того, ця потреба дедалі ширшим стає географічно. Зниження цін постачальниками, ослаблення монопольних позицій держави в телекомунікаціях і неослабний інтерес до використання Інтернету призводять тільки до збільшення попиту на швидкість передачі.

У багатьох випадках завдяки застосуванню сучасних цифрових технологій пропускна здатність лінії зв'язку може бути збільшена в сотні разів.

Вражаюче зростання пропускної здатності досягається при збільшенні швидкості передачі даних в кожному каналі.

Перехід до широкосмугових сигналів при побудові систем зв'язку різного призначення йде по шляху впровадження цифрових методів передачі інформації.

Це пояснюється в основному гарною електромагнітною сумісністю таких сигналів, що в умовах постійного зростання потреби в послугах зв'язку і жорсткого обмеження частотного ресурсу призводить до необхідності їх більш ефективного використання.

Введення в таку систему кодів, контролюючих помилки дозволяє не тільки зменшити ймовірність появи помилок при передачі інформації, але і істотно знизити рівень інтерференційного шуму [7].

4.6. Аналіз нового стандарту WPA3

Версія протоколу WPA2 була введена в 2004 році і за останні кілька років неодноразово була дискредитована. З цієї причини в липні 2018 року Wi-Fi Alliance оголосив про початок сертифікації пристроїв, що підтримують WPA3 (Wi-Fi Protected Access 3) - найбільшого оновлення безпеки за останні 14 років.

У WPA2 завжди великою проблемою залишалося використання слабких паролів. Якщо користувачі ставлять легкий пароль на бездротову мережу, то його без зусиль можна було підібрати за допомогою автоматизованих атак з використанням словників, таких як Dictionary і Brute-Force.

Протокол WPA2 ніколи не пропонував варіантів для вирішення цієї проблеми. Від розробників були лише рекомендації використовувати складні і більш надійні паролі. У WPA3 будуть вжиті заходи, що дозволяють протидіяти таким атакам.

Для цього в WPA3 був реалізований новий механізм аутентифікації SAE (Simultaneous Authentication of Equals), який замінює використовуваний в WPA2 метод PSK (Pre-Shared Key).

Саме в PSK описано чотириступінчастою рукоштовування для встановлення зв'язку. Цей метод був скомпрометований KRACK-атакою, яка перериває серію рукоштовувань і намагається повторити запит на підключення. Неодноразова повторна відправка вітальних повідомлень змушує учасників мережі перевстановити узгоджений ключ. Коли жертва переустановлює ключ, асоційовані з ним параметри скидаються, що порушує безпеку, яку повинен гарантувати WPA2.

Таким чином, зловмисник отримує можливість прослуховувати трафік і впроваджувати свої пакети.

SAE перекладається як «одночасна аутентифікація рівних», згідно з цим алгоритмом аутентифікація пристроїв проводиться одночасно і на рівних правах.

Розробники відмовилися від суворої послідовності дій при авторизації і пішли від того, щоб вважати точку доступу головним пристроєм в мережі при авторизації.

Згідно з механізмом SAE, всі пристрої в мережі (точки доступу і абонентські пристрої) працюють на рівних правах. Тому будь-який пристрій може почати відправляти запити на аутентифікацію і в довільному порядку відправляти інформацію по встановленню ключів.

В результаті чого, можливість реалізації KRACK-атаки була усунена. З появою SAE у зловмисника принципово не буде можливості перервати процес аутентифікації, несанкціоновано підключаючись між точкою доступу і абонентським пристроєм.

Незважаючи на те, що новий стандарт WPA3 ще не введений в експлуатацію, недоліки безпеки в цьому протоколі дозволяють зловмисникам зламати пароль Wi-Fi. Протокол Wi-Fi Protected Access III (WPA3) був запущений з метою усунути технічні недоліки протоколу WPA2, який довгий час вважався небезпечним і вразливим [5].

Хоча WPA3 спирається на більш безпечне «рукопостискання», відоме як Dragonfly, яке спрямоване на захист мереж Wi-Fi від автономних атак за словником (офлайн-перебір), фахівці виявили слабкі місця в ранній реалізації WPA3-Personal, які можуть дозволити зловмиснику відновити Wi-Fi-паролі.

Алгоритм кодування паролю в «Dragonfly», також відомий як алгоритм «полювання і кльову» (hunting and pecking), містить умовні гілки. Якщо зловмисник може визначити, яка галузь гілки була обрана, він може дізнатися, чи був знайдений елемент пароля в конкретній ітерації цього алгоритму.

На практиці було виявлено, що якщо зловмисник може запустити непривілейований код на комп'ютері-жертви, можливо використовувати атаки на основі кешу, щоб визначити, яка гілка була зроблена в першій ітерації алгоритму генерації пароля.

Інформація може бути використана для виконання атаки з поділом пароля (схоже на автономну атаку по словнику).

Захист мережі в такому випадку полягає в заміні умовних гілок, які залежать від секретних значень, утилітами вибору з постійним часом.

Перехідний режим вразливий для атак з пониженням рейтингу, які злоумисники можуть використовувати для створення шахрайської точки доступу, що підтримує тільки WPA2, що змушує пристрої, які підтримують WPA3, підключатися за допомогою небезпечного чотиристороннього «рукоштовування» WPA2 [6].

Переваги WPA3-Personal:

- Користувачі можуть вибрати паролі, які легко запам'ятати, не замислюючись про безпеку;
- Нові алгоритм SAE забезпечує поліпшену захист за рахунок зміни алгоритму авторизації;
- Шифрування дани Forward Secrecy, захищає трафік даних, навіть якщо пароль був скомпрометований;

Корпоративні мережі частіше використовують Enterprise-протокол безпеки. WPA3-Enterprise також буде покращено за рахунок посилення ключа шифрування з 128 до 192 біт. Розробники вважають таку довжину ключа надлишковою для більшості мереж, однак, його буде більш ніж достатньо для цінної інформації.

При цьому WPA3 зберігає зворотну сумісність з пристроями, що використовують WPA2 [7].

WPA3-Enterprise, версія WPA3, призначена для роботи в урядових та фінансових установах, а також в корпоративному середовищі, володіє шифруванням в 192 біта.

Такий рівень шифрування для домашнього маршрутизатора буде надлишковим, але його має сенс використовувати в мережах, що працюють з особливо критичною інформацією.

Зараз Wi-Fi працює з безпекою в 128 біт. Безпека в 192 біта не буде обов'язковою до використання - це буде варіант налаштувань для тих організацій, мереж яких вона буде потрібна.

Wi-Fi Alliance також підкреслює, що в промислових мережах необхідно посилювати безпеку по всіх фронтах: стійкість системи визначається стійкістю найслабшої ланки.

Щоб гарантувати належний рівень безпеки всієї мережі, від початку до кінця, WPA3-Enterprise буде використовувати 256-бітний протокол Galois / Counter Mode для шифрування, 384-бітний Hashed Message Authentication Mode режим для створення і підтвердження ключів, і алгоритми Elliptic Curve Diffie-Hellman exchange, Elliptic Curve Digital Signature Algorithm для аутентифікації ключів.

У них багато складної математики, але плюс в тому, що на кожному кроці буде підтримуватися шифрування в 192 біта.

Easy Connect - це визнання наявності в світі величезної кількості пристроїв, приєднаних до мережі. І хоча, можливо, не всі люди захочуть користуватись розумними будинками, у середньої людини до домашнього маршрутизатора сьогодні, швидше за все, підключено більше пристроїв, ніж в 2004 році.

Easy Connect - спроба Wi-Fi Alliance зробити під'єднання всіх цих пристроїв більш інтуїтивним.

Замість того, щоб кожен раз при додаванні пристрою вводити пароль, у пристроїв будуть унікальні QR-коди - і кожен код пристрою буде працювати як публічний ключ. Для додавання пристрою можна буде просканувати код за допомогою смартфона, вже з'єднаного з мережею.

Після сканування пристрій обмінюється з мережею ключами аутентифікації для встановлення подальшої зв'язку. Протокол Easy Connect не пов'язаний з WPA3 - пристрої, сертифіковані для нього, повинні мати сертифікат для WPA2, але не обов'язково сертифікат для WPA3.

Enhanced Open - ще один окремий протокол, розроблений для захисту користувача у відкритій мережі.

Відкриті мережі - такі, якими ви користуєтесь в кафе або аеропорту - несуть в собі цілий комплекс проблем, які зазвичай не стосуються вас, коли ви встановлюєте з'єднання будинку або на роботі.

Багато атак, що відбуваються у відкритій мережі, відносяться до пасивних. Коли до мережі підключається купа людей, атакуючий може зібрати дуже багато даних, просто фільтруючи інформацію, яка є в доступі.

Enhanced Open використовує опортуністична бездротове шифрування (Opportunistic Wireless Encryption, OWE), певний в стандарті Internet Engineering Task Force RFC 8110, щоб захищатися від пасивного підслуховування.

Для OWE не потрібна додатковий захист з аутентифікації, оскільки воно концентрується на поліпшенні шифрування даних, що передається по публічних мережах, з метою запобігти їх крадіжку.

Воно також запобігає просту ін'єкцію пакетів, в якій атакуючий намагається порушити роботу мережі, створюючи і передаючи особливі пакети даних, що виглядають, як частина нормальної роботи мережі.

Enhanced Open не дає захисту з аутентифікацією через особливості організації відкритих мереж - вони за визначенням призначені для загального використання.

Enhanced Open був розроблений для поліпшення захисту відкритих мереж проти пасивних атак, так, щоб не вимагати від користувачів введення додаткових паролів або проходження додаткових кроків.

Пройде, щонайменше, кілька років, до того, як WPA3, Easy Connect і Enhanced Open стануть нормою.

Широке поширення WPA3 відбудеться тільки після заміни або поновлення маршрутизаторів.

Однак якщо Вас турбує безпека вашої особистої мережі, ви зможете замінити свій поточний маршрутизатор на інший, що підтримує WPA3, як тільки виробники почнуть продавати їх, що може статися найблищим часом [11].

Перехід на WPA3 почався в 2018 році, коли Міжнародна асоціація виробників бездротового обладнання (Wi-Fi Alliance) затвердила специфікацію стандарту. Очікується, що він підвищить безпеку WiFi-інфраструктур і зробить їх зручніше - наприклад, відкриє користувачам підключення до мережі по QR-коду. На даний момент розробники забезпечують своїх пристроїв паралельну підтримку WPA2 і WPA3.

Нарешті, виявлена технологія DoS-атаки побудована на створенні великої кількості повідомлень про «рукоостискання» з точкою доступу WPA3.

Хоча розробники стандарту передбачили спеціальний механізм для захисту від подібних перевантажень, фахівці змогли його обійти.

Протокол Dragonfly використовується в рішенні EAP-PWD, тому описані вразливості актуальні і для нього. За відсутності захисних патчів експерти не стали публікувати технічні подробиці по цій темі.

Адміністратори можуть перевірити вразливість своїх EAP-мереж за допомогою утиліт, які опубліковані на сайті дослідників.

За словами представників Wi-Fi Alliance, злочинці поки не встигли скористатися проломи, а всі виявлені вразливості можна виправити програмними патчами. Виробники обладнання вже почали оновлення своїх продуктів.

У свою чергу, самі дослідники вказали, що проблем можна було уникнути, якби розробники WPA3 зробили цей процес більш відкритим. Незважаючи на всі описані проблеми, експерти все одно вважають новий стандарт набагато більш захищеним, ніж WPA2 [12].

Раніше в Wi-Fi Alliance стверджували, що після публікації оновлень безпеки використання кривих Брейпула була відновлена. Рішення включало в себе виконання тесту квадратичного залишку Dragonfly без будь-яких витоків в бічних каналах.

Однак дослідники Метті Ванхоеф і Еяль Ронен заявили, що використання кривих Брейпула несе в собі загрозу іншого класу в бічних каналах при рукоостисканні Dragonfly в стандарті WPA3.

У сухому залишку це означає, що, незважаючи на всі запевнення, вразливість існує, як і раніше, дозволяючи зловмисникам викрадати паролі Wi-Fi, ставлячи під загрозу конфіденційність переданої інформації.

Дві нові уразливості отримали назви CVE-2019-13377 і CVE-2019-13456.

Вразливість CVE-2019-13377 проявляється при рукоостисканні Dragonfly в стандарті WPA3 з використанням кривих Брейпула.

Це спосіб авторизації користувачів WPA3-сумісних маршрутизаторів і точок доступу.

Незважаючи на те, що в даний час рекомендують виробникам обладнання використовувати криві P-521, зломисники, скориставшись новою вразливістю, можуть знизити цю функцію до слабшої - P-256.

Друга вразливість Dragonblood пов'язана з функцією EAP-pwd, яка є системою авторизації для стандартів WPA і WPA2.

Функцію EAP-pwd можна використовувати також в маршрутизаторах WPA3, де вона присутня з метою забезпечення підтримки роботи старіших версій.

Дослідники в черговий раз продемонстрували своє невдоволення принципами, на підставі яких Wi-Fi Alliance випускає свої оновлення.

Замість використання відкритих стандартів, що дають можливість експертам з безпеки вносити свій внесок у зміцнення безпеки, розробники покладаються на закриті стандарти.

Тому після виявлення уразливості до випуску необхідного оновлення проходить чималий термін, що дає зломисникам масу часу для планування чергових нових атак [13].

У світлі виявлення згаданих вище вразливостей Dragonblood, Wi-Fi Alliance в даний час проводить оновлення системи захисту стандарту Wi-Fi.

Таким чином, оскільки повне впровадження WPA3 та допрацювання на сумісність з існуючим обладнанням потребує ще значного проміжку часу, тому розроблений спосіб генерування паролів можна вважати актуальним, а в ході цілковитого впровадження WPA3 оптимізувати запропонований спосіб під новий тип захисту та додатково вивчити нові види атак.

Висновки до четвертого розділу

Таким чином, за результатами четвертого розділу можливо зробити такі висновки:

по-перше, спосіб генерування ускладнених паролів в системах бездротового зв'язку з введенням змінного правила дозволяє зменшити витрати часу на створення паролю приблизно на 20%;

по-друге, для ускладненого паролю, що створений за вдосконаленим способом, отримано значне зниження ймовірності підбору паролю, оскільки на підбір потрібно у $3,73 \cdot 10^4$ разів більше часу, ніж для випадкової комбінації з 63 символів ASCII, або в $3,50 \cdot 10^{15}$ разів більше ніж для випадкового паролю з 8 символів;

по-третє, спосіб генерування ускладнених паролів може використовуватись не тільки як частина паролівних політик, а і як додаткова складова для програмних та апаратних засобів захисту, облікових записів користувачів, а також в інших системах захисту інформації, де необхідне використання стійкого до підбору паролю.

Тим не менш використання зловмисниками комплексного підходу для спроб несанкціонованого доступу до систем бездротового зв'язку (шляхом об'єднання соціальної інженерії та перехоплення даних з використанням зловмисного програмного забезпечення), а також нових видів кібератак, що дозволяють приховано встановлювати шкідливе ПЗ на мобільні пристрої може сприяти зниженню ефективності існуючих методів та засобів захисту бездротових мереж.

Враховуючи статистику та проведені в роботі розрахунки, можна стверджувати, що впровадження способу генерування ускладнених паролів дозволить суттєво підвищити рівень захищеності бездротових мереж.

Список використаних джерел у четвертому розділі

1. Бурячок В.Л. Генерування пароллю для бездротових мереж з використанням змінного правила ускладнення/ В.Л. Бурячок, А. О. Аносов, **А.В Платоненко**. // Захист інформації. – 2019. – Том 21, №1. – С. 52–59.
2. Одияненко Е. В. Синтез оптимальной структуры системы защиты информации / Е. В. Одияненко, Г. Н. Розоринов, **А. В. Платоненко**. // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Часть I. – 2014. – С. 443–445.
3. Розорінов Г. М. Захист інформаційних систем від потужних електромагнітних випромінювань / Г. М. Розорінов, **А. В. Платоненко**. // Сучасний захист інформації. – 2014. – №3. – С. 16–20.
4. Odiyanenko H. V. Evaluation of parameters and compensation of noises in protected telecommunication systems / H. V. Odiyanenko, G. N. Rozorynov, **A. V. Platonenko**. // Научно-практический журнал Западно-Казахстанского аграрно-технического университета имени Жангир хана "Наука и образование". – 2014. – С. 91–94.
5. Розоринов Г. Н. Пассивная оптическая сеть с кодовым разделением каналов / Г. Н. Розоринов, **А. В. Платоненко**. // Телекомунікаційні та інформаційні технології. – 2014. – №4. – С. 20–26.
6. WPA3 – Крупнейшее обновление безопасности Wi-Fi за последние 14 лет. URL:<https://nag.ru/articles/article/102617/wpa3-krupneyshee-obnovlenie-bezopasnosti-wi-fi-za-poslednie-14-let.html> (дата звернення: 12.06.2019).
7. Взлом WPA3_ DragonBlood_Блог компании Инфосистемы Джет. URL: <https://habr.com/ru/company/jetinfosystems/blog/447628/> (дата звернення: 15.06.2019).
8. Wi-Fi становится безопаснее_ всё, что вам нужно знать про WPA3. URL: <https://habr.com/ru/post/424925/> (дата звернення: 18.06.2019).
9. Эксперты взломали пароли WiFi-сетей на основе WPA3. URL: <https://threatpost.ru/wpa3-vulnerabilities-allow-to-crack-wifi-paaswords/32257/> (дата звернення: 10.07.2019).

10. В стандарте WPA3 Wi-Fi выявлены ещё две уязвимости типа Dragonblood. URL: <http://mediasat.info/2019/08/06/dragonblood-wifi-wpa3-2/> (дата звернення: 10.09.2019).

11. Opirsky Ivan. Use of near field communication technology for automated profile replication/ Opirsky Ivan, Ivanchenko Ihor, **Platonenko Artem**, Skladannyi Pavlo, Roshchuk Mariia. // Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, Bielsko-Biala, Poland

12. **Платоненко А.В.** Захист інформації у безпроводових мережах WI-FI./ Платоненко А.В. // Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави» – Київ: ДУТ, 2014 – С.40-41.

13. **Платоненко А.В.** Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах. / Платоненко А.В. // Науково-технічна конференція «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.34-35.

14. **Платоненко А. В.** Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко. // Сучасний захист інформації. – 2015. – №4. – С. 86–90.

15. **Платоненко А. В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту / А. В. Платоненко. // Сучасний захист інформації. – 2017. – №1. – С. 128–132.

ВИСНОВКИ

У дисертації вирішено актуальне **наукове завдання**, що полягає в *створенні технології забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик*, яка за рахунок впровадження оцінки ступеня близькості між базовим способом генерування паролів і кожним способом-аналогом та урахування можливості співпадіння з паролями системи словників, а також використання інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів (обраних за правилом комбінації з введенням певного ускладнення) *дозволяє*:

- обрати серед множини існуючих способів генерування паролів спосіб, найбільш раціональний з точки зору його вдосконалення та забезпечити функціональну безпеку систем бездротового зв'язку в умовах впливу кібернетичних атак;
- підвищити рівень захищеності систем бездротового зв'язку стандарту IEEE 802.11 від можливого злому (спроб несанкціонованого доступу) в $3,73 \cdot 10^4$ разів;
- зменшити витрати часу на створення паролю приблизно на 20%.

З цією метою в роботі, як результат:

1) проведено аналіз множини актуальних загроз та уразливостей системам бездротового зв'язку, а також варіанти формування та застосування парольних політик для забезпечення функціональної безпеки таких систем в умовах кібернетичних атак;

2) вперше розроблений метод обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку для забезпечення їх надійності і живучості в умовах кібернетичних атак, за рахунок вибору раціонального способу генерування паролів серед множини існуючих;

3) удосконалений спосіб генерування випадкових паролів для систем бездротового зв'язку, за показниками довжини та набору символів, з метою формування більш стійких до підбору паролів;

4) досліджено стан можливого злому (спроб несанкціонованого доступу) на прикладі систем бездротового зв'язку стандарту IEEE 802.11.

Перспективним напрямком подальших досліджень є підтримка в актуальному стані бази словників паролів для впровадження аналізу та подальша повна автоматизація запропонованого способу.

Таким чином, поставлене актуальне наукове завдання розв'язане у повному обсязі. Усі визначені часткові завдання вирішено, мету досліджень досягнуто.

ДОДАТКИ

Додаток А. Акти впровадження

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА

Вул. Бульварно-Кудрявська, 18/2, м. Київ,
Україна, 04053, тел./факс: +380 44 272-19-02
e-mail: kubg@kubg.edu.ua, www.kubg.edu.ua



BORYS GRINCHENKO
KYIV UNIVERSITY

18/2 Bulvarno-Kudriavska St., Kyiv,
Ukraine, 04053, tel./fax: +380 44 272-19-02
e-mail: kubg@kubg.edu.ua, www.kubg.edu.ua

15.04.2019 № 20/1-11

На № _____ від _____

АКТ

про впровадження результатів дисертаційного дослідження
Платоненка Артема Вадимовича

Цим Актом, ґрунтуючись на рішенні кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка (протокол №7 від 06 березня 2019 року) засвідчуємо, що *нижчеперелічені наукові положення, а саме:*

а) метод обґрунтування рішення на вдосконалення паролівних політик в системах бездротового зв'язку;

б) спосіб генерування випадкових паролів для систем бездротового зв'язку, – *розроблені особисто Платоненком Артемом Вадимовичем* в ході проведення ним дисертаційних досліджень за темою «Технологія забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення паролівних політик» та *отримали високу оцінку* при обговоренні на засіданнях кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка, а також за результатами озвучення відповідних доповідей в процесі роботи вітчизняних і міжнародних наукових конференцій та семінарів.

Зазначені наукові результати:

по-перше, впроваджені в освітній процес Київського університету імені Бориса Грінченка в навчальних і робочих програмах дисциплін «Основи ОС та сучасних інтернет-технологій» та «Прикладні аспекти аналізу та синтезу політик безпеки» першого (бакалаврського) рівня вищої освіти;

по-друге, впроваджені в програмно-апаратне забезпечення «Центру дослідження технологій захисту інформаційних активів» Київського університету імені Бориса Грінченка при розгортанні «Лабораторії безпеки інформаційних активів» (навчальний кіберполігон).

Це дозволило зменшити витрати часу на створення паролю приблизно на 20%, а також зменшити ймовірність злому шляхом збільшення часу для можливого підбору в $3,73 \cdot 10^4$ разів, та ґрунтуючись на нових аналітично-програмних рішеннях, суттєво підвищити якість підготовки фахівців із кібербезпеки за спеціалізацією «Безпека інформаційно-комунікаційних систем».

Акт видано для подання до спеціалізованої вченої ради.

Проректор з наукової роботи,
доктор філологічних наук, доцент



Н. М. Віннікова



З. П. БІКБУЛАТОВ
Директор
ТОВ "ІТТК "Технології безпеки"
Бікбулатов С. Ю.
20 березня 2019 р.

АКТ

Про впровадження результатів дисертаційного дослідження Платоненка Артема Вадимовича

Комісія у складі:

голови комісії Бікбулатова С. Ю.,

членів комісії:

Левченко С. М.

фахівця з технічного захисту інформації,

Бойко О. В.

фахівця з технічного захисту інформації,

встановила, що результати наукових досліджень Платоненко А.В., отримані ним в рамках дисертаційної роботи, зокрема таких наукових положень, як:

а) метод обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, який дозволяє серед множини існуючих способів генерування паролів обрати спосіб, найбільш раціональний з точки зору його вдосконалення;

б) спосіб генерування випадкових паролів для систем бездротового зв'язку, який завдяки урахуванню можливості співпадіння з паролями системи словників та використанню інтегрованого підходу, забезпечує підвищення рівня захищеності систем бездротового зв'язку стандарту IEEE 802.11 від можливого злому;

використані в роботі фахівцями Товариство з обмеженою відповідальністю "Науково-технічна компанія "Технології безпеки".

Застосування зазначених наукових досліджень дає можливість створювати актуальну базу надійних паролів, що в подальшому можуть використовуватись для проектування захищених бездротових мереж, для зменшення ймовірності їх можливого підбору.

Голова комісії, Бікбулатов С. Ю.

Члени комісії:

Левченко С. М.

Бойко О. В.

ТОВ «КВАДРОКОПТЕР»

Юридична адреса: 03164, м. Київ: ВУЛИЦЯ КЛАВДІЙСЬКА, БУДИНОК 16

код ЄДРПОУ 34645286

Банк: ПАТ КБ ПРИВАТБАНК р/р: 26000052648509, МФО 320649

Тел./факс: +380674745290

Електронна адреса: info@quadro.ua



ЗАТВЕРДЖУЮ

Директор ТОВ «Квадрокоптер»

О.І. Горбач

19 квітня 2019 р.

АКТ

Про впровадження результатів дисертаційного дослідження

Платоненка Артема Вадимовича

Комісія у складі:

голови - директора Горбача О.І. та членів комісії - начальника технічного відділу Куликовського О.С, та інженера Семенюти О.О. склали цей акт про те, що результати наукових досліджень спрямованих на розробку технології забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик корпоративних користувачів:

- а) методу обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку;
- б) способу генерування випадкових паролів для систем бездротового зв'язку;

особисто отримані Платоненко А.В. та реалізовані при проектуванні та розробці елементів парольної політики корпоративних користувачів бездротової мережі ТОВ «Квадрокоптер», а також застосовані у налаштуваннях безпеки моделей, що використовують бездротові системи типу Wi-Fi для підключення, а саме:

- DJI Phantom 3 Standart,
- DJI Spark,
- DJI Mavic AIR
- DJI Osmo.

Голова комісії: О. І. Горбач

Члени комісії: О. С. Куликовський

О. О. Семенюта

Додаток Б. Список опублікованих праць за темою дисертації

Колективна монографія в іноземному науковому виданні:

1. Opirskyy Ivan. Use of near field communication technology for automated profile replication/ Opirskyy Ivan, Ivanchenko Ihor, **Platonenko Artem**, Skladannyi Pavlo, Roshchuk Mariia. // Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, Bielsko-Biala, Poland.

Статті в іноземних наукових виданнях:

2. Odiyanenko H. V. Evaluation of parameters and compensation of noises in protected telecommunication systems / H. V. Odiyanenko, G. N. Rozorynov, **A. V. Platonenko**. // Научно-практический журнал Западно-Казахстанского аграрно-технического университета имени Жангир хана "Наука и образование". – 2014. – С. 91–94.

3. Одияненко Е. В. Синтез оптимальной структуры системы защиты информации / Е. В. Одияненко, Г. Н. Розоринов, **А. В. Платоненко**. // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Часть I. – 2014. – С. 443–445.

Статті у наукових фахових виданнях України:

4. Розорінов Г. М. Захист інформаційних систем від потужних електромагнітних випромінювань / Г. М. Розорінов, **А. В. Платоненко**. // Сучасний захист інформації. – 2014. – №3. – С. 16–20.

5. Розоринов Г. Н. Пассивная оптическая сеть с кодовым разделением каналов / Г. Н. Розоринов, **А. В. Платоненко**. // Телекомунікаційні та інформаційні технології. – 2014. – №4. – С. 20–26.

6. **Платоненко А. В.** Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко. // Сучасний захист інформації. – 2015. – №4. – С. 86–90.

7. Аносов А. О. Модель перехоплення та захист інформації в бездротових мережах / А. О. Аносов, **А. В. Платоненко**. // Сучасний захист інформації. – 2017. – №2. – С. 90–94.

8. **Платоненко А. В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту / А. В. Платоненко. // Сучасний захист інформації. – 2017. – №1. – С. 128–132.

9. Аносов А. О. Генерування унікального паролю зі змінним правилом ускладнення / А. О. Аносов, **А. В. Платоненко**. // Сучасний захист інформації. – 2017. – №3. – С. 82–86.

10. Бурячок В.Л. Генерування паролю для бездротових мереж з використанням змінного правила ускладнення/ В.Л. Бурячок, А. О. Аносов, **А.В Платоненко**. // Захист інформації. – 2019. – Том 21, №1. – С. 52–59.

11. Бурячок В.Л. Вибір раціонального способу генерування паролів серед множини існуючих / В.Л. Бурячок, **А.В Платоненко**, О.В. Семко. // Безпека інформації. – 2019. – Том 25, № 1. – С. 59–64.

Публікації у наукометричних базах Scopus i Web of Science:

12. Vladymyrenko Maksym. Analysis of implementation results of the distributed access control system. / Maksym Vladymyrenko, Sokolov Volodymyr, Buriachok Volodymyr, **Platonenko Artem**. // Preprint. PIC S&T`2019 IEEE conference, Kyiv.

Тези наукових доповідей:

13. **Платоненко А.В.** Захист інформації у безпроводових мережах WI-FI./ Платоненко А.В. // Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави» – Київ: ДУТ, 2014 – С.40-41.

14. **Платоненко А.В.** Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах. / Платоненко А.В. // Науково-технічна конференція «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.34-35.

15. **Платоненко А.В.** Сучасні загрози інформаційної безпеки для пристроїв у корпоративних мережах. Матеріали Міжнародної науково-технічної конференції «Актуальні проблеми розвитку науки і техніки» – Київ: ДУТ, 2015 – С.128.

16. **Платоненко А.В.** Сучасні загрози інформаційної безпеки для державних та приватних установ України. / Платоненко А.В. // II Міжнародна науково-технічна конференція «Актуальні проблеми розвитку науки і техніки» – Київ: ДУТ, 2015 – С.137-138.

17. **Платоненко А.В.** Сучасні загрози інформаційної безпеки та засоби захисту від них. / Платоненко А.В. // Міжнародна науково-технічна конференція студентства та молоді «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.159-160.

18. **Платоненко А.В.** Актуальні загрози інформаційної безпеки сучасних мобільних пристроїв у мережах нового покоління. / Платоненко А.В. // II Міжнародна науково-практична конференція «Тенденції розвитку конвергентних мереж: рішення пост - NGN, 4G та 5G» – Київ: ДУТ, 2016 – С.182-183.

19. **Платоненко А.В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв в Україні. / Платоненко А.В. // III Міжнародна науково-технічна конференція студентства та молоді» – Київ: ДУТ, 2016 – С.134-136.

20. **Платоненко А.В.** Средства защиты современных мобильных устройств в сетях нового поколения / А. В. Платоненко, А. А. Аносов. // Региональная конференция «Перспективы предоставления услуг на основе сетей пост-NGN, 4G и 5G. Организационные и технические решения по их построению и защите» – Київ: ДУТ, 2017.

Додаток В. Відомості про апробацію результатів дисертації

№ п/п	Назва заходу (конференції, симпозіуму, семінару, круглого стола)	Місце проведення	Дата проведення	Форма участі
1.	Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави»	м. Київ	грудень 2014	Очна
2.	Студентська науково-технічна конференція молодих вчених присвячена Дню науки «Світ телекомунікації та інформатизації»	м. Київ	травень 2015	Очна
3.	Міжнародна науково-технічна конференція «Актуальні проблеми розвитку науки і техніки»	м. Київ	жовтень 2015	Очна
4.	Міжнародна науково-технічна конференція «Сучасні інформаційно-телекомунікаційні технології»	м. Київ	листопад 2015	Очна
5.	Міжнародна науково-технічна конференція студентства та молоді «Світ телекомунікації та інформатизації»	м. Київ	грудень 2015	Очна
6.	II Міжнародна науково-практична конференція «Тенденції розвитку конвергентних мереж: рішення пост - NGN, 4G та 5G»	м. Київ	листопад 2016	Очна
7.	III Міжнародна науково-технічна конференція студентства та молоді»	м. Київ	грудень 2016	Очна
8.	Міжнародна конференція «Перспективы предоставления услуг на основе сетей пост-NGN, 4G и 5G. Организационные и технические решения по их построению и защите»	м. Київ	червень 2017	Очна
9.	PIC S&T`2019 IEEE conference	м. Київ	жовтень 2019	Очна