УДК 35.077:347.97/99:004.8
DOI https://doi.org/10.32689/maup.it.2022.3.1

Микола ВАСИЛЕНКО
доктор фізико-математичних наук, доктор юридичних наук, професор, професор кафедри кібербезпеки, Національний університет «Одеська юридична академія», вул. Рішельєвська, 28, Одеса, Україна, індекс 65011 (vasylenko.it@journals.maup.kiev.ua)

ORCID: http://orcid.org/0000-0002-8555-5712

Валерія СЛАТВІНСЬКА
викладач кафедри кібербезпеки, Національний університет «Одеська юридична академія», вул. Рішельєвська, 28, Одеса, Україна, індекс 65011 (slatvinskaya_valeriya@ukr.net)

ORCID: https://orcid.org/0000-0002-6082-981X

Nikolai VASILENKO
Doctor of Physical and Mathematical Sciences, Doctor of Law, Professor, Professor of the Department of cybersecurity, National University «Odessa Law Academy», 28 Richelevskaya str., Odessa, Ukraine, postal code 65011 (vasylenko.it@journals.maup.kiev.ua)

Valeriia SLATVINSKA
Assistant Professor of the Department of cybersecurity, National University «Odessa Law Academy», 28 Richelevskaya str., Odessa, Ukraine, postal code 65011 (slatvinskaya_valeriya@ukr.net)

Бібліографічний опис статті: Василенко, М., Слатвінська, В. Кібернетичний захист операційних систем (аналітичне оглядове дослідження). *Інформаційні технології та суспільство*. 2022. Вип. 3 (5), 6–13. DOI:

Bibliographic description of the article: Vasilenko, M., Slatvinska, V. (2022). Kibernetychnyi zakhyst operatsiinykh system (analitychne ohliadove doslidzhennia) [Cyber security of operating systems (analytical and review research)]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 3 (5), 6–13. DOI:

КІБЕРНЕТИЧНИЙ ЗАХИСТ ОПЕРАЦІЙНИХ СИСТЕМ (АНАЛІТИЧНЕ ОГЛЯДОВЕ ДОСЛІДЖЕННЯ)

Кібернетичний захист операційних систем (ОС) обговорюється як оглядове дослідження. Оскільки ОС складається з ядра ОС та базового набору прикладних програм йдеться про їх захист в процесі функціонування системи. Однак організація ефективного та надійного захисту ОС неможлива за допомогою одних лише програмно-апаратних засобів, а потребує цілий комплекс заходів. Будь-який комп'ютер складається з чотирьох основних компонентів: центрального процесора; оперативної пам'яті, яка тимчасово зберігає оброблювану інформацію, програмні коди та результати обробки; пристрою введення/виводу, системної магістралі, що визначає механізм взаємодії зазначених вище компонентів. При цьому важко усвідомити усю безліч дій, що виконують і фіксують ОС, яка потребує захисту від внутрішніх та зовнішніх небезпек. Існують певні послуги, що надають ОС в захищеному (незахищеному) режимі. Сформульовані послуги, що надаються в цих умовах типовими ОС, до яких відносять наступні: розробка програм, виконання програм, доступ до пристроїв вводу-виводу; контрольований доступ до файлів; системний доступ; виявлення помилок та їх обробка; облік використання ресурсів; структура системи команд; інтерфейс прикладного програмування; а також бінарний інтерфейс програми. Можливість доступу до об'єктів ОС визначається не тільки архітектурою ОС, а й поточної безпековою ситуацією доступу до об'єкта. Показано, як у практично значущих ситуаціях захищена ОС зазвичай містить засоби управління доступом користувачів до різних ресурсів, засоби перевірки справжності користувача, що починає роботу з ОС, а також застосовувати засоби реєстрації дій користувачів потенційно небезпечних з точки зору безпеки. Розглянемо типові загрози безпеці ОС мобільного пристрою, які суттєво відрізняються від аналогічних загроз для ОС персонального комп'ютера або мережевого сервера. Констатується в результаті обговорень, що основною проблемою забезпечення безпеки ОС все ж таки залишається контроль доступу до ресурсів системи.

Ключові слова: *обчислювальна машина, мобільний пристрій, операційна система, доступ, захист, безпека.*

CYBER SECURITY OF OPERATING SYSTEMS (ANALYTICAL AND REVIEW RESEARCH)

Cyber security of operating systems (OS) is discussed as a survey research. Since the OS consists of the OS kernel and the basic set of applications, it is about their protection in the process of system operation. However, the organization of effective and reliable OS protection is impossible with the help of software and hardware alone, but requires a whole range of

measures. Any computer consists of four main components: the central processor; RAM, which temporarily stores the processed information, program codes and processing results; input/output device, system backbone, which determines the mechanism of interaction of the above components. At the same time, it is difficult to realize all the many actions performed and recorded by the OS, which needs protection from internal and external dangers. There are certain services that provide OS in protected (unprotected) mode. The services provided in these conditions by typical operating systems are formulated, which include the following: program development, program execution, access to input/output devices; controlled access to files; system access; error detection and processing; resource usage accounting; command system structure; application programming interface; and binary program interface. The possibility of access to OS objects is determined not only by the OS architecture, but also by the current security situation of access to the object. It is shown how, in practically significant situations, a secure OS usually contains means of controlling user access to various resources, means of authenticating a user who starts working with the OS, as well as applying means of registering user actions that are potentially dangerous from a security point of view. Consider typical security threats to the OS of a mobile device, which are significantly different from similar threats to the OS of a personal computer or network server. It is stated as a result of the discussion that the main problem of OS security is still the control of access to system resources.

Key words: *computer, mobile device, operating system, access, protection, security.*

Актуальність проблеми. Виходячи із загальних положень кібербезпеки, операційну систему слід вважати захищеною, якщо вона передбачає засоби захисту від основних загроз конфіденційності, цілісності та доступності інформації, актуалізованих з урахуванням особливостей експлуатації конкретного екземпляра операційної системи (ОС, англ. OS).

Адекватною безпековою політикою можна вважати таку політику безпеки, яка забезпечує достатній рівень захищеності ОС. Слід особливо відзначити, що адекватна безпекова політика не обов'язково є тією політикою безпеки, при якій досягається максимально можлива захищеність системи.

З іншого боку, користувачами ОС виступають особи, в інтересах яких здійснюється обробка даних обчислювальних систем (виконання складний розрахунків, управління виробничими процесами і т. д.). Основним технічним засобом для цього стали електронно-обчислювальні машини, включаючи комп'ютери, які здатні ефективно обробляти будь-які види інформації (числову, текстову, табличну, графічну, відео, звукову), заздалегідь перетворивши її в цифрову форму. Програмні засоби керуються наборами цифрових кодів (інструкцій), що управляють технічними засобами залежно від алгоритмів рішення конкретних інформаційний завдань користувача. Отже, для роботи такої системи потрібен комплекс програм, що виконує керування апаратною складовою комп'ютера та забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем. Таким комплексом програм стала ОС, яка звичайно складається з ядра ОС та базового набору прикладних програм. Однак організація ефективного та надійного захисту ОС неможлива за допомогою одних лише програмно-апаратних засобів. Ці засоби обов'язково мусять входити в комплексну систему захисту ОС, надійно їх захищаючи. При цьому комплексний оглядовий підхід до цієї проблеми в періодичній літературі майже не висвітлений, хоча спеціалісти одностайні в тому, що без постійної кваліфікованої підтримки з боку адміністратора навіть найнадійніший програмно-апаратний захист обертається фікцією.

Аналіз останніх досліджень і публікацій. ОС за останні півстоліття змінилися до невпізнання: мінилася оболонка, манера програмування ОС, функціональність і можливість використовувати як для особистих потреб, так і для систем управління на всіляких виробництвах. При цьому ОС залишаються невід'ємною частиною обчислювальних систем. Звичайний користувач навіть не уявляє, які складні процеси відбуваються одночасно у системі, дозволяючи, наприклад читати новини в Інтернеті. Тому, варто враховувати всю складність створення нової та неповторної ОС. Очевидно, що змінилися підходи щодо захищеності таких систем.

Слід наголосити на тому, що ОС представляють собою громіздке програмне забезпечення, що складається з мільйонів рядків. Над розробкою нової системи працюють цілі команди фахівців, проводячи за роботою багато часу, оскільки ОС здебільшого визначається як величезний інженерний проект, який можна порівняти з будівництвом чогось дуже значущого.. Величезні блоки програмного коду часто не можуть бути відокремленими одиницями та постійно взаємодіють з іншими блоками інформації, ускладнюючи завдання, що стоять перед розробниками. Існує досить велика кількість різних операційних систем: від довгожителів, таких як UNIX та його клони, до дуже нових і маловідомих систем. В той же час робіт, присвячених захисту та безпеці операційний систем, небагато. Деякий базовий матеріал викладено в підручниках (див., наприклад [1]). Однак сьогодення пред'являє більш високі вимоги та перспективніші методи захисту ОС ніж це було раніше [2]. В книзі [3] розглядаються загальні концепції безпеки, включаючи принципи інформаційної безпеки, стандарти, регулювання та дотримання; автентифікація, авторизація та облік; та контроль доступу. Аналіз звітів і публікацій про виявлені вразливості у системі Windows і патчів для їх усунення, висвітлені, наприклад на офіційних сайті Microsoft, дають зрозуміти напрями підвищення забезпечення безпеки операційної системи [4-6]. В статті [7]

визначено, що базовим підходом щодо безпеки операційних систем виступає процес «загартовування операційної системи». Показано приклади реалізації Блокчейн для перевірки сертифікатів, враховуючи деякі із варіацій перевірок, які реалізовано на Python 3.0. Автори [7] стверджують: «Використання загартовування системи, є одним з дієвих та комплексних підходів щодо забезпечення інформації безпеки, що дозволить своєчасно виявляти вразливості та своєчасно реагувати на порушення базових властивості операційної системи». В роботі [8] зазначено складність і невичерпність проголошених завдань, які потребують значного наукового опрацювання. Система виявлення вторгнень з використанням технології зв'язаних списків (блокчейн) в процесі реалізації програмного забезпечення обговорювалася також в [9-12]. При обговоренні захисту ОС різні автори фактично розглядають окремі питання щодо проблеми, не виходячи за межі конкретного обговорення. В свою чергу, це ще більше ускладнює і так досить складні питання генези їх захисту. Тому, враховуючи величезну широту і глибину проблеми, а також її багатогранність, наступні дослідження потребують всебічного оглядового аналізу, який і пропонується в наведеній статті.

Метою статті є загальний аналітичний огляд стану захисту ОС в динаміці кібернетичного розуміння їх безпеки.

Виклад основного матеріалу. Важко не погодитися з тим, що будь-який комп'ютер складається з чотирьох основних компонентів: центрального процесора, що керує іншими компонентами та викидає функції обробки інформації; оперативної пам'яті, яка тимчасово зберігає оброблювану інформацію, програмні коди та результати обробки; пристрою введення/виводу, що переміщує інформацію від користувача; системної магістралі, що визначає механізм взаємодії зазначених вище компонентів. При цьому важко усвідомити усю безліч дій, що виконують і фіксують ОС. Однак очевидним для фахівців є і те, що кожен користувач системи має доступ тільки до тих об'єктів ОС, до яких йому надано доступ відповідно до поточної політики безпеки. Доступ користувачів до інших суб'єктів доступу може бути довільно обмежений. Ключовим словом в даному визначенні є слово «довільно». Однак, говорячи про доступ до ОС, треба знати саме ті послуги, що надають ті ж самі ОС. До послуг, що надаються типовими ОС можна віднести ті, які наводяться нами нижче.

• **Розробка програм.** Сприяючи програмісту при розробці програм, операційна система надає йому різноманітні інструменти та служби, наприклад, редактори або відладчики. Зазвичай ці служби реалізовані у вигляді програм утиліт, які підтримуються операційною системою, хоч і не входять до її ядра.

Такі програми називають інструментами розробки прикладних програм.

• **Виконання програм.** Для виконання програми потрібно здійснити ряд дій. Слід завантажити в основну пам'ять команди та дані, ініціалізувати пристрої вводу-виводу та файли, а також підготувати інші ресурси. ОС виконує всю цю рутинну роботу замість користувача.

• **Доступ до пристроїв вводу-виводу.** Для керування роботою кожного пристрою вводу-виводу потрібен особливий набір команд або контрольних сигналів. ОС надає користувачеві одноманітний інтерфейс, який приховує всі ці деталі та забезпечує програмісту доступ до пристроїв введення-виведення за допомогою простих команд читання та запису.

• **Контрольований доступ до файлів.** Працюючи з файлами управління з боку операційної системи передбачає як глибоке розуміння природи пристроїв вводу-виводу (дисковода, стрічкопротяжного пристрою), а також знання структур даних, записаних у файлах Багатокористувацькі ОС, крім того, можуть забезпечувати роботу механізмів захисту під час звернення до файлів.

• **Системний доступ.** Операційна система керує доступом до спільно використовуваної або загальнодоступної обчислювальної системи в цілому, а також окремих системних ресурсів. Вона повинна забезпечувати захист ресурсів та даних від несанкціонованого використання, а також вирішувати конфліктні ситуації.

• **Виявлення помилок та їх обробка.** При роботі комп'ютерної системи можуть відбуватися різноманітні збої. До них належать внутрішні та зовнішні помилки, що виникли в апаратному забезпеченні (наприклад, помилки пам'яті,

відмова або збій пристроїв). Можливі (різні) програмні помилки (такі, як арифметичне переповнення, розподіл на нуль, спроба звернутися до осередку пам'яті, доступ до якого заборонено, або неможливість виконання запиту програми). У кожному з цих випадків операційна система має виконати дії, що мінімізують вплив помилки на роботу програми. Реакція ОС на помилку може бути різною – від простого повідомлення про помилку до аварійної зупинки програми, що її викликала.

• **Облік використання ресурсів.** Хороша операційна система повинна мати засоби обліку використання різних ресурсів та відображення параметрів продуктивність. Ця інформація вкрай важлива у будь-якій системі, особливо у зв'язку з необхідністю подальших поліпшень та налаштування обчислювальної системи підвищення її продуктивності. У розрахованих на багато користувачів системах ця інформація може застосовуватися для виставлення рахунків.

• **Структура системи команд** (instruction set architecture – ISA). Визначає набір команд машинної мови, які можуть виконувати комп'ютер. Цей інтерфейс є межею між апаратним та програмним забезпеченням. Зверніть увагу, що і прикладні програми, і утиліти можуть отримати безпосередній доступ до ISA. Для цих програм доступне підмножина команд (користувацька ISA). ОС має доступ до додаткових команд машинної мови, що належать до керування ресурсами системи (системна ISA).

• **Бінарний інтерфейс програми** (application binary interface – ABI). ABI визначає стандарт бінарної переносимості між програмами. ABI визначає інтерфейс системних викликів операційної системи та апаратних ресурсів та служб, доступних у системі через користувальницьку ISA.

• **Інтерфейс прикладного програмування** (application programming interface – API). API забезпечує програмі доступ до апаратних ресурсів та служб, доступних у системі через користувальницьку ISA з бібліотечними викликами мовою високого рівня. Зазвичай будь-які системні дзвінки виконуються через бібліотеки. Застосування API забезпечує легку переносимість прикладного програмного забезпечення інші системи, що підтримують той же API шляхом перекомпіляції.

Якщо правила обмежують доступ суб'єктів до деякого елементу ОС, вони визначені жорстко і не допускають зміни з плином часу. Іншими словами, можливість доступу до об'єктів ОС визначається не тільки архітектурою ОС, а й поточної безпековою ситуацією (методом) доступу до об'єкта. Наприклад, для файлів можуть бути визначені: методи доступу «читання», «запис» і «додавання» (дописування інформації в кінець файлу). Суб'єктом доступу тут слід називати будь-яку сутність, здатну ініціювати виконання операцій над об'єктами (звертатися до об'єктів за деякими методами доступу).

У практично значущих ситуаціях захищена ОС зазвичай містить засоби управління доступом користувачів до різних ресурсів, засоби перевірки справжності користувача, що починає роботу з ОС, а також застосовувати засоби реєстрації дій користувачів потенційно небезпечних з точки зору безпеки. Крім того, захищена операційна система повинна містити засоби протидії випадковому або навмисному виведенню операційної системи з ладу.

Вважається визнаною політикою безпеки набір норм, правил і практичних прийомів, які регламентують порядок зберігання та обробки цінної інформації. У застосуванні до операційної системи політика безпеки визначає те, які користувачі можуть працювати з операційною системою, які мають доступ до конкретних об'єктів операційної системи, які події повинні реєструватися в системних журналах і т.д.

Важливим ланцюжком з ОС стає ідентифікація та аутентифікація. Жоден користувач не може почати роботу з ОС, який не ідентифікував себе і не надавши системі аутентифікуючу інформацію, яка підтверджує, що користувач дійсно є тим, за кого він себе видає. (В захищеної операційної системи будь-який суб'єкт доступу, перед тим як почати роботу з системою, повинен пройти ідентифікацію, аутентифікацію і авторизацію. Ідентифікація суб'єкта доступу полягає у тому, що суб'єкт повідомляє операційній системі ідентифікаційну інформацію про себе (ім'я, обліковий номер і т. д.) і таким чином ідентифікує себе. Так,конкретна ОС може надавати захист різного ступеню для різних об'єктів, користувачів та додатків. У захищеній операційній системі будь-який суб'єкт доступу, перед тим як розпочати роботу з системою, повинен пройти ідентифікацію, автентифікацію та авторизацію.

Аутентифікація суб'єкта доступу полягає в тому, що суб'єкт надає системі крім ідентифікаційної інформації ще й аутентифікаційну інформацію, що підтверджує, що він дійсно є тим суб'єктом доступу, до якого належить ідентифікаційна інформація.

Авторизація суб'єкта доступу відбувається після успішної ідентифікації та аутентифікації. При авторизації суб'єкта операційна система виконує дії, необхідні для того, щоб суб'єкт міг почати роботу в системі – завантажує індивідуальні налаштування користувача, запускає програму-оболонку і т.п.

Авторизація суб'єкта не відноситься безпосередньо до захисту операційної системи. У процесі авторизації вирішуються суто технічні завдання, пов'язані з організацією початку роботи в системі вже ідентифікованого та автентифікованого суб'єкта доступу. Зауважимо, що у ряді джерел термін «авторизація» використовується як синонім терміна «управління доступом». Це вносить певну плутанину в термінологію у цій галузі.

З точки зору забезпечення безпеки комп'ютерної системи процедура аутентифікації є дуже відповідальною. Якщо порушник зумів увійти в систему від імені іншого користувача, тим самим порушник легко отримує доступ до всіх об'єктів системи, до яких має доступ цей користувач. Якщо при цьому процесі роботи порушника з операційною системою підсистема аудиту генерує повідомлення про потенційно небезпечних подіях, то в журнал аудиту буде внесено не ім'я порушника, а ім'я користувача, від імені якого порушник працює у системі.

Хоча аутентифікація може здійснюватися як фізичних користувачів, так псевдокористувачів, найбільший інтерес з погляду забезпечення інформаційної безпеки представляє аутентифікація фізичних

користувачів. Якщо в системі реалізується адекватна безпекова політика, фізичний користувач просто не може увійти в систему від імені псевдокористувача. Якщо псевдокористувач має великі повноваження, вхід порушника в систему від імені псевдокористувача дає порушнику великі можливості для здійснення несанкціонованого доступу, проте на практиці здійснити таку атаку зазвичай вкрай важко. Тому надалі ми розглядатимемо аутентифікацію тільки звичайних користувачів.

Зазвичай підсистема аутентифікації операційної системи будується за однією з трьох схем: парольна автентифікація; аутентифікація з використанням зовнішніх носіїв інформації; біометрична автентифікація.

Можливе використання комбінацій двох або навіть усіх трьох схем аутентифікації в одній системі.

В зв'язку з наведеними вище варіантами захищеності ОС виникає питання про їх характеристики і створення підходів до них. Відомі два основні підходи до створення захищених ОС – фрагментарний та комплексний. При фрагментарному підході спочатку створюється захист від однієї загрози, потім від іншої і т.д. Прикладом фрагментарного підходу може бути с ситуація, коли за основу береться незахищена операційна система, на неї встановлюються антивірусний пакет, потім система шифрування, система реєстрації дій користувачів і т.д.

Основний недолік фрагментарного підходу очевидний – при застосуванні цього підходу підсистема захисту операційної системи є набір розрізнених програмних продуктів, як правило, вироблених різними виробниками. Ці програмні засоби працюють незалежно один від одного, організувати їхню тісну взаємодію практично неможливо. Крім того, окремі елементи такої підсистеми захисту можуть некоректно працювати в присутності один одного, що призводить до різкого зниження загальної надійності системи. Оскільки підсистема захисту, створена з урахуванням фрагментарного підходу, перестав бути невід'ємною компонентою операційної системи, при відключенні окремих захисних функцій у результаті несанкціонованих дій користувача-порушника інші елементи операційної системи продовжують нормально працювати, що ще більше знижує надійність захисту.

При комплексному підході до організації захисту захисні функції вносяться в операційну систему ще на етапі проектування архітектури операційної системи та є її невід'ємною частиною. Окремі елементи підсистеми захисту, створеної на основі комплексного підходу, тісно взаємодіють один з одним при вирішенні різних завдань, пов'язаних з організацією захисту інформації. Оскільки вся підсистема захисту розробляється та тестується в сукупності, конфлікти між її окремими компонентами практично неможливі. Підсистема захисту, створена на основі комплексного підходу, може бути влаштована так, що при фатальних збоях у функціонуванні її ключових елементів підсистеми захисту вона викликає аварійне завершення роботи операційної системи, що не дозволяє порушнику відключати захисні функції системи. З використанням фрагментарного підходу така організація підсистеми захисту неможлива.

Як правило, підсистему захисту ОС, створену на основі комплексного підходу, проєктують так, що окремі її елементи є замінними і відповідні програмні модулі можуть бути замінені іншими модулями, що реалізують передбачений і належним чином документований інтерфейс взаємодії відповідного програмного модуля коїться з іншими елементами підсистеми захисту. Відома і така ситуація, коли існує відсутність захисту. Цей варіант підходить, коли відповідні процедури виконуються за часом окремо.

Існує також така ситуація як ізоляція. Кожний процес працює окремо від інших процесів, не використовуючи сумісно ресурси і не обмінюючись інформацією. Кожний процес має свій адресний простір, свої файли та інші об'єкти.

Можливими є повний розподіл або повна його відсутність. Власник об'єкту (файлу, сегмента пам'яті) об'являє його відкритим або закритим. У першому випадку доступ до об'єкта може отримати будь-який процес; у другому – доступ до цього об'єкта надається тільки власнику.

Спільне використання з обмеженнями доступу полягає в тому, що ОС перевіряє дозволеність доступу кожного окремого користувача до кожного окремого об'єкта. В цьому сенсі ОС виступає в якості охоронця, гарантуючи, що доступ до об'єкта отримають тільки авторизовані користувачі.

Спільне використання за допомогою динамічних можливостей. Цей варіант розширює концепцію контролю доступу, дозволяючи динамічно створювати права спільного використання об'єкта.

Існує також така ситуація, коли йдеться про обмежене використання об'єкта. При цьому обмежується не стільки доступ до об'єкта, скільки його використання. Наприклад, користувачеві дозволено переглядати важливий документ, але не роздруковувати, або користувач має доступ до бази даних, може брати з неї статистичні зведення, але не має можливості визначити значення певних величин.

Необхідно зауважити наступне: в ОС має підтримуватися баланс між можливостями спільного використання компонентів комп'ютерної системи в цілому, що сприяє підвищенню ефективності її використання, і стає ступенем захищеності ресурсів окремих користувачів.

При всій багатогранності проблеми не можна не відзначити негативний вплив на захищеність ОС незаконного використання привілеїв та щкідливе програмне забезпечення. Останнє розглядалося нами раніше у [13], тому це питання нами вже не обговорюється.

Наприкінці розглянемо типові загрози безпеці ОС мобільного пристрою, які суттєво відрізняються від аналогічних загроз для ОС персонального комп'ютера або мережевого сервера. Деякі загрози, незначні для звичайних комп'ютерів, стають дуже небезпечними для мобільних пристроїв, і навпаки. Наприклад, крадіжка мобільного телефону кишеньковим злодієм є набагато серйознішою загрозою, ніж крадіжка сервера злодієм-домушником. Програмна закладка, впроваджена в ОС персонального комп'ютера і що отримала доступ до електронних банківських рахунків користувача, зазвичай має дуже обмежені можливості з несанкціонованого переказу коштів з цих рахунків. Але програмна закладка, внесена в ОС мобільного пристрою, елементарно вирішує це завдання шляхом несанкціонованого замовлення дорогих SMS-послуг з телефонного номера, контрольованого порушником, або (рідше) шляхом імітації голосового дзвінка на платний номер. З іншого боку, загрози, пов'язані з одночасним доступом кількох користувачів до одного екземпляра ОС, для мобільних ОС, як правило, неактуальні.

До найбільш актуальних загроз безпеки мобільних ОС зазвичай відносять такі:

• розкриття конфіденційної інформації внаслідок втрати чи крадіжки мобільного пристрою;

• несанкціоноване замовлення дорогих послуг програмною закладкою, впровадженою в операційну систему мобільного пристрою;

• розкриття конфіденційної інформації в результаті перехоплення бездротового мережевого трафіку, що генерується мобільним пристроєм;

• несанкціонований збір програмною закладкою персональних даних користувача мобільного пристрою;

• втрата даних, що зберігаються на мобільному пристрої.

В даний час для мобільних операційних систем розробляється величезна кількість шкідливого програмного забезпечення. За даними [14], близько чверті всіх додатків, написаних для ОС Android, є шкідливими. Кількість шкідливих програм для Android зростає експонентно, щороку воно збільшується в 2-16 разів. Така велика різниця в цифрах, що даються різними джерелами, пояснюється тим, що межа між множинами шкідливих і неушкоджених мобільних додатків дуже умовна. Хорошим прикладом «прикордонних» додатків є програми, що дозволяють легальному власнику телефону виявити вкрадений у нього телефон шляхом непомітного перехоплення та доставки на задану адресу електронної пошти інформації про зроблені дзвінки, відправлені та отримані SMS, географічне розташування тощо.

Практичні дані свідчать, що компанія Google, на відміну від Apple, декларує максимальну відкритість своєї ОС Android. Кожна програма для Android повинна бути підписана розробником, але завірення цього підпису будь-яким засвідчуючим центром не потрібно. До каталогу Google Play та інтернет-магазину Android Market допускаються всі додатки, крім свідомо шкідливих і свідомо непрацездатних. Іноді це призводить до скандальних ситуацій, що негативно впливають на репутацію торгової марки Android. Наприклад, Android-версія програми eMobiStudio MemoryUp, що добре зарекомендувала себе на платформах Symbian, BlackBerry і Windows Mobile, несанкціоновано видалила через програмну помилку дані адресних книг кількох тисяч користувачів, які встановили цю програму.

На наш погляд, відкритість операційної системи Android не слід перебільшувати. На відміну від більшості розробників універсальних ОС, Google зберігає за собою контроль над усіма додатками, що працюють на всіх примірниках операційної системи Android. При необхідності компанія Google, як і Apple, може одночасно видалити всі екземпляри будь-якої заданої програми, встановленої на всіх мобільних пристроях зі своєю ОС.

Довгий час забезпечення безпеки мобільних ОС розглядалося їх розробниками як другорядне, низькопріоритетне завдання. Але ситуація поступово змінюється на краще, з кожною наступною версією мобільні операційні системи стають все більш захищеними. При цьому розробники мобільних ОС широко використовують рішення, апробовані на універсальних ОС.

Висновки та перспективи подальших досліджень. Таким чином, основною проблемою забезпечення безпеки ОС залишається контроль доступу до ресурсів системи. Для вирішення цієї проблеми ОС повинна мати власний допоміжний захист. Здебільшого зустрічаються такі атаки на ОС як сканування системи та спроби злому пароля. Виділяють дві основні загрози: крадіжка та добірка, а сам процес не повинен мати багато привілеїв. Існують фрагментарний та комплексний підхід створення захищеної ОС. При фрагментарному підході система насамперед захищається від однієї погрози, тільки потім від іншої. При комплексному підході захист системи вкладається в ОС під час проектування архітектури і є частиною ОС. Плюсом такого підходу є те, що захист, створений комплексним підходом, взаємодіє

один з одним і надійніше допомагає організовувати захист інформації. Під час розробки підсистема проходить перевірку на сумісність та конфліктів між частинами підсистеми захисту не відбувається. Головним здобутком такої підсистеми захисту є те, що при збоях, викликаних зловмисником, система не дозволяє вимкнути систему захисту. В мобільних ОС широко використовують рішення, апробовані на універсальних ОС.

Список використаних джерел:

1. Т*анненбаум Э.* Современные операционные системы. СПб. : Питер, 2006, 1040 с.

2. Проскурин В. Г. Защита в операционных системах. Учебное пособие для вузов. М. : Горячая линия – Телеком, 2014. 192 с.

3. Derrick Rountree, Security for Microsoft Windows System Administrators Introduction to Key Information Security Concepts, Syngress, 211 p., 2011.

4. Artes, N.O., and S.M. Elsakov. "Protection System of Applications on 'Windows' Platform on the Basis of Activity Profile". *Journal of Computational and Engineering Mathematics.* 3, no. 3 (2016): 3–9. https://doi.org/10.14529/jcem160301.

5. HU, Hong-yin, Feng YAO, and Cheng-wan HE. "Solution of Windows Files Security Protection Based on File System Filter Driver". *Journal of Computer Applications.* 29, no. 1 (June 25, 2009): 168–171. https://doi.org/10.3724/sp.j.1087.2009.00168.

6. Küenzlen, Jürgen, Eckehard Scheller, and Hermann Hamm. "Fixing of Windows with Fall Protection / Befestigung von Absturzsichernden Fensterelementen". Mauerwerk 20, no. 6 (December 2016): 423–444. https://doi.org/10.1002/dama.201600714.

7. Ільєнко А.В., Ільєнко С.С., Куліш Т.М. Перспективні методи захисту операційної системи WINDOWS. *Кібербезпека. Освіта, наука, техніка.* № 4(8). 2020. С. 124- 132.

8. Зерко А., Оксіюк О. Аналіз питань захисту інформації в операційних системах на прикладах захищених операційних систем. Геометричне моделювання та інформаційні технології. 2017. № 1 (3). С. 53-55.

9. Бойко В.Д., Василенко М.Д. Відкриті системи і протоколи взаємодії в контексті кібербезпеки «розумного міста». *Безпека та виклики сучасності: ризики та кібербезпека в період пандемії безпека в сучасному світі* : матеріали II Всеукраїнської науково-практ. конф. (м. Одеса, 20 листоп. 2020 р.) / за ред. О. В. Дикого. Одеса : Видавничий дім «Гельветика», 2020. С. 99-106.

10. Бойко В. Д., Василенко М. Д., Слатвінська В. М. Версіонування файлової системи для боротьби з програмами-вимагачами. Тези VIII Міжнар. науково-техн. конф. *«Інформатика, управління та штучний інтелект»* (м. Харків, 16–19 листоп. 2021 р.). Харків: НТУ «ХПІ», 2021. С. 9.

11. Бойко В.Д., Василенко М.Д., Новіков В.П., Рачук В.О. «Розумне місто» в контексті розвитку технологій блокчейн. *Комунальне господарство міст. Серія : технічні науки та архітектура.* Харків, 2021. Вип. 3 (163). С. 152-158.

12. Бойко В.Д., Василенко М.Д., Слатвінська В.М. Живучість та стійкість функціонування компонентів інформаційних систем розумного міста. Науково-технічний збірник *«Комунальне господарство міст». Серія: технічні науки та архітектура*. Харків, 2021. Вип. 6 (166). С. 20-27.

13. Василенко М.Д., Рачук В.О. Слатвінська В.М. Шкідливі програми в контексті розуміння комп'ютерної вірусології та техніко-правової змагальності: міждисциплінарне дослідження. *Наукові праці Національного університету «ОЮА».* Т. 28. Одеса : 2021. С. 28-36.

14. Android отметила 5-летие. URL: https://www.cybersecurity.ru/os/ 163693.html

References:

1. Tannenbaum Je. (2006). Sovremennye operacionnye sistemy [Modern operating systems]. SPb. : Piter, 1040 [in Russian].

2. Proskurin V. G. (2014). Zashhita v operacionnyh sistemah [Protection in operating systems]. Uchebnoe posobie dlja vuzov. M. : Gorjachaja linija – Telekom, 192 [in Russian].

3. Derrick Rountree (2011). Security for Microsoft Windows System Administrators Introduction to Key Information Security Concepts, Syngress, 211.

4. Artes, N.O., Elsakov S.M. (2016). "Protection System of Applications on 'Windows' Platform on the Basis of Activity Profile." *Journal of Computational and Engineering Mathematics.* 3, 3: 3–9. https://doi.org/10.14529/jcem160301.

5. HU, Hong-yin, Feng YAO, and Cheng-wan HE. (2009). "Solution of Windows Files Security Protection Based on File System Filter Driver." *Journal of Computer Applications.* 29, 1: 168–171. https://doi.org/10.3724/sp.j.1087.2009.00168.

6. Küenzlen, Jürgen, Eckehard Scheller, and Hermann Hamm. (2016). "Fixing of Windows with Fall Protection / Befestigung von Absturzsichernden Fensterelementen." Mauerwerk 20, 6: 423–444. https://doi.org/10.1002/dama.201600714.

7. Ilienko A.V., Ilienko S.S., Kulish T.M. (2020). Perspektyvni metody zakhystu operatsiinoi systemy WINDOWS [Perspective methods of protecting the WINDOWS operating system]. *Kiberbezpeka. Osvita, nauka, tekhnika – Cybersecurity. Education, science, technology*. 4(8). 124-132. [in Ukrainian].

8. Zerko A., Oksiiuk O. (2017). Analiz pytan zakhystu informatsii v operatsiinykh systemakh na prykladakh zakhyshchenykh operatsiinykh system [Analysis of information security issues in operating systems on the examples of secure operating systems]. *Heometrychne modeliuvannia ta informatsiini tekhnolohii – Geometric modeling and information technology*, 1, (3), 53-55. [in Ukrainian].

9. Boiko V.D., Vasylenko M.D. (2020). Vidkryti systemy i protokoly vzaiemodii v konteksti kiberbezpeky «rozumnoho mista» [Open systems and interaction protocols in the context of cybersecurity of the "smart city"]. Bezpeka ta vyklyky suchasnosti: ryzyky ta kiberbezpeka v period pandemii bezpeka v suchasnomu sviti : materialy II Vseukrainskoi nau-

kovo-prakt. konf. (m. Odesa, 20 lystop. 2020 r.) / za red. O. V. Dykoho. Odesa : Vydav nychyi dim «Helvetyka», 99-106. [in Ukrainian].

10. Boiko V. D., Vasylenko M. D., Slatvinska V. M. (2021). Versionuvannia failovoi systemy dlia borotby z prohramamy-vymahachamy [File system versioning to combat ransomware]. Tezy VIII Mizhnar. naukovo-tekhn. konf. «Informatyka, upravlinnia ta shtuchnyi intelekt». (m. Kharkiv, 16 – 19 lystop. 2021 r.). Kharkiv: NTU «KhPI», 9. [in Ukrainian].

11. Boiko V.D., Vasylenko M.D., Novikov V.P., Rachuk V.O. (2021). «Rozumne misto» v konteksti rozvytku tekhnolohii blokchein ["Smart city" in the context of blockchain technology development]. *Komunalne hospodarstvo mist. Seriia: tekhnichni nauky ta arkhitektura – Municipal economy of cities. Series: technical sciences and architecture*. Kharkiv, 3 (163), 152-158. [in Ukrainian].

12. Boiko V.D., Vasylenko M.D., Slatvinska V.M. (2021). Zhyvuchist ta stiikist funktsionuvannia komponentiv informatsiinykh system rozumnoho mista [Survivability and sustainability of smart city information system components]. *Naukovo-tekhnichnyi zbirnyk «Komunalne hospodarstvo mist». Seriia: tekhnichni nauky ta arkhitektura – Municipal economy of cities. Series: technical sciences and architecture*. Kharkiv, 6 (166), 20-27. [in Ukrainian].

13. Vasylenko M.D., Rachuk V.O. Slatvinska V.M. (2021). Shkidlyvi prohramy v konteksti rozuminnia kompiuternoi virusolohii ta tekhniko-pravovoi zmahalnosti: mizhdystsyplinarne doslidzhennia [Malware in the context of understanding computer virology and technical-legal competition: an interdisciplinary study]. *Naukovi pratsi Natsionalnoho universytetu «OIuA» – Scientific works of the National University «OSA»*. T. 28. Odesa: 28-36. [in Ukrainian].

14. Android otmetyla 5-letye [Android celebrated its 5th anniversary]. Retrieved from https://www.cybersecurity.ru/os/ 163693.html [in Russian].