Опирский И.Р., Головатый Т.И. **Последовательная проверка нескольких прогнозов несанкционированного доступа в байесовской постановке задачи**

Приведены исследования и анализ прогнозирования НСД при байесовской постановке задачи. Показано, что оптимальное последовательное правило проверки многоальтернативных гипотез, при принятых в работе предположениях, заключается в сравнении апостериорной вероятности гипотезы с переменным (случайным) порогом, зависит от совокупности апостериорных вероятностей остальных гипотез. Полное решение задачи состоит в нахождении явного выражения для границы, вид которой определяется распределением вероятностей наблюдения.

Определено, что в случае очень "дальних" гипотез оптимальное последовательное решающее правило заключается в выборе на каждом шагу номера гипотезы, соответствующей максимальной апостериорной вероятности, ее сравнение со случайным порогом. Представлены отношения для нахождения оптимальных порогов в случае независимых и зависимых наблюдений.

Ключевые слова: байесовское последовательное правило, прогноз, информационная сеть государства, несанкционированный доступ, апостериорный риск, оптимальное правило, транзитивность.

Opirskyy I.R., Holovaty T.I. **Serial Testing of Several Tamper Forecasts in Bayesian Formulation of the Problem**

The paper presents research and analysis at forecasting tamper in Bayesian formulation of the problem. It is shown that the optimal sequence validation rule for many alternative hypotheses, when taken in the assumptions, is to compare the posterior probability of the hypothesis with a variable (random), the threshold depends on the totality of the remaining posterior probabilities of hypotheses. Complete solution to the problem is to find an explicit expression for the boundary, the form of which is determined by the probability distribution of observation. It was determined that in the case of a very "distant" hypotheses consistent optimal decision rule is to choose numbers at each step of the hypothesis corresponding to the maximum a posteriori probability of its comparison with the random threshold. The article presents the relationship for finding optimal thresholds in the case of independent and dependent events.

Keywords: Bayesian sequential rule, the forecast, the state news network, unauthorized access, posteriori risk, the optimal rule transitivity.

УДК 681.5

АНАЛІЗ ОСОБЛИВОСТЕЙ ТА ЕФЕКТИВНОСТІ РОБОТИ АНТИВІРУСНИХ СИСТЕМ ДЛЯ ANDROID

О.О. Качурін[1], А.Ю. Кіт[2,3]

Проаналізовано особливості та ефективність роботи антивірусних систем для Android. Здійснено аналіз сучасного стану Android на предмет вірусних атак. Проведено типологію вірусів за доступом до даних і їхньої небезпеки. Проаналізовано типологію і функції троянських програм (вірусів), які можуть використовуватись на Android. Висвітлено проблематику тестувань ефективності роботи антивірусів для Android. Досліджено ефективність роботи антивірусів на Android. На основі досліджень подано рекомендації щодо підвищення захисту від вірусів під час використання антивірусних додатків для Android.

[1] студ. О.О. Качурін – НУ "Львівська політехніка";
[2] аспір. А.Ю. Кіт – НУ "Львівська політехніка";
[3] наук. керівник: проф. В.А. Мельник, д-р техн. наук

Ключові слова: антивірус, Android, вірус, троянська програма, смартфон, антизлодій, сканер.

Постановка проблеми. Цього року ринок мобільних пристроїв уперше обігнав ринок ПК. Це знакова подія, а також стрімке зростання обчислювальної потужності і можливостей мобільних пристроїв ставлять перед нами нові питання та проблеми в галузі забезпечення інформаційної безпеки [1-3].

Сучасні смартфони і планшети містять в собі цілком дорослий функціонал, аналогічний такому у своїх "старших братів". Видалене адміністрування, підтримка VPN, браузери з flash і java-script, синхронізація пошти, заміток, обмін файлами. Усе це дуже зручно, проте ринок засобів захисту для подібних пристроїв розвинений ще слабо. Вдалим прикладом корпоративного стандарту є BlackBerry, смартфон з підтримкою централізованого управління через сервер, шифруванням, можливостями видаленого знищення даних на пристрої. Проте його частка на ринку не така велика, а на російському і зовсім практично відсутній. Але існує маса пристроїв на базі Windows Mobile, Android, iOS, Symbian, які захищені значно слабше. Основні проблеми безпеки пов'язані з тим, що різноманіття ОС для мобільних пристроїв дуже велике, також як і кількість їх версій в одному сімействі [4-6].

Тестування та пошук вразливості у них відбувається не так інтенсивно як для ОС на ПК, те ж саме стосується і мобільних застосувань. Сучасні мобільні браузери вже практично наздогнали настільні аналоги, проте розширення функціонала спричиняє за собою велику складність і меншу захищеність. Далеко не всі виробники випускають оновлення, що закривають критичні уразливості для своїх пристроїв, – справа в маркетингу і в термінах життя конкретного апарату. Пропонуємо розглянути типові дані, що зберігаються на смартфоні, які можуть бути корисні для зловмисника.

Мета роботи – дослідити особливості та ефективність роботи антивірусних систем для Android, та на основі цього розробити рекомендації, щодо підвищення захисту смартфона від вірусів.

Виклад основного матеріалу. Тенденція така: чим більш функціональний телефон, тим до більшої кількості загроз він схильний. Будь-які команди, функції і можливості, що дають змогу створювати програми і застосування для мобільних телефонів, можуть стати інструментом для створення вірусів. Найбільш перспективною платформою для написання вірусів є Java 2ME, оскільки більшість сучасних телефонів підтримують цю платформу [2].

Основною метою мобільних вірусів, як і у випадку з комп'ютерними вірусами, є отримання персональної інформації, яку можна продати або використовувати в особистих потребах. До такої інформації можна віднести особисті дані власника телефону, дані самого пристрою, особисті повідомлення, іноді номери кредитних карт [3, 4]. Отже, усі види вірусів або т. зв. троянських програм, можна поділити на 3 основні типи:

1. Крадіжка персональної інформації. В даному випадку віруси збирають різні відомості, наявні в телефоні, наприклад, контакти власника телефону, паролі від програм, параметри облікових записів, таких, як Google Play або AppStore. Уся інформація, отримана вірусом, вирушає на сервер зловмис-

ників, де використовується на їх розсуд. Один із найсерйозніших вірусів такого плану – Android.Geinimi. Потрапляючи в систему, він визначає місце розташування смартфону, завантажує файли з Інтернету, прочитує і записує закладки браузера, отримує доступ до контактів, здійснює дзвінки, відправляє, читає і редагує SMS-повідомлення.

2. Відправка платних SMS-повідомлень, дзвінки на "партнерський номер" без відома власника. У цьому випадку за надсилання повідомлення або за дзвінок списується серйозна сума коштів з особистого рахунку власника телефону. Зрозуміло, гроші потрапляють до рук зловмисників. З найвідоміших подібних загроз можна назвати Android.SmsSend, а також давно відомі RedBrowser і Webster для Java-платформи. Вони маскуються під різні корисні програми, викликаючи цим самим довіру у користувача. Також існують віруси і для інших платформ, наприклад, Symbian OS, Windows Mobile та ін.
3. Шахрайство за допомогою використання систем інтернет-банкінгу. У цьому випадку вірус відкриває доступ до мобільного застосування для роботи з банком або відповідного веб-сайту, або перехоплює SMS, що передаються користувачеві від систем інтернет-банкінгу. Небезпека цього типу може підстерігати власників мобільних телефонів, що працюють на різних платформах. Відомий троян Trojan – Spy.SymbOS.Zbot.a, що працює в комплексі з популярним вірусом Zbot для звичайних ПК.

Основними вірусами, які існують наразі на Android, є:

- Троян Trojan – SMS.AndroidOS.FakePlayer.a;
- Android.Geinimi – A;
- Android.SMSReplicator;
- Android.Ewalls.

Android – це відкрита операційна UNIX подібна система, заснована на ядрі Linux.Unix подібна означає те, що усі дії програм і файлів (копіювання, переміщення, управління системою тощо) відбуваються тільки за дозволу користувача.

Табл. Результати тестування антивірусів на Android

Назва антивіруса	Ефективність захисту	Зручність	Додаткові функції	Використання батареї	Завантаження системи	Оцінка
TrustGo Antivirus & Mobile Security	6	5	4	4	5	24
AVL 2.2.23	6	6	-	6	6	24
Bitdefender Mobile Security & Antivirus	4	5	4	4	4	21
Lookout Antivirus	4	5	5	3	3	20
Norton Mobile Security	5	4	4	3	4	20
avast! Mobile Security	5	6	5	3	4	23
Kaspersky Mobile Security	4	5	5	3	3	20
Dr.Web	3	5	6	3	4	21

Якщо немає прав суперкористувача (тобто рути), смартфон ніколи не вийде з ладу або не зависатиме від якоїсь "поганої програми". Фактично на сьогодні налічується близько 6 типів (типу "страшних" рядків коду), які можуть

вивести девайс з ладу. Але невдача, для того, щоб це сталося, має бути певна модель смартфона з певним процесором (а таких моделей всього 8), і потрібно змінити системні параметри або поставити прошивку/ядро з цим "девайс-кіллером", що теж неможливе, оскільки кастомні прошивки завжди перевіряються.

Отже, проаналізувавши відомі антивіруси, створено табл. з їхнього забезпечення безпеки, функціональності, підвантаження системи і використання батареї. Антивірус повинен виконувати свою вимогу захисту від вірусів чи троянів і мати хорошу функціональність в пошуку вкраденого телефону. Порівнюючи з лабораторію AZ-test, наявні певні розбіжності, тому кожен може визначити для себе якомога кращий антивірус.

Висновки. Дослідження та тестування сучасних антивірусних систем на Android, проведених на основі запропонованих критеріїв оцінки, таких як ефективність захисту, зручність, додаткові функції, використання батареї та завантаження системи, показало, що оптимальним й ефективним антивірусом, згідно з цими критеріями, є антивіруси TrustGo Antivirus & Mobile Security та AVL. Окрім цього, з'ясовано, що поза додатковими функціями ці антивіруси поступаються своїм конкурентам, що важливо, оскільки такі додаткові функції, як антизлодій, визначення місця знаходження викраденого телефону, блокування вкраденого телефону, стирання інформації дистанційно з викраденого телефону тощо є необхідним атрибутом смартфона щодо захисту інформації.

Також урахування сучасних недоліків цих систем дало змогу розробити рекомендації щодо політики безпеки використання телефона на Android незалежно від використання антивірусу, основою з яких є: блокування пристрою, використання криптографічних засобів, заборона на збереження паролів у браузері мобільного пристрою, заборона використання менеджерів паролів для корпоративних облікових записів, заборона на установку з неперевірених джерел, здійснення "зломів" ос, використання політик exchange activesync і засобів антивірусного й іншого захисту, у разі надання доступу в довірену зону здійснювати ретельний контроль, обмежити список даних, які можна передавати хмарним сервісам.

Література

1. Інформація з вікіпедії. [Електронний ресурс]. – Доступний з http://ru.wikipedia.org/wiki/мобільний вірус.

2. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К. : Изд-во "Юниор", 2003. – 504 с.

3. Список мобильних вірусів. [Електронний ресурс]. – Доступний з http://netler.ru/pc/mobivir.htm (дата обращения 18.11.2013).

4. Історія мобільних вірусів. [Електронний ресурс]. – Доступний з http://andromania.org/2011/02/13/mobil-nye-virusy.html (дата обращения 21.11.2013).

5. Goodman M. International Dimensions of Cybercrime // S. Ghosh and E. Turrini (eds.), Cybercrimes: A Multidisciplinary Analysis. Berlin, Heidelberg, 2010, 123-129 pp.

6. International Data Corporation. [Electronic resource]. – Mode of access http://www.idc.com/.

Надійшла до редакції 16.05.2016 р.

Качурин О.О., Кит А.Ю. **Анализ особенностей и эффективности работы антивирусных систем для Android**

Проведен анализ особенностей и эффективности работы антивирусных систем для Android. Проанализировано современное состояние Android на предмет вирусных атак. Приведена типология вирусов по доступу к данным и их опасности. Проведен анализ типологии и функций троянских программ (вирусов), которые могут использоваться на Android. Освещена проблематика тестирования эффективности работы антивирусов для Android. Проведено исследование эффективности работы антивирусов на Android. На основе исследований представлены рекомендации по повышению защиты от вирусов при использовании антивирусных приложений для Android.

Ключевые слова: антивирус, Android, вирус, троянская программа, смартфон, антивор, сканер.

Kachurin O.O., Kit A.Yu. **The Analysis of Features and Performance Protection of Viruses for Android**

This paper is devoted to the analysis of the characteristics and performance of antivirus systems for android. The analysis of the current state of Android in terms of virus attacks is being conducted. A typology of viruses on access to data and their dangers is made. The analysis of the typology and functions of Trojans (viruses) that can be used on Android is completed. The scope of the study of the test performance of antivirus for Android is described. A study of the effectiveness of anti-virus on Android is given. Some recommendations to improve virus protection using anti-virus applications for Android are proposed based on the studies conducted.

Keywords: antivirus, Android, virus, Trojan, smartphone, antitheft, scanner.

УДК 621.01:624.046.3

РОЗРАХУНОК НА СТІЙКІСТЬ БАГАТОПРОГОНОВОЇ ВИСОТНОЇ КОНСТРУКЦІЇ З ЛОКАЛЬНИМИ ПОСЛАБЛЕННЯМИ

О.Є. Кунта[1,2]

Побудовано математичну модель напружено-деформованого стану та узагальнений алгоритм розрахунку багатопрогонової висотної конструкції на стійкість із застосуванням некласичної теорії балок С. Тимошенка. Споруда защемлена в основі і додатково закріплена на межах прогонів за допомогою відтяжок. На верхньому кінці висотна конструкція навантажена статичною осьовою силою. Момент інерції поперечного перерізу і поздовжня сила змінюються за ступінчастим законом по висоті. Місцеві послаблення розглянуто як пружні шарнірні з'єднання прогонів. Розрахунок виконано з урахуванням податливості кріпильних вузлів, із застосуванням матричного методу початкових параметрів. На розрахункових прикладах проілюстровано вплив місцевих послаблень на стійкість висотної конструкції.

Ключові слова: багатопрогонова висотна конструкція, локальні послаблення, стійкість, теорія балок С. Тимошенка, матричний метод початкових параметрів.

Постановка проблеми. У канатних установках для транспортування деревини, на підіймально-транспортних машинах та пристроях, установках вітрової енергетики, бурових установках, лініях електропередач тощо широко застосовують висотні несні конструкції щоглового типу. Здебільшого, такі конструкції жорстко закріплюють на фундаментах і додатково з'єднують з основою за допомогою відтяжок або інших кріпильних елементів.

[1] аспір. О.Є. Кунта – НУ "Львівська політехніка";
[2] наук. керівник: проф. І.В. Кузьо, д-р техн. наук – НУ "Львівська політехніка"

Основним критерієм працездатності щоглових конструкцій є їхня стійкість. Саме тому проблемі стійкості пружних систем у науковій літературі приділяють значну увагу. Класичні задачі стійкості пружних однопрогонових і багатопрогонових систем зводяться до знаходження й аналізу фундаментальних розв'язків диференціальних рівнянь зігнутої осі стрижня [1-3, 4, 5]. Для дослідження стійкості висотних довгомірних конструкцій застосовують також енергетичні та динамічні критерії [6, 8]. Вивчають вплив особливостей прикладання навантажень, зокрема дії неконсервативних сил на стійкість однопрогонових конструкцій [3, 6, 8]. Досліджують особливості розрахунку складених довгомірних конструкцій [1, 5], а також конструкцій змінного поперечного перерізу [4].

Розглядають вплив власної ваги на стійкість висотних конструкцій [5, 10], а також вплив дії пружного середовища на критичне осьове навантаження стрижнів [1-3, 5]. У зв'язку з однотипністю задач про вільні коливання та про стійкість пружних систем, ці задачі нерідко розв'язують у спільній постановці [8, 10, 13, 15] та розробляють спільні алгоритми розрахунку власних частот, критичних навантажень, а також власних форм коливань та форм деформування на межі стійкості. Особливу увагу приділяють розробленню комп'ютерних методів і алгоритмів розрахунку довгомірних конструкцій на стійкість [1, 2, 11, 13, 16]. Вивчають стійкість довгомірних конструкцій, що перебувають під дією динамічних навантажень [3, 6, 10, 12, 17]. Зауважимо, що у дослідженнях стійкості і коливань висотних або довгомірних конструкцій застосовують як технічну теорію згину [2-4, 7, 17], так і некласичну теорію балок С. Тимошенка [1, 5, 13, 15]. Для виконання розрахунків багатопрогонових конструкцій набув застосування матричний метод початкових параметрів [2, 7].

Особливе місце відводиться вивченню динаміки та стійкості довгомірних конструкцій з локальними послабленнями, що можуть бути зумовлені місцевими звуженнями поперечного перерізу, наявністю податливих з'єднань, а також дефектами матеріалу, що з'являються у процесі його старіння (корозія, тріщини, розшарування металу тощо). У найпростішому випадку розрахунок таких конструкцій виконують на основі застосування моделей зі скінченним числом ступенів вільності, у яких споруду розглядають як систему твердих тіл, зв'язаних між собою за допомогою пружних шарнірів [4, 6, 16]. У праці [16] вивчено вплив як лінійних, так і нелінійних жорсткісних властивостей пружних шарнірів на стійкість системи під дією неконсервативних сил. Більш точну, двопрогонову модель довгомірної конструкції з лінійним пружним шарніром побудовано зі застосуванням теорії балок С. Тимошенка [13] і реалізовано під час визначення власних частот і критичних навантажень механічної системи. Дослідження коливань і стійкості двопрогонових пружних конструкцій з тріщинами висвітлено у працях [12, 14], у яких розглянуто особливості визначення жорсткісних характеристик локальних послаблень. Експериментальні дослідження динамічної стійкості консольної балки з тріщиною [9] засвідчують несиметричний характер коливальних процесів у механічній системі, що можна пояснити нелінійністю жорсткісної характеристики місцевого послаблення з тріщиною. Для дослідження стійкості двопрогонової конструкції з місцевим послабленням, що характеризується податливістю у поперечному і в оберталь-