

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

**ВІДГУК
офіційного опонента**

професора кафедри інженерії програмного забезпечення
Національного авіаційного університету
доктора технічних наук, доцента Зибіна Сергія Вікторовича
на дисертаційну роботу Платоненка Артема Вадимовича за темою
«Технологія забезпечення функціональної безпеки систем бездротового зв'язку на
основі вдосконалення паролівних політик», подану на здобуття наукового ступеня
кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології

1. Актуальність теми дисертаційної роботи

Аналіз сучасних засобів телекомунікацій показує, що найбільш стрімко розвиваються мережі мобільного зв'язку, а мобільні пристрої вже стали звичкою у повсякденному житті. Дуже важно у теперішній час уявити собі людину в сучасному світі без мобільного телефону. Вони приносять нам зручність у спілкуванні та багато технічних можливостей, які щороку покращуються, але в той самий час являють собою небезпеку для інформації, яка в них зберігається та передається. Використання високошвидкісних мобільних мереж призводить до зростання кількості загроз інформаційної безпеки, як для державних так і для приватних установ, оскільки працівники використовують мобільні пристрої для віддаленої роботи, що в свою чергу збільшує ризики несанкціонованого доступу до мережі їх організації. Таким чином для зловмисників відкриваються значно ширші технічні можливості для здійснення атак, що потребує впровадження засобів захисту інформації.

Виходячи із зазначеного, питання щодо забезпечення функціональної безпеки систем бездротового зв'язку, які розглядаються в дисертації є важливими та актуальними.

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

Дисертація складається зі вступу, чотирьох розділів, висновків, 3 додатків та списку використаних джерел, що містить 95 найменувань. Загальний обсяг дисертації становить 138 аркушів, з яких основний зміст роботи розкрито на 120 сторінках. Зміст роботи відповідає поставленому науковому завданню та сформульованим задачам. Їх рішення являються суттю та змістом виконаних досліджень, які відповідають п. 14 паспорта спеціальності 05.13.06 – інформаційні технології й направлені на дослідження моделей і методів оцінювання якості і підвищення надійності функціональної безпеки і живучості інформаційних та інформаційно-управляючих систем.

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.

Перший розділ присвячено проведенню аналізу 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 паролівних 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.

Четвертий розділ 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.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконувалась у рамках науково-дослідної роботи «Розробка методів та заходів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак» (шифр «Захист ІКС», № д/р 0114U000391), а також результати дисертаційного дослідження впроваджені в освітній процес Київського університету імені Бориса Грінченка в дисциплінах «Основи ОС та сучасних інтернет-технологій» та «Прикладні аспекти аналізу та синтезу політик безпеки» першого (бакалаврського) рівня вищої освіти.

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 захисту інформації з використанням системного підходу до вирішення сучасних проблем бездротових мереж, використанням методів дослідження, які відповідають сутності наукової проблеми, що вирішується.

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

Достовірність отриманих в роботі положень і наукових результатів підтверджується результатами проведених досліджень, коректністю застосування

математичного апарату, можливих обмежень і припущень та формулюванням умов досліджень при обґрунтуванні раціонального вибору способу для ускладнення, а також раціонального розподілу правил ускладнення для вдосконаленого способу.

Додатково достовірність отриманих результатів підтверджується проведенням досліджень на технічній базі та впровадженням у навчальний процес Київського університету імені Бориса Грінченка та в практичну частину розроблення політик інформаційної безпеки двох приватних організацій, в яких автор приймав участь, що підтверджено відповідними актами впровадження.

Наукова новизна одержаних результатів полягає в розробленні методичного апарату для оцінювання та забезпечення обґрунтованості результатів багатокритеріальної оптимізації складних організаційно-технічних систем військового призначення, який і складає сутність розвитку сучасної методології багатокритеріальної оптимізації таких систем. У роботі автором *вперше одержано*:

- метод обґрунтування рішення та вдосконалення паролічних 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;

Окрім цього в роботі автором *удосконалено*:

- 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.

Зазначені наукові положення та отримані результати дисертаційних досліджень вирішують важливу наукову проблему, яка полягає у необхідності розвитку теоретичних і методологічних основ створення методів генерування паролів при впровадженні політик інформаційної безпеки.

Практичне значення одержаних результатів полягає в формуванні паролічних політик, що дозволяє раціонально обрати спосіб генерування паролів серед множини існуючих, а спосіб генерування ускладнених паролів в системах бездротового зв'язку дозволяє сформулювати стійкий до підбору пароль.

Повнота викладення одержаних результатів в опублікованих працях. Основні результати дисертаційного дослідження достатньо повно викладено в одній монографії, 8 статтях у фахових наукових виданнях України з технічних наук, у тому числі 3 статті – у виданнях, які входять до міжнародних науково-метричних баз.

Окрім того, результати досліджень пройшли апробацію на 8 науково-практичних (технічних) конференціях та семінарах.

Недоліки та зауваження.

Дисертація Платоненка А.В. та її автореферат не позбавлені певних недоліків. Найбільш визначальними серед них є такі:

1) не приведено розрахунку часу, що необхідний для створення паролю згідно запропонованого способу, що відповідно ускладнює можливість оцінки необхідного часу для створення паролів завдяки способам-аналогам, які розглядаються в роботі;

2) не зрозуміло, в якій операційній системі передбачається використання запропонованої автором способу генерування паролів та які вимоги висуваються до обчислювальної потужності комп'ютерної техніки;

3) не наведено прикладів практичної реалізації вдосконаленого способу генерування паролів, відповідно досить складно оцінити та порівняти його перевагу перед способами-аналогами;

4) не повною мірою розкрито аспект створення програмного забезпечення, як основної складової для впровадження запропонованого способу генерування паролів;

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

Зазначені недоліки не є визначальними й не знижують загальної наукової цінності та практичного значення основних положень дисертаційної роботи, а також отриманих у ній результатів.

3. Відповідність дисертаційної роботи встановленим вимогам та загальний висновок

Дисертаційна робота Платоненка Артема Вадимовича за темою «Технологія забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення паролівних 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 значно впливають на забезпечення відмовостійкості систем бездротового зв'язку за рахунок підвищення стійкості паролівних політик до спроб несанкціонованого доступу.

За актуальністю, ступенем новизни, обґрунтованістю, науковою і практичною значимістю одержаних результатів дисертаційна робота Платоненка А.В. відповідає паспорту спеціальності 05.13.06 – «інформаційні технології» та вимогам «Порядку присудження наукових ступенів», затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами), а її автор Платоненко Артем Вадимович заслуговує присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «інформаційні технології».

Офіційний опонент
доктор технічних наук, доцент,
професор кафедри інженерії програмного забезпечення
Національного авіаційного університету

С. В. Зибін



Зибін С.В.

свідчую

Вчений секретар

Національного авіаційного університету

Г. Гурбо