УДК 004.056.5:004.451

https://doi.org/10.52058/3041-1793-2025-12(17)-306-315

Ковальова Тетяна Іванівна кандидат юридичних наук, доцент,доцент кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки Київського інституту Національної гвардії України, м. Київ, http://orcid.org/0009-0001-0668-3047

Скоморохов Владислав Андрійович слухач 144 М навчальної групи, кафедри державної безпеки факультету забезпечення державної безпеки, Київський інститут Національної гвардії України, https://orcid.org/0009-0006-9451-5815

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМ ANDROID ТА IOS

Анотація. У статті наведено комплексний аналіз сучасних загроз інформаційній безпеці мобільних операційних систем Android та iOS, що безпосередньо пов’язані з отриманням зловмисниками несанкціонованих підвищених привілеїв (root-прав та jailbreak), а також із розповсюдженням шкідливого програмного забезпечення типу програм-вимагачів. Обґрунтовано високу актуальність досліджуваної проблеми в умовах стрімкого зростання частки мобільних пристроїв у доступі до критично важливих цифрових сервісів, зокрема систем мобільного банкінгу, корпоративних платформ електронного документообігу та хмарних сховищ, де обробляються чутливі персональні й біометричні дані користувачів.

На основі детального аналізу фахових наукових джерел, аналітичних звітів провідних міжнародних компаній у сфері кібербезпеки та відкритої статистики інцидентів здійснено порівняльний огляд архітектурних особливостей та вбудованих механізмів захисту екосистем Android та iOS. Виявлено їхні ключові сильні та вразливі сторони в контексті ризиків ескалації привілеїв. Окреслено та систематизовано типові вектори атак і сценарії компрометації пристроїв із активованим рут-доступом та «зламаних» (jailbroken) смартфонів. Зокрема, розглянуто загрози, що надходять через альтернативні неофіційні крамниці додатків, інфіковані оновлення, експлойти вразливостей нульового дня в системних службах та методи соціальної інженерії.

Подано структуровану класифікацію сучасних мобільних програм-вимагачів (блокувальників екрана та криптовимагачів), детально описано їхні моделі монетизації, канали масового поширення та технічні особливості алгоритмів шифрування або блокування доступу до файлової системи.

Запропоновано комплекс організаційно-технічних заходів протидії, що включає впровадження суворих політик заборони рутування та джейлбрейку в корпоративному периметрі, обов'язкове використання рішень класу MDM (Mobile Device Management) та EDR (Endpoint Detection and Response), посилення контролю легітимності джерел інсталяції програмного забезпечення, налагодження регулярного резервного копіювання критичних даних, а також підвищення рівня кібергігієни та обізнаності користувачів щодо специфіки мобільних загроз.

Наукова новизна роботи полягає в узагальненні еволюції векторів атак на платформи Android та iOS через призму несанкціонованої ескалації привілеїв і діяльності програм-вимагачів, а також у формуванні цілісної моделі ризиків і розробленні практичних рекомендацій, які можуть бути використані для побудови ешелонованих систем захисту мобільної інфраструктури підприємств.

Ключові слова: інформаційна безпека; мобільні операційні системи; Android; iOS; root; jailbreak; програми-вимагачі; мобільні загрози.

Kovalova Tetiana Ivanivna Candidate of Law, Associate Professor, Associate Professor of the Department of State Security, Faculty of State Security, Kyiv Institute of the National Guard of Ukraine, Kyiv, https://orcid.org/0009-0001-0668-3047

Skomorokhov Vladyslav Andriiovych Student of 144M Study Group, Department of State Security, Faculty of State Security, Kyiv Institute of the National Guard of Ukraine, Kyiv, https://orcid.org/0009-0006-9451-5815

MODERN INFORMATION SECURITY THREATS TO ANDROID AND iOS MOBILE OPERATING SYSTEMS

Abstract. The article examines modern information security threats to Android and iOS mobile operating systems related to obtaining elevated privileges (root and jailbreak) and the spread of ransomware-type malicious software. The relevance of the issue is substantiated in the context of the growing share of mobile devices used to access digital services, particularly financial, corporate, and cloud services.

Based on the analysis of scientific sources, reports from leading cybersecurity companies, and publicly available incident statistics, a comparative overview of the built-in security mechanisms in Android and iOS is provided, highlighting their strengths and vulnerabilities in the context of privilege escalation. Typical scenarios of device compromise involving root access and jailbroken smartphones are outlined, including through alternative app stores, malicious updates, exploits in system services, and social engineering. A structured classification of mobile

ransomware is presented, describing their monetization models, distribution channels, and the specifics of data encryption or access blocking. A set of organizational and technical countermeasures is proposed, including corporate policies prohibiting rooting and jailbreaking, the use of MDM/EDR-class solutions, strengthened control over application installation sources, implementation of critical data backups, and raising user awareness about mobile-specific threats.

The scientific novelty of the work lies in summarizing the evolution of threats to Android and iOS through the lens of privilege escalation and ransomware, as well as in developing a comprehensive risk model and recommendations aimed at practical application in mobile infrastructure protection systems.

Keywords: information security; mobile operating systems; Android; iOS; root; jailbreak; ransomware; mobile threats.

Постановка проблеми. Стрімке зростання частки мобільних пристроїв у структурі цифрового трафіку, поширення мобільного банкінгу, цифрових гаманців, державних послуг та корпоративних застосунків призвели до того, що смартфони на базі Android та iOS перетворилися на ключову ціль для кіберзлочинців. Для Національної гвардії України, діяльність якої пов’язана з виконанням завдань із забезпечення державної безпеки, охорони об’єктів критичної інфраструктури, участі в операціях оборонного характеру та підтриманні правопорядку, питання безпеки мобільних пристроїв набуває особливої актуальності. Мобільний пристрій одночасно поєднує особисті дані користувача, доступ до фінансових операцій, корпоративної пошти й хмарних сховищ.

Мобільні телефони військовослужбовців НГУ використовуються для доступу до службової кореспонденції, інформаційних ресурсів, службових месенджерів, систем двофакторної автентифікації та в окремих випадках – навіть до елементів службового документообігу. Компрометація пристрою військовослужбовця означає ризик витоку оперативної інформації, розкриття місцеперебування підрозділів, втручання у канали комунікації, стеження за рухом сил і засобів НГУ, що безпосередньо загрожує ефективності та безпеці виконання службово-бойових завдань.

Особливо небезпечними є загрози, пов’язані з отриманням підвищених привілеїв (root на Android та jailbreak на iOS), оскільки вони дають змогу обійти вбудовані механізми безпеки операційних систем, модифікувати системні компоненти, приховувати шкідливий код і блокувати роботу антивірусних та захисних засобів. На цьому тлі активно розвивається клас мобільного шкідливого ПЗ типу програм-вимагачів (ransomware), що шифрують або блокують доступ до даних і екрану пристрою з подальшою вимогою викупу. У військовому середовищі та серед силових структур такі втручання можуть бути використані для встановлення шпигунських модулів, віддаленого керування смартфоном або інсталяції програм-вимагачів, здатних

заблокувати пристрій чи шифрувати службову інформацію. Це може призвести до зриву службових операцій, компрометації персоналу, порушення стійкості комунікацій, що перетворює проблему мобільної безпеки з технічної на елемент воєнної та національної безпеки.

Проблема у сфері мобільної безпеки полягає в тому, що традиційні моделі захисту, спроєктовані для стаціонарних систем, не враховують специфіку мобільних платформ, їхніх магазинів додатків, моделей оновлення, користувацької поведінки та практики рутування/джейлбрейку. Це зумовлює необхідність поглибленого аналізу еволюції загроз для Android та iOS з акцентом на ескалації привілеїв і програмах-вимагачах, а також розробки комплексних рекомендацій щодо їх нейтралізації.

Аналіз останніх досліджень і публікацій. Проблематика захисту мобільних операційних систем Android та iOS активно досліджується як українськими, так і зарубіжними авторами. У вітчизняних працях (наприклад, І. Горбенко, Т. Гриненко, О. Додонов, С. Каденко та ін.) розглядаються загальні підходи до побудови систем захисту інформації в інформаційно-телекомунікаційних системах, описуються базові моделі загроз, механізми криптографічного захисту, а також методи виявлення інформаційних атак. Окремі дослідники аналізують особливості мобільного шкідливого ПЗ, але, як правило, зосереджуються на загальній класифікації вірусів і троянів без детального розгляду наслідків рутування/джейлбрейку для цілісності системи захисту.

Серед зарубіжних авторів значний внесок у дослідження безпеки Android зробили W. Enck, A. P. Felt, H. Chen, які вивчали моделі дозволів, уразливості в механізмах ізоляції застосунків та проблеми конфіденційності користувачів. Дослідження M. Bianchi, K. Allix, L. Li та інших присвячені статичному й динамічному аналізу мобільних шкідливих програм, виявленню прихованих привілеїв, а також класифікації сімейств мобільного malware, включно з програмами-вимагачами. Низка робіт досліджує специфіку jailbreak для iOS, механізми експлуатації вразливостей ядра та підсистем безпеки, а також наслідки встановлення неавторизованих застосунків поза офіційним App Store.

Разом з тим, попри значний обсяг публікацій, низка аспектів залишається недостатньо опрацьованою. По-перше, часто окремо розглядаються або механізми ескалації привілеїв, або мобільні програми-вимагачі, тоді як взаємозв’язок між рутуванням/джейлбрейком і збільшенням ефективності ransomware-атак на мобільні платформи аналізується фрагментарно. По-друге, у багатьох роботах відсутня порівняльна оцінка підходів до захисту в Android та iOS саме в контексті root/jailbreak-стану пристрою та його впливу на обхід вбудованих захисних механізмів. По-третє, бракує узагальнених рекомендацій, які одночасно враховували б технічні, організаційні й поведінкові фактори (політики BYOD, використання MDM/EDR-рішень, користувацькі практики

тощо). Це зумовлює необхідність комплексного дослідження еволюції загроз для Android та iOS з фокусом на ескалації привілеїв і програмах-вимагачах та формування цілісної моделі ризиків для мобільної інфраструктури.

Мета статті є аналіз еволюції загроз інформаційній безпеці мобільних операційних систем Android та iOS, пов'язаних з отриманням підвищених привілеїв (root/jailbreak) та поширенням програм-вимагачів, а також у розробці комплексних рекомендацій щодо мінімізації відповідних ризиків для користувачів і організацій.

Виклад основного матеріалу. Мобільні операційні системи Android та iOS спочатку проєктувалися за багаторівневою моделлю захисту, що включає ізоляцію застосунків у «пісочницях», систему дозволів, захищені канали оновлення, перевірку цілісності ядра та системних компонентів, а також контроль джерел інсталяції програм. Для Android ключову роль відіграють механізми Google Play Protect, перевірка підписів застосунків і модель дозволів на рівні маніфеста, тоді як в iOS базою безпеки є апаратне коріння довіри Secure Enclave, жорстка політика підписування та верифікації коду й закритість екосистеми з єдиним офіційним магазином App Store [1, с. 98]. Попри це, Android залишається основною мішенню атак через свою домінуючу частку ринку (орієнтовно близько 70 % проти приблизно 30 % у iOS) та фрагментацію версій і політик оновлення, що ускладнює підтримання однорідного рівня захисту на різних пристроях [2, с. 31]. За даними аналітичних звітів компаній з кібербезпеки, у 2023 році кількість атак на мобільні пристрої сягнула десятків мільйонів інцидентів, причому саме Android найчастіше виступає платформою поширення шкідливого програмного забезпечення, у тому числі програм-вимагачів [3, с. 168].

Отримання прав суперкористувача (root-доступ у Android) або виконання jailbreak в iOS означає свідоме зняття частини вбудованих обмежень безпеки та відкриває можливість виконання коду з підвищеними привілеями, модифікації системних бібліотек, зміни параметрів політик безпеки та інсталяції неавторизованих модулів [4, с. 282]. Такий стан пристрою знижує ефективність роботи антивірусних рішень, механізмів контролю цілісності та корпоративних засобів керування мобільністю, а також спрощує приховування шкідливого коду. У цьому контексті доцільно трактувати root та jailbreak не як нейтральну «кастомізацію», а як мультиплікатор ризику, що понижує ефективність базової моделі безпеки, спрощує приховування шкідливих компонентів і підвищує ймовірність успішної інсталяції та стійкого закріплення програм-вимагачів на пристрої [5, с. 104]. З огляду на це пропонується умовно поділяти мобільні пристрої на три стани: стандартний, коли використовується штатна конфігурація без root/jailbreak та офіційні магазини додатків; проміжний, за якого користувач дозволяє встановлення застосунків із невідомих джерел, активно використовує сумнівні VPN та проксі-сервіси; і високоризиковий, коли наявні root/jailbreak, кастомні

прошивки або модифіковане ядро. Перехід пристрою до високоризикової категорії різко збільшує площу атаки, оскільки шкідливий код отримує прямий доступ до файлової системи, може перехоплювати трафік і втручатися в механізми автентифікації та шифрування.

На основі аналізу спеціалізованих публікацій і звітів сформовано класифікацію мобільних програм-вимагачів, що враховує спосіб впливу на дані та користувача. До першої групи належать так звані screen-locker ransomware, які блокують екран пристрою та відображають вікно з вимогою викупу, часто маскуючись під «штрафи» від правоохоронних органів; у цьому разі дані, як правило, не шифруються, але користувач втрачає доступ до інтерфейсу [6, с. 39]. Друга група – crypto-ransomware, які шифрують користувацькі файли (фотографії, документи, медіа) або певні каталоги файлової системи, що робить відновлення без відповідного ключа практично неможливим. До третьої групи можна віднести гібридні рішення, які одночасно блокують екран, шифрують дані та доповнюються функціональністю шпигунського ПЗ, наприклад можливістю витоку контактів, листування або одноразових паролів. Окремо виділяються випадки інтеграції функцій шифрування й шантажу в banking Trojan та інші види шкідливого ПЗ, де програма-вимагач виступає лише однією з опцій монетизації зловмисників [7, с. 204]. Статистичні дані свідчать, що кількість виявлених інсталяційних пакетів мобільних програм-вимагачів упродовж останніх років зростає, причому найбільш уразливою платформою залишається Android через підтримку встановлення APK-файлів зі сторонніх джерел та високу популярність піратського контенту [3, с. 141; 8].

Найбільш поширеними сценаріями компрометації є встановлення застосунків із неофіційних магазинів або вебсайтів із піратським програмним забезпеченням, використання «зламаних» версій популярних програм чи ігор, перехід за фішинговими посиланнями в SMS-повідомленнях та месенджерах, а також експлуатація вразливостей браузера чи вбудованих компонентів відображення вебконтенту. У разі рутованих або джейлбрейк-пристроїв додатковий ризик становить інсталяція модулів і «твікерів», що містять прихований шкідливий код і можуть отримувати системні привілеї без відома користувача [5, 105; 7]. Відкритість Android, яка є перевагою з погляду гнучкості та кастомізації, водночас створює суттєві труднощі для централізованого контролю стану пристрою, особливо в корпоративному середовищі, де один скомпрометований смартфон може стати точкою входу до внутрішніх ресурсів організації [2, с. 241; 4, с. 284].

Для iOS ситуація відрізняється більш жорстким контролем підписування коду та джерел інсталяції, що істотно обмежує масове поширення шкідливих додатків. Більшість успішних атак з використанням програм-вимагачів фіксуються на пристроях із jailbreak або реалізуються завдяки соціальній інженерії, коли користувач сам надає застосунку надмірні дозволи, вклю-

чаючи доступ до файлів, фотографій і хмарних сховищ [1, с. 134; 6, с. 39]. Водночас зростання ролі хмарних сервісів та резервного копіювання призводить до появи нових векторів атак: шифрування синхронізованих даних, погрози публікації конфіденційної інформації, комбінування шифрування та витоку даних як додаткового важеля тиску на жертву.

Узагальнюючи результати дослідження, доцільно розглядати загальний ризик для мобільного пристрою як функцію трьох груп параметрів: базової стійкості операційної системи й частоти її оновлення, рівня привілеїв, наданих користувачем або отриманих зловмисником (наявність root/jailbreak, кастомних модулів, модифікованої прошивки), а також поведінкових факторів, які відображають цифрову гігієну користувача й організації (джерела інсталяції програм, ставлення до фішингу, практика резервного копіювання). У найризикованішій конфігурації поєднуються модифікований стан пристрою та низька обізнаність користувача щодо мобільних загроз, що створює сприятливі умови для успішної реалізації атак із використанням програм-вимагачів.

Запропоновані напрями удосконалення захисту охоплюють як технічні, так і організаційні та освітні заходи. До технічних належать упровадження політик категоричної відмови від root/jailbreak для банківських, платіжних і державних застосунків, використання механізмів перевірки стану пристрою (attestation), розгортання систем керування мобільними пристроями й засобів виявлення та реагування (MDM/EDR), які дозволяють автоматично визначати модифіковані смартфони та блокувати їхній доступ до корпоративних ресурсів [4, с. 312; 8]. Важливим компонентом є посилення контролю джерел програмного забезпечення, обмеження встановлення додатків офіційними магазинами та корпоративними каталогами, регулярний аудит дозволів застосунків і примусове застосування шифрування даних на пристрої. Організаційні заходи включають розробку та актуалізацію політик використання особистих мобільних пристроїв у межах концепції BYOD, формування планів реагування на інциденти з урахуванням можливих сценаріїв зараження програмами-вимагачами та визначення процедур відновлення після атаки. Освітній компонент спрямований на підвищення обізнаності користувачів щодо ризиків рутування, інсталяції піратських застосунків, використання сумнівних VPN-сервісів, а також щодо типових ознак зараження та правил поведінки у випадку появи вимог викупу на екрані смартфона [1, с. 139; 5, с. 106; 7, с. 299].

Для НГУ особливе значення має ризик інфікування пристроїв під час використання особистих телефонів у межах концепції BYOD, що поширена серед військовослужбовців у зоні дислокації та на місцях виконання завдань. Встановлення застосунків із неофіційних джерел, експлуатація вразливостей браузера, підключення до незахищених мереж Wi-Fi чи використання VPN неперевірених провайдерів може стати точкою входу для кібератаки противника. Ведення бойових дій та гібридних операцій російсько-української

війни мобільні програми-вимагачі та шпигунські модулі дедалі частіше використовуються як інструмент кібершпигунства, виявлення пересування військових колон, збору голосових повідомлень, зняття координат, віддаленої активації камери чи мікрофона. Наявність root/jailbreak значно спрощує зловмиснику реалізацію таких сценаріїв.

Отже, підвищені привілеї на мобільних пристроях можуть бути використані для:

- встановлення модулів прихованого аудіо- чи відеоспостереження;
- компрометації службових чатів і каналів зв'язку;
- доступу до службових фото/відеоматеріалів, знятих на місці подій;
- геолокаційного контролю за військовослужбовцем та його підрозділом;
- блокування телефонів підрозділів НГУ під час операцій;
- шифрування службових даних і вимагання викупу.

Висновки. Узагальнюючи проведений аналіз, можна сформулювати кілька ключових висновків, що мають теоретичне й практичне значення. Перш за все, ескалація привілеїв через root та jailbreak виступає головним мультиплікатором ризику, оскільки руйнує вихідну модель безпеки Android та iOS і створює сприятливі умови для роботи програм-вимагачів, даючи їм глибокий доступ до системи й даних користувача. Android через домінування на ринку й відкритість екосистеми закономірно залишається основною ціллю мобільних атак, проте iOS також є вразливою за наявності jailbreak та в разі надання застосункам надмірних дозволів, що вимагає однаково серйозного підходу до захисту обох платформ.

У ході дослідження встановлено, що ескалація привілеїв через root/jailbreak є одним із ключових факторів компрометації мобільних систем і створює критично небезпечні умови для діяльності Національної гвардії України. Модифікований стан пристрою у поєднанні з несанкціонованими застосунками та низькою цифровою гігієною користувача може становити пряму загрозу виконанню службово-бойових завдань і впливати на результативність оперативних дій.

Виявлено, що мобільні програми-вимагачі еволюціонують від простих блокувальників екрана до гібридних рішень, які поєднують шифрування даних, шантаж витоком інформації та можливості шпигунського ПЗ, що збільшує потенційні збитки для користувачів. Запропонована модель оцінки ризику, яка враховує параметри операційної системи, рівень привілеїв і поведінкові чинники, дає змогу структурувати загрози та показує, що найвищий рівень небезпеки пов'язаний саме з комбінацією модифікованих пристроїв і низької цифрової гігієни.

Рекомендації та модель оцінки ризиків можуть бути інтегровані в систему кібербезпеки НГУ та використані для: підвищення стійкості службових комунікацій, запобігання витоку оперативної інформації, впровадження ефективних MDM/EDR-рішень у підрозділах, стандартизації політик безпеч-

ного використання мобільних пристроїв у НГУ, підготовки військовослужбовців до сучасних викликів кіберпростору.

Практичне значення роботи полягає в тому, що результати дослідження можуть бути використані сектором безпеки та оборони, державними органами та корпоративними структурами для оновлення політик мобільної безпеки, зокрема для впровадження обов'язкової перевірки стану пристрою перед наданням доступу до критичних сервісів, заборони роботи застосунків на рутованих і джейлбрейк-смартфонах, а також для побудови процедур реагування на інциденти з використанням програм-вимагачів. Перспективами подальших досліджень є розробка автоматизованих методів виявлення ознак root/jailbreak і ранньої детекції ransomware на мобільних пристроях.

Таким чином, забезпечення інформаційної безпеки мобільних операційних систем Android і iOS є невід'ємним елементом системи державної та військової безпеки, а результати дослідження становлять практичну цінність для зміцнення кіберстійкості Національної гвардії України.

Література:

1. Андрєєв А. М., Пшенична О. С. Методологія наукових досліджень : навчальний посібник для здобувачів ступеня вищої освіти магістра спеціальності «Середня освіта» (ОП «Середня освіта (Інформатика)»). Запоріжжя : Запорізький національний університет, 2024. 145 с.

2. Антонюк А. О. Основи захисту інформації в автоматизованих системах. Київ : КМ Академія, 2006. 244 с.

3. Арістова І. В., Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг : монографія. Київ : Право України ; Харків : Право, 2013. 184 с.

4. Вимірювання в освіті : підручник / за ред. О. В. Авраменка. Кіровоград : Лисенко В. Ф., 2011. 360 с.

5. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні // Підприємництво, господарство і право. 2019. № 9. С. 100–108.

6. Бондаренко О. М. Сучасні інноваційні технології навчання у старшій школі: теорія і практика // Педагогічний альманах. 2022. № 4. С. 37–42.

7. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Львів : 2024. 320 с.

8. Василішин С. Удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи // Економіка та суспільство. 2021. № 1. URL: https://visnykj.wunu.edu.ua/index.php/visnykj/article/view/1218 (дата звернення: 04.10.2024).

9. Віннікова І. І., Марчук С. В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними // Ефективна економіка. 2019. № 6. URL: https://chmnu.edu.ua/wp-content/uploads/2019/07/Vinnikova-I.I.-Marchuk-S.V..pdf (дата звернення: 04.10.2024).

10. Всеосвіта. Національна освітня платформа. URL: https://vseosvita.ua/ (дата звернення: 04.10.2024).

References:

1. Andreiev, A. M., Pshenychna, O. S. (2024). *Metodolohiia naukovykh doslidzhen* (Training manual for Master's students of the specialty "Secondary Education" (OP "Secondary Education (Informatics)")). Zaporizhzhia: Zaporizhzhia National University [in Ukrainian].

2. Antoniuk, A. O. (2006). *Osnovy zakhystu informatsii v avtomatyzovanykh systemakh* (Fundamentals of information protection in automated systems). Kyiv: KM Akademiia [in Ukrainian].

3. Aristova, I. V., Sulatskyi, D. V. (2013). *Informatsiina bezpeka liudyny yak spozhyvacha telekomunikatsiinykh posluh* (Information security of a person as a consumer of telecommunication services) (Monograph). Kyiv: Pravo Ukrainy; Kharkiv: Pravo [in Ukrainian].

4. Avramenko, O. V. (Ed.). (2011). *Vymiriuvannia v osviti* (Measurements in education) (Textbook). Kirovohrad: Lysenko V. F. [in Ukrainian].

5. Bakalinska, O., Bakalynskyi, O. (2019). Pravove zabezpechennia kiberbezpeky v Ukraini (Legal support of cybersecurity in Ukraine). *Pidpryiemnytstvo, hospodarstvo i pravo* (Entrepreneurship, Economy and Law), (9), 100–108 [in Ukrainian].

6. Bondarenko, O. M. (2022). Suchasni innovatsiini tekhnolohii navchannia u starshii shkoli: teoriia i praktyka (Modern innovative learning technologies in high school: theory and practice). *Pedahohichnyi almanakh*(Pedagogical Almanac), (4), 37–42 [in Ukrainian].

7. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V. (2024). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt* (Information and cybersecurity: socio-technical aspect) (Textbook). Lviv [in Ukrainian].

8. Vasylishyn, S. (2021). Udoskonalennia vazheliv upravlinnia dyzhytalizatsiinymy ryzykamy ekonomichnoi bezpeky ta formuvannia kiberbezpeky oblikovoi systemy (Improvement of levers for managing digitalization risks of economic security and formation of cybersecurity of the accounting system). *Visnyk ekonomichnoi bezpeky*(Bulletin of Economic Security), (1). Retrieved from https://visnykj.wunu.edu.ua/index.php/visnykj/article/view/1218 [in Ukrainian].

9. Vinnikova, I. I., Marchuk, S. V. (2019). Kiber-ryzyky yak odyn iz vydiv suchasnykh ryzykiv u diialnosti maloho ta serednoho biznesu ta upravlinnia nymy (Cyber-risks as one of the types of modern risks in the activities of small and medium-sized businesses and their management). *Efektyvna ekonomika* (Effective Economy), (6). Retrieved from https://chmnu.edu.ua/wp-content/uploads/2019/07/Vinnikova-I.I.-Marchuk-S.V..pdf [in Ukrainian].

10. Vseosvita. Natsionalna osvitnia platforma (National educational platform). (n.d.). Retrieved from https://vseosvita.ua/ [in Ukrainian].