УДК 342:351

https://doi.org/10.52058/3041-1254-2025-12(22)-1305-1315

Радзівілов Григорій Данилович заступник начальника з наукової роботи, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, кандидат технічних наук, професор, https://orcid.org/0000-0002-6047-1897

ДЕРЖАВНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ МОБІЛЬНИХ ПЛАТФОРМ ANDROID ТА IOS

Анотація. У статті розглядаються актуальні аспекти державного управління інформаційною безпекою мобільних платформ Android та iOS, що набувають особливого значення в умовах стрімкого розвитку цифрових технологій та зростання залежності від мобільних пристроїв у повсякденному житті, бізнесі та державному управлінні. Увага акцентується на тому, що мобільні платформи Android і iOS є найпоширенішими операційними системами для смартфонів і планшетів, забезпечуючи доступ до широкого спектра сервісів, включаючи банківські послуги, електронну комерцію, соціальні мережі та корпоративні ресурси.

Автор аналізує сучасні виклики для інформаційної безпеки цих платформ, зокрема ризики, пов'язані з рутуванням (root) пристроїв Android та джейлбрейком (jailbreak) iOS, які призводять до значного зниження рівня захисту мобільних пристроїв. Висвітлюються загрози, пов'язані з використанням шкідливого програмного забезпечення, зокрема програм-вимагачів, фішингових атак, експлуатації вразливостей системних компонентів та неконтрольованого поширення шкідливих APK-файлів і неавторизованих додатків.

Окрему увагу приділено аналізу механізмів безпеки Android та iOS. У статті описано багаторівневі системи захисту, які включають ізоляцію додатків у «пісочницях», перевірку підписів програмного забезпечення, механізми контролю доступу та оновлення, а також апаратні засоби захисту, такі як Secure Enclave в iOS. Водночас наголошується на проблемах фрагментації версій Android, що створює труднощі для забезпечення однакового рівня безпеки на різних пристроях, а також на ризиках, пов'язаних із відкритістю екосистеми Android.

У статті запропоновано умовну класифікацію мобільних пристроїв за рівнем ризику: стандартний стан (використання офіційних магазинів додатків без рутування чи джейлбрейку), проміжний стан (встановлення програм із невідомих джерел, використання сумнівних сервісів) та високоризиковий стан (root/jailbreak, кастомні прошивки, модифіковане ядро). Показано, що перехід до високоризикової категорії значно збільшує ймовірність успішної реалізації кібератак.

На основі аналізу спеціалізованих джерел і звітів сформовано класифікацію програм-вимагачів, які спрямовані на мобільні платформи, залежно від способів впливу на дані та користувача. Виділено screen-locker ransomware, які блокують екран пристрою, crypto-ransomware, що шифрують дані користувачів, та гібридні програми, які поєднують функції блокування, шифрування та шпигунського ПЗ.

Також у статті обґрунтовано необхідність розробки ефективної державної політики у сфері інформаційної безпеки мобільних платформ. Зокрема, пропонується впровадження нормативно-правових актів, які регулюють використання мобільних пристроїв у державному секторі, створення національних стандартів для управління ризиками, пов'язаними з мобільними платформами, а також розробка рекомендацій для користувачів і організацій щодо мінімізації кіберзагроз.

У статті також досліджено сучасні тенденції у сфері захисту мобільних платформ, зокрема впровадження багатофакторної аутентифікації, використання штучного інтелекту для виявлення кіберзагроз, шифрування даних, а також важливість регулярних оновлень програмного забезпечення. Окрему увагу приділено ролі користувачів у забезпеченні інформаційної безпеки, зокрема їх обізнаності про ризики та дотриманню правил кібергігієни.

Результати дослідження підкреслюють необхідність комплексного підходу до захисту мобільних платформ, що включає співпрацю між розробниками програмного забезпечення, виробниками пристроїв, урядами та користувачами. Запропоновані рекомендації спрямовані на підвищення рівня інформаційної безпеки мобільних платформ Android та iOS, що є важливим кроком у забезпеченні безпеки персональних даних у сучасному цифровому середовищі.

Ключові слова: державне управління, інформаційна безпека, мобільні платформи, Android, iOS, кіберзагрози, мобільні пристрої, шкідливе програмне забезпечення, кібербезпека.

Radzivilov Hryhorii Danilovich Deputy Head for Scientific Work, Kruty Heroes Military Institute of Telecommunications and Information Technologies, candidate of technical sciences, professor, https://orcid.org/0000-0002-6047-1897

STATE MANAGEMENT OF INFORMATION SECURITY OF ANDROID AND IOS MOBILE PLATFORMS

Abstract. The article discusses the current aspects of public administration regarding the information security of mobile platforms Android and iOS, which are gaining particular significance amid the rapid development of digital technologies and the growing dependence on mobile devices in everyday life, business, and public administration. It emphasizes that Android and iOS mobile platforms are the most widely used operating systems for smartphones and tablets, providing access to a wide

range of services, including banking, e-commerce, social media, and corporate resources.

The author analyzes the modern challenges to information security on these platforms, including risks associated with the rooting of Android devices and jailbreaking of iOS devices, which lead to a significant reduction in the protection levels of mobile devices. Threats related to the use of malware, such as ransomware, phishing attacks, exploitation of vulnerabilities in system components, and uncontrolled distribution of malicious APK files and unauthorized applications are highlighted.

Special attention is given to analyzing the security mechanisms of Android and iOS. The article describes multi-layered protection systems that include application isolation in "sandboxes," software signature verification, access control mechanisms, and updates, as well as hardware protection features such as Secure Enclave in iOS. At the same time, it emphasizes the issues of Android version fragmentation, which creates difficulties in ensuring a uniform security level across different devices, as well as risks related to the openness of the Android ecosystem.

The article proposes a conditional classification of mobile devices according to risk levels: standard state (using official app stores without rooting or jailbreaking), intermediate state (installing apps from unknown sources, using dubious services), and high-risk state (root/jailbreak, custom firmware, modified kernels). It is shown that moving to the high-risk category significantly increases the likelihood of successful cyberattacks.

Based on the analysis of specialized sources and reports, a classification of ransomware targeting mobile platforms is formed, depending on the methods of affecting data and users. This includes screen-locker ransomware that block the device's screen, crypto-ransomware that encrypt user data, and hybrid programs that combine blocking, encryption, and spyware functions.

The article also justifies the need for developing effective public policy in the sphere of information security for mobile platforms. In particular, it suggests the implementation of regulations governing the use of mobile devices in the public sector, the creation of national standards for managing risks associated with mobile platforms, and the development of recommendations for users and organizations to minimize cyber threats.

Current trends in mobile platform protection are also investigated, including the implementation of multi-factor authentication, the use of artificial intelligence to detect cyber threats, data encryption, and the importance of regular software updates. Special attention is given to the role of users in ensuring information security, particularly their awareness of risks and adherence to cyber hygiene practices.

The research results underscore the necessity for a comprehensive approach to protecting mobile platforms, which includes collaboration among software developers, device manufacturers, governments, and users. The proposed recommendations aim to

enhance the level of information security for Android and iOS mobile platforms, which is an important step in ensuring the safety of personal data in today's digital environment.

Keywords: public administration, information security, mobile platforms, Android, IOS, cyber threats, mobile devices, malware, cybersecurity.

Постановка проблеми Сучасний розвиток цифрових технологій та стрімке зростання популярності мобільних пристроїв, що працюють на операційних системах Android та iOS, створили нові можливості для обробки, зберігання та передачі інформації. Мобільні платформи стали невід'ємною частиною повсякденного життя, забезпечуючи доступ до банківських послуг, електронної пошти, соціальних мереж, хмарних сховищ та інших сервісів. Однак, разом із цим зростає і кількість кіберзагроз, спрямованих на компрометацію конфіденційної інформації, що зберігається на цих пристроях.

Однією з ключових проблем є постійне вдосконалення методів кібератак, серед яких поширення шкідливого програмного забезпечення, фішингові атаки, експлойти, атаки на вразливості мобільних додатків та використання соціальної інженерії. Особливої актуальності набуває проблема фрагментації версій операційної системи Android, що ускладнює своєчасне оновлення безпеки для користувачів. Водночас, хоча iOS демонструє більш закриту екосистему та високий рівень захисту, ця платформа також не є повністю захищеною від кіберзагроз, особливо у випадках використання сторонніх додатків або зламу пристроїв (джейлбрейк).

Зростання кількості мобільних додатків і їх інтеграція у повсякденне життя користувачів створює додаткові ризики, оскільки велика частина таких додатків може містити вразливості або використовуватися для збору конфіденційної інформації. Крім того, уразливість мобільних платформ до атак на критичну інфраструктуру та персональні дані користувачів стає все більш актуальною у контексті зростання обсягу мобільного трафіку та використання мобільних пристроїв у корпоративному секторі.

З огляду на це, постає нагальна потреба у дослідженні сучасних викликів інформаційній безпеці мобільних платформ Android та iOS, а також у розробленні ефективних підходів до забезпечення їх захисту. Вирішення цієї проблеми є важливим не лише для мінімізації ризиків втрати конфіденційної інформації, але й для забезпечення загальної кібербезпеки в умовах зростання цифрових загроз.

Аналіз останніх досліджень і публікацій. Питання захисту мобільних операційних систем Android та iOS є об'єктом активного вивчення як українських, так і зарубіжних науковців. У роботах вітчизняних авторів, таких як І. Горбенко, Т. Гриненко, О. Додонов, С. Каденко та інших, розглядаються основні підходи до побудови систем інформаційної безпеки в інформаційно-

телекомунікаційних системах. Зокрема, вони описують базові моделі загроз, досліджують механізми криптографічного захисту та методи виявлення інформаційних атак. Окремі дослідження присвячені аналізу мобільного шкідливого програмного забезпечення, проте зазвичай акцент робиться на загальній класифікації вірусів і троянів, без детального висвітлення впливу рутування чи джейлбрейку на цілісність системи безпеки.

Серед зарубіжних дослідників значний внесок у вивчення безпеки Android зробили W. Enck, A. P. Felt, H. Chen, які аналізували моделі дозволів, уразливості механізмів ізоляції додатків та питання конфіденційності користувачів. Роботи M. Bianchi, K. Allix, L. Li та інших були присвячені статичному і динамічному аналізу мобільного шкідливого ПЗ, виявленню прихованих привілеїв і класифікації сімейств мобільного malware, зокрема програм-вимагачів. Окремі дослідження детально розглядають специфіку джейлбрейку для iOS, механізми експлуатації вразливостей ядра та підсистем безпеки, а також ризики, пов'язані з використанням неавторизованих додатків, що завантажуються поза межами офіційного App Store.

Попри значну кількість наукових публікацій, окремі аспекти проблематики залишаються недостатньо дослідженими. По-перше, у багатьох роботах механізми ескалації привілеїв і мобільні програми-вимагачі розглядаються окремо, тоді як взаємозв'язок між рутуванням/джейлбрейком та підвищенням ефективності ransomware-атак на мобільні платформи аналізується лише частково й фрагментарно. По-друге, у наукових дослідженнях часто відсутній порівняльний аналіз підходів до забезпечення безпеки в операційних системах Android і iOS у контексті стану root/jailbreak пристрою, а також його впливу на можливість обходу вбудованих механізмів захисту.

По-третє, бракує цілісних рекомендацій, які б одночасно враховували технічні, організаційні та поведінкові аспекти. Наприклад, такі фактори, як політика використання особистих пристроїв у робочих цілях (BYOD), впровадження рішень для управління мобільними пристроями (MDM) та засобів розширеного захисту кінцевих точок (EDR), а також користувацькі практики, не отримують належної уваги.

Ці прогалини у дослідженнях вказують на необхідність комплексного аналізу еволюції загроз для мобільних платформ Android та iOS, з особливим акцентом на ескалації привілеїв і впливі програм-вимагачів. Важливим завданням також є формування інтегрованої моделі ризиків, яка враховуватиме всі аспекти безпеки мобільної інфраструктури.

Мета статті – дослідження сучасних викликів та загроз інформаційній безпеці мобільних платформ Android та iOS, а також обґрунтування підходів до формування ефективної системи державного управління у цій сфері. У статті визначаються ключові аспекти забезпечення безпеки мобільних пристроїв, аналізуються особливості функціонування механізмів захисту операційних

систем Android та iOS, а також вплив рутування та джейлбрейку на зниження рівня інформаційної безпеки.

Особливу увагу приділено розробці рекомендацій щодо впровадження державної політики, спрямованої на мінімізацію ризиків, пов'язаних із використанням мобільних платформ у державному секторі, корпоративному середовищі та серед пересічних користувачів.

Виклад основного матеріалу. Мобільні операційні системи Android та iOS були створені з використанням багаторівневої архітектури безпеки, що включає такі механізми, як ізоляція додатків у «пісочницях», система дозволів, захищені канали для оновлення, перевірка цілісності ядра та системних компонентів, а також контроль джерел інсталяції програм. Для Android ключовими елементами безпеки є Google Play Protect, перевірка підписів додатків і система дозволів на основі файлу маніфеста, тоді як для iOS фундаментом захисту виступають апаратне коріння довіри Secure Enclave, сувора політика підписування та верифікації коду, а також закрита екосистема з єдиним офіційним магазином App Store [1, с. 98].

Незважаючи на ці заходи, Android залишається основною ціллю для атак через свою домінуючу частку ринку (приблизно 70 % проти 30 % у iOS) та значну фрагментацію версій і політик оновлення, що ускладнює підтримання єдиного рівня безпеки на різних пристроях [2, с. 31]. Згідно з аналітичними звітами компаній у сфері кібербезпеки, у 2023 році кількість атак на мобільні пристрої досягла десятків мільйонів випадків, причому найбільше шкідливе програмне забезпечення, зокрема програми-вимагачі, поширюється саме через Android [3, с. 168].

Отримання root-доступу в Android або виконання джейлбрейку в iOS призводить до зняття частини вбудованих обмежень безпеки. Це відкриває можливість виконання коду з підвищеними привілеями, модифікації системних бібліотек, зміни параметрів політик захисту та інсталяції неавторизованих модулів [4, с. 282]. У таких випадках ефективність антивірусних рішень, механізмів перевірки цілісності та корпоративних інструментів управління мобільними пристроями значно знижується, що спрощує приховування шкідливого коду. Таким чином, root і jailbreak слід розглядати не як нейтральну «кастомізацію», а як фактор, який значно підвищує ризики, знижує ефективність базових механізмів захисту та сприяє інсталяції і закріпленню програм-вимагачів на пристрої [5, с. 104].

Залежно від рівня ризику мобільні пристрої можна умовно класифікувати на три категорії:

Стандартний стан – використовується штатна конфігурація без root/jailbreak, інсталяція додатків здійснюється лише з офіційних магазинів.

Проміжний стан – користувач дозволяє встановлення програм із невідомих джерел, використовує сумнівні VPN чи проксі-сервіси.

Високоризиковий стан – пристрій має root/jailbreak, кастомні прошивки або модифіковане ядро.

Перехід до високоризикового стану значно збільшує площу атаки, оскільки шкідливий код отримує доступ до файлової системи, можливість перехоплення трафіку, втручання у механізми автентифікації та шифрування.

На основі аналізу спеціалізованих джерел і звітів була розроблена класифікація мобільних програм-вимагачів залежно від способів їх впливу на користувачів та дані.

Screen-locker ransomware – блокують екран пристрою, відображаючи повідомлення з вимогою викупу, часто маскуючись під офіційні штрафи від імені правоохоронних органів. У цьому випадку дані зазвичай не шифруються, однак користувач втрачає доступ до інтерфейсу [6, с. 39].

Crypto-ransomware – шифрують файли користувача (фото, документи, мультимедіа) або окремі каталоги файлової системи, що унеможливлює відновлення без спеціального ключа.

Гібридні програми-вимагачі – поєднують функції блокування екрану, шифрування даних та функціональність шпигунського ПЗ, наприклад, для викрадення контактів, повідомлень або одноразових паролів.

Окремо виділяються випадки, коли функції шифрування та шантажу інтегровані в банківські трояни або інші типи шкідливого програмного забезпечення, де програма-вимагач використовується як один із методів отримання прибутку зловмисниками [7, с. 204].

Статистичні дані демонструють зростання кількості виявлених інсталяційних пакетів програм-вимагачів для мобільних пристроїв, причому Android залишається найбільш уразливою платформою через можливість встановлення APK-файлів із зовнішніх джерел і популярність піратського контенту [3, с. 141; 8].

Найбільш поширеними способами компрометації мобільних пристроїв є інсталяція програм із неофіційних джерел, завантаження неліцензійних версій популярних додатків чи ігор, перехід за фішинговими посиланнями в SMS або месенджерах, а також експлуатація вразливостей браузера чи компонентів для відображення вебконтенту. У разі рутованих або джейлбрейк-пристроїв додаткову загрозу становить встановлення модулів чи «твікерів», які можуть містити прихований шкідливий код і отримувати системні привілеї без відома користувача [5, 105; 7].

Відкритість Android, яка є її перевагою з точки зору гнучкості та налаштувань, водночас створює значні труднощі для централізованого контролю стану пристроїв. Це особливо актуально для корпоративного середовища, де компрометація одного смартфона може стати точкою доступу до внутрішніх ресурсів організації [2, с. 241; 4, с. 284].

Для iOS характерним є суворий контроль підписування коду та джерел інсталяції, що значно ускладнює масове розповсюдження шкідливих додатків.

Успішні атаки із застосуванням програм-вимагачів найчастіше трапляються на пристроях із jailbreak або здійснюються за допомогою методів соціальної інженерії, коли користувач власноруч надає додаткам надмірні дозволи, зокрема доступ до файлів, фотографій чи хмарних сховищ [1, с. 134; 6, с. 39].

Зростання популярності хмарних сервісів і резервного копіювання відкриває нові напрямки атак, серед яких шифрування даних, синхронізованих із хмарою, погрози розголошення конфіденційної інформації, а також комбінація шифрування й витоку даних для посилення тиску на жертву.

Результати дослідження дозволяють визначити загальний ризик для мобільного пристрою як поєднання трьох основних факторів: стійкості операційної системи та частоти її оновлення, рівня привілеїв, які надав користувач або отримав зловмисник (root/jailbreak, кастомне ПЗ, модифіковані прошивки), а також поведінкових аспектів, що відображають цифрову грамотність користувача чи організації (наприклад, джерела завантаження додатків, захист від фішингових атак, регулярність створення резервних копій). Найвищий ризик виникає при поєднанні модифікованого стану пристрою з низьким рівнем обізнаності користувача щодо мобільних загроз, що створює сприятливі умови для успішного здійснення атак програмами-вимагачами.

Для підвищення рівня захисту запропоновано низку заходів, які охоплюють технічні, організаційні та освітні аспекти. До технічних заходів належить заборона використання root/jailbreak для банківських, платіжних і державних додатків, впровадження механізмів перевірки стану пристрою (attestation), розгортання систем управління мобільними пристроями (MDM) та засобів виявлення і реагування (EDR), що дозволяють автоматично ідентифікувати модифіковані пристрої та обмежувати їхній доступ до корпоративних ресурсів [4, с. 312; 8]. Важливим є також контроль джерел встановлення програмного забезпечення, обмеження інсталяції додатків лише з офіційних магазинів або корпоративних каталогів, регулярний аудит дозволів додатків і обов'язкове застосування шифрування даних на пристроях.

Організаційні заходи включають розробку та актуалізацію політик використання особистих мобільних пристроїв у рамках концепції BYOD, створення планів реагування на інциденти, пов'язані з інфікуванням програмами-вимагачами, і визначення процедур відновлення після таких атак.

Освітні заходи спрямовані на підвищення рівня обізнаності користувачів щодо небезпеки рутування пристроїв, встановлення піратських додатків, використання ненадійних VPN-сервісів, а також на навчання розпізнаванню ознак зараження пристрою та правильному реагуванню на появу вимог викупу на екрані смартфона [1, с. 139; 5, с. 106; 7, с. 299].

Для ЗСУ особливо актуальними є ризики, пов'язані з інфікуванням мобільних пристроїв під час використання особистих телефонів у рамках концепції BYOD. Така практика є поширеною серед військовослужбовців як у зоні дисло-

кації, так і під час виконання службових завдань. Завантаження додатків із неофіційних джерел, використання вразливостей браузера, підключення до незахищених Wi-Fi мереж або застосування VPN від неперевірених провайдерів можуть стати точкою входу для здійснення кібератак з боку противника.

У контексті ведення бойових дій та гібридних операцій у російсько-українській війні мобільні програми-вимагачі та шпигунські модулі дедалі частіше застосовуються як засоби кібершпигунства. Вони можуть бути використані для збору інформації про пересування військових колон, перехоплення голосових повідомлень, визначення координат, а також для віддаленої активації камер чи мікрофонів на пристроях. Наявність root-доступу або jailbreak значно полегшує зловмисникам реалізацію таких сценаріїв.

Підвищені привілеї на мобільних пристроях можуть бути використані для:

встановлення прихованих модулів для аудіо- або відеоспостереження;

компрометації службових чатів і каналів зв'язку;

отримання доступу до службових фото- та відеоматеріалів, зроблених на місці подій;

відстеження геолокації військовослужбовців і їхніх підрозділів;

блокування мобільних пристроїв підрозділів ЗСУ під час виконання операцій;

шифрування службової інформації з подальшим вимаганням викупу.

Висновки. На основі проведеного аналізу можна виокремити кілька важливих висновків, які мають як теоретичне, так і практичне значення. Насамперед, ескалація привілеїв через використання root-доступу та jailbreak є одним із ключових чинників підвищення ризиків. Це порушує початкову модель безпеки операційних систем Android та iOS, створюючи сприятливі умови для функціонування програм-вимагачів, що отримують глибокий доступ до системи та даних користувача. Через свою відкритість і домінування на ринку Android закономірно залишається головною ціллю мобільних атак. Однак, iOS також демонструє вразливість у разі використання jailbreak або надання додаткам надмірних дозволів, що вимагає однаково серйозного підходу до захисту обох платформ.

У ході дослідження встановлено, що ескалація привілеїв через root/jailbreak є одним із головних факторів, які призводять до компрометації мобільних пристроїв. Це створює серйозні загрози для діяльності Національної гвардії України. Поєднання модифікованого стану пристрою з використанням несанкціонованих додатків і низьким рівнем цифрової гігієни користувача може безпосередньо впливати на виконання службово-бойових завдань і знижувати ефективність оперативних дій.

З'ясовано, що мобільні програми-вимагачі значно еволюціонували – від простих блокувальників екрана до складних гібридних рішень. Вони поєднують шифрування даних, шантаж через витік інформації та функціонал шпигунського

ПЗ, що значно збільшує потенційні збитки для користувачів. Запропонована модель оцінки ризиків враховує параметри операційної системи, рівень привілеїв і поведінкові фактори користувачів. Вона дозволяє структурувати загрози та демонструє, що найвищий рівень небезпеки виникає при поєднанні модифікованого стану пристрою та низького рівня цифрової гігієни.

Рекомендації та модель оцінки ризиків можуть бути інтегровані в систему кібербезпеки ЗСУ. Вони спрямовані на підвищення стійкості службових комунікацій, зменшення ризику витоку оперативної інформації, впровадження ефективних рішень MDM/EDR у підрозділах, стандартизацію політик безпечного використання мобільних пристроїв у НГУ, а також на підготовку військовослужбовців до сучасних кіберзагроз.

Практичне значення отриманих результатів полягає в тому, що вони можуть бути використані в секторі безпеки та оборони, державних органах і корпоративних структурах. Це дозволить оновити політики мобільної безпеки, зокрема впровадити обов'язкову перевірку стану пристроїв перед наданням доступу до критично важливих сервісів, заборонити роботу додатків на рутованих або джейлбрейк-пристроях, а також розробити ефективні процедури реагування на інциденти, пов'язані з використанням програм-вимагачів.

Подальші дослідження можуть бути спрямовані на створення автоматизованих методів виявлення ознак root/jailbreak і раннього виявлення програм-вимагачів на мобільних пристроях.

Таким чином, забезпечення інформаційної безпеки операційних систем Android і iOS є важливою складовою державної та військової безпеки. Результати цього дослідження мають практичну цінність для підвищення кіберстійкості Збройних Сил 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: 16.12.2025).

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: 16.12.2025).

10. Всеосвіта. Національна освітня платформа. URL: https://vseosvita.ua/ (дата звернення: 16.12.2025).

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/wpcontent/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].