Прим. № ___

Голові спеціалізованої вченої ради
Д 26.255.01
03186, м. Київ, бул. Чоколівський, 13

ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА

начальника кафедри бойового застосування та експлуатації АСУ Харківського національного університету Повітряних Сил імені Івана Кожедуба, доктора технічних наук, професора Баранніка Володимира Вікторовича

на дисертаційну роботу Платоненка Артема Вадимовича за темою «Технологія забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології

1. Актуальність теми

Серед сучасних засобів телекомунікацій найбільш стрімко розвиваються мережі мобільного зв'язку, а мобільні пристрої стали невід'ємною частиною нашого життя. На сьогоднішній день неможливо собі уявити людину у сучасному світі без мобільного телефону. Окрім зручності та багатьох технічних можливостей, нажаль, вони несуть за собою 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, що в свою чергу збільшує ризики несанкціонованого доступу до мережі компанії. 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.

Вирішенню саме зазначених задач й присвячена дисертаційна робота Платоненка Артема Вадимовича який, враховуючи множини існуючих актуальних загроз та уразливостей для систем бездротового зв'язку стандарту IEEE 802.11, а також варіантів формування та застосування парольних політик для забезпечення функціональної безпеки таких систем в умовах кібернетичних атак, розв'язує **актуальну науково-прикладну проблему** щодо формування парольних політик, що дозволяє раціонально обрати спосіб генерування паролів серед множини існуючих та генерування ускладнених паролів в системах бездротового зв'язку, що дозволяє сформувати стійкий до підбору пароль.

2. Аналіз основного змісту, наукової новизни та практичної значимості, оцінка достовірності та обґрунтованості результатів

Дисертація складається зі вступу, чотирьох розділів, висновків, трьох додатків та списку використаних джерел, що містить 95 найменувань. Загальний обсяг дисертації становить 138 аркушів, з яких основний текст розкрито на 120 аркушах.

Зміст роботи відповідає поставленій науково-технічній проблемі та сформульованим задачам. Їх рішення є суттю та змістом виконаних досліджень, які відповідають п. 14 паспорту спеціальності 05.13.06 – «Інформаційні технології» та направлені на дослідження моделей і методів оцінювання якості і підвищення надійності функціональної безпеки і живучості інформаційних та інформаційно-управляючих систем.

При цьому у ***вступі*** автором обґрунтовано актуальність теми, сформульовано мету і завдання досліджень, визначено наукову новизну та практичне значення роботи, наведено відомості про публікації, апробацію та впровадження результатів роботи.

У ***першому розділі*** автором 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, а також сформовано загальну модель перехоплення та захисту інформації в бездротових мережах.

У ***другому розділі*** автором 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.

У ***третьому розділі*** автором розроблено процедуру вдосконалення обраного в другому розділі способу генерування випадкових паролів, який складається з чотирьох етапів та завдяки використанню інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів дозволяє створити пароль, ймовірність підбору якого буде мінімальною та збільшити кількість варіантів правила ускладнення, та кількість можливих комбінацій підбору, а також рівень невизначеності для зловмисника.

У ***четвертому розділі*** автором присвячено дослідженню вдосконаленого способу генерування ускладнених паролів, а також формуванню рекомендацій щодо його застосування на базі існуючих засобів захисту систем бездротового зв'язку стандарту IEEE 802.11. 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 розроблений спосіб.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації, переконливо окреслена використанням сучасних методів математичного та технічного моделювання процесів у сучасних інформаційних системах для яких є принциповими питання забезпечення цілісності та доступності інформації. Підґрунтям цього є застосування у дисертації основних положень теорії множин, теорії ймовірностей і математичної статистики, експертного оцінювання, математичного моделювання, графічного методу, а також порівняння та формалізації.

Отримані автором наукові результати у відповідності до поставлених задач досліджень є логічними, не суперечать фундаментальним математичним закономірностям та підтверджуються достатньою апробацією основних положень і висновків як на міжнародних, так і всеукраїнських науково-технічних конференціях та семінарах.

Достовірність отриманих в роботі положень і наукових результатів підтверджується результатами проведених досліджень, коректністю застосування математичного апарату, можливих припущень та формулюванням умов досліджень при моделюванні процесів, які відбуваються при формуванні словників паролів та їх підборі, що підтверджено малими значеннями розбіжностей між результатами математичного та технічного моделювання.

Додатково достовірність отриманих результатів підтверджується проведенням досліджень на технічний базі та впровадженням у навчальний процес Київського університету імені Бориса Грінченка та в практику розроблення політик інформаційної безпеки двох приватних організацій, що підтверджено відповідними актами впровадження.

Новими результатами, що отримані здобувачем в дисертації є:

1) *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;

2) 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.

Впровадження отриманих результатів забезпечило:

- зменшення: витрат часу на створення паролю приблизно на 20%,
- зменшення ймовірності злому паролю шляхом збільшення часу для його можливого підбору в $3{,}73 \cdot 10^4$ разів.

Практичне значення одержаних автором наукових результатів.

Як показав аналіз, дисертаційна робота відповідає основним положенням Закону України «Про Концепцію Національної програми інформатизації» від 04 лютого 1998 р., № 75/98-ВР, «Концепції розвитку зв'язку України» від 09 грудня 1999 р. № 2238 та спрямона на досягнення мети і завдань розділу 3, 4 та 6 «Концепції розвитку телекомунікацій в Україні», схваленої розпорядженням КМ України від 7 червня 2006 року, п. 1.2.5.4, 1.2.7.1 та п. 1.2.8.1 «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009-2013 р.р.», які визначені постановою Президії НАН України від 25.02.2009 р., №55. Доцільність виконаних наукових досліджень підтверджуються Розпорядженням Кабінету Міністрів України від 5 листопада 2014 року № 1135-р «Про затвердження плану заходів щодо захисту державних інформаційних ресурсів».

Теоретична цінність отриманих результатів полягає в тому, що автором отримано результати, які сприяють подальшому розвитку теоретичних і методологічних основ створення методів генерування паролів, які можуть задаватися як проектні вимоги при створенні політик інформаційної безпеки, й забезпечити, як наслідок, збереження, цілісності та доступності державних та приватних інформаційних ресурсів.

Наукова і практична цінність отриманих результатів полягає у тому, що формування парольних політик дозволяє раціонально обрати спосіб генерування паролів серед множини існуючих, а спосіб генерування ускладнених паролів в системах бездротового зв'язку дозволяє сформувати стійкий до підбору пароль. Запропонований спосіб генерування ускладнених паролів може використовуватись не тільки як частина парольних 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.

Оцінка мови та стилю викладання дисертації та автореферату. Дисертація та автореферат написані грамотно, а стиль викладення в них матеріалів досліджень, наукових положень, висновків і рекомендацій відповідає вимогам стандарту ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки» й у цілому забезпечує доступність їх сприйняття.

Зміст автореферату відображає основні результати роботи, які приведені в дисертації.

Дисертація по тематиці і результатам відповідає паспорту спеціальності 05.13.06 – інформаційні технології.

Повнота викладення наукових результатів дисертації в опублікованих роботах. Основні результати дисертаційного дослідження опубліковано у 20 наукових працях. Серед них: 1 – монографія, 3 – статті у зарубіжних виданнях; 8 – статті у фахових наукових виданнях, 8 – тези у матеріалах наукових конференцій. Серед зазначених праць 9 опубліковано у виданнях, які входять до наукометричних баз та індексуються у МНБД SCOPUS, Index Copernicus, Google Scholar та РІНЦ.

Недоліки дисертаційної роботи.

1) у першому розділі не всі аналітичні дані відносяться до 2019 року, адже існує багато нових вразливостей та атак, які можуть значно вплинути на дослідження;

2) у другому розділі роботи не зрозуміло чому не було порівняння з рівнем захисту WPA3. Не наведено математичної моделі для розрахунку часу, що необхідний для створення паролю згідно запропонованого способу, відповідно дуже складно оцінити та порівняти час, що необхідний для створення паролів завдяки способам-аналогам, які розглядаються в роботі;

3) у третьому розділі не чітко зрозуміло, що мається на увазі під множиною та підмножиною паролів;

4) у четвертому розділі не зрозуміло, як саме зберігати створений відповідно до запропонованого способу, стійкий до підбору пароль. Не повною мірою розкрито аспект створення програмного забезпечення, як основної складової для впровадження запропонованого способу генерування паролів;

5) як додаток до дисертаційної роботи здобувачеві доцільно було б привести варіанти реалізації розробленого способу на основі реальних систем бездротового зв'язку, що значно спростило б процес оцінювання результатів, отриманих у дисертації;

6) у тексті роботи та в авторефераті мають місце описки та інколи використовуються терміни і позначення без пояснень, які не є загальновідомими або загальноприйнятими.

Зазначені недоліки суттєво не впливають на загальне позитивне враження від роботи, не зменшують її якості, а також наукової та практичної цінності. Вони не є визначальними і можуть бути враховані як деякі напрямки подальших досліджень.

3. Відповідність дисертаційної роботи встановленим вимогам та загальний висновок

Дисертаційна робота Платоненка Артем Вадимовича за темою «Технологія забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик» є завершеною, одноосібно написаною кваліфікаційною науковою працею, що:

1) являє собою системне дослідження, проведене з певною метою;

2) має внутрішню єдність і свідчить про особистий внесок автора в науку;

3) розв'язує актуальну проблему, яка має важливу наукову і практичну спрямованість й результати вирішення якої істотно впливають на забезпечення відмовостійкості систем бездротового зв'язку за рахунок підвищення стійкості парольних політик до спроб несанкціонованого доступу.

За змістом, актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною значимістю одержаних результатів дисертаційна робота Платоненка А.В. відповідає паспорту спеціальності 05.13.06 – «Інформаційні технології», а також вимогам п.п. 9, 11, 12-14 Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 із змінами, внесеними згідно з Постановами Кабінету Міністрів України № 656 від 19.08.2015 р., № 1159 від 30.12.2015 р., а її автор Платоненко Артем Вадимович заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології.

Офіційний опонент
доктор технічних наук, професор,
начальник кафедри бойового застосування та експлуатації АСУ
Харківського національного університету Повітряних Сил імені Івана Кожедуба
полковник В. БАРАННІК

Підпис полковника БАРАННІКА В.В. засвідчую

ТВО начальника відділу персоналу та стройового –
заступника начальника штабу Харківського національного
університету Повітряних Сил імені Івана Кожедуба
підполковник О.ГОРОХОВСЬКИЙ