4. В.Базилевич, І. Мазур «Методичні аспекти оцінки масштабів тіньової економіки»// Економіка України — 2004 — № 8. — с. 41

5. Коляда Ю.В. Адаптивна парадигма моделювання економічної динаміки/ Ю.В. Коляда: монографія. — К.: КНЕУ, 2011.-297с

6. Коляда Ю.В., Семашко К.А. « Комп'ютерні сценарії взаємодії легальної й тіньової економіки суспільства»//Тенденції забезпечення сталого розвитку економічної системи України : матеріали економічної наукової інтернет-конференції — Тернопіль, 2012.-С. 94-97

7. Малинецкий Г.Г. Хаос. Структуры. Вычислительный эксперимент. Введение в нелинейную динамику. Изд. 3-е, стереотипное. — М.: Едиториал УРСС, 2002. — 256 с.

8. О.Черевко, Є.Романів «Механізм запобігання розвитку тіньової економічної діяльності у сфері фінансово-грошових відносин»// «Вісник Національного банку України», №3, 2004. — С. 21

9. Юрій Сколотяний «Прихований ресурс: як оцінити обсяги тіньового сектора?»// «Дзеркало тижня. Україна» №28, 17 серпня 2012.

Статтю подано до редакції 15.10.2020

УДК 004.056.53 DOI 10.33111/mise.99.13

Толюпа С. В., д.т.н.,
професор кафедри комп'ютерної математики та інформаційної безпеки,
Пархоменко І. І., к.т.н.,
доцент кафедри комп'ютерної математики та інформаційної безпеки,
Кириленко А. І.,
студентка IV курсу спеціальності «Кібербезпека»,
Вадис К. А.,
студент IV курсу спеціальності «Кібербезпека»,
ДВНЗ «КНЕУ імені Вадима Гетьмана»

Toliupa S. V., Dr. of Sc.,
Professor of Computer Mathematics and Information Security,
Parkhomenko I. I., Ph.D.,
Associate Professor of Computer Mathematics and Information Security,
Kyrylenko A. I.,
4th year student majoring Cybersecurity,
Vadis K. A.,
4th year student majoring Cybersecurity,
SHEI KNEU named after V. Hetman.

ЗАХИСТ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ НА МОБІЛЬНИХ ПРИСТРОЯХ

PROTECTION OF CORPORATE INFORMATION ON MOBILE DEVICES

Анотація. *Захист мобільних пристроїв важливий, як і захист будь-яких інших пристроїв. Число шкідливих програм, веб-сайтів і фішингових атак, націлених на мобільні телефони, зростає з кожним днем. На мобільних пристроях може зберігатися великий обсяг конфіденційних даних, що становить значну загрозу безпеці. На сьогоднішній будь-який бізнес — мобільний. У цій ситуації виключно важливі безпечний доступ з мобільних пристроїв до документів компанії, збереження бізнес-даних і захист смартфонів і планшетів від кіберзагроз. Деякі організації надають своїм співробітникам корпоративні смартфони та планшети, а деякі дозволяють використовувати для роботи особисті пристрої. У будь-якому випадку відстеження всіх пристроїв і забезпечення безпеки корпоративної середовища стає складним і трудомістким завданням. Ненадійні паролі, використання потенційно небезпечних програм і відмова від шифрування даних можуть привести до того, що конфіденційна інформація потрапить до рук зловмисників. У зловмисників є безліч шляхів реалізації атак. При цьому витрати на проведення атаки можуть в реальному середовищі бути вельми низькими в порівнянні з можливою вигодою. Вплив злочинних дій може бути як незначним, наприклад вираженим у зниженні швидкодії і розсилці спаму, так і істотним -наприклад, що призводить до того, що користувач не може здійснювати і приймати дзвінки або зазнає фінансових втрат. Користуючись вразливостями, хакери можуть проникати в корпоративні мережі, перехоплювати паролі та інші дані, збирати конфіденційну особисту інформацію або комерційні секрети, встановлювати шкідливий для отримання контролю над пристроями. Наразі дуже великий інтерес науковців та дослідників викликають пошуки нових засобів для захисту інформації, що зберігаються на мобільних пристроях. Метою статті є огляд існуючих загроз і вразливостей операційних платформ мобільних пристроїв і вибір механізмів захисту інформаційних ресурсів, що зберігаються на мобільних пристроях. Стаття носить оглядовий характер. Під час аналізу захищеності мобільного додатка проводиться оцінка захищеності трьох основних компонентів: каналу зв'язку, серверної частини і клієнтської частини.*
Ключові слова: *інформаційна безпека; мобільний пристрій; захист мобільних пристроїв; загрози персональним даним; витік інформації; шкідливе програмне забезпечення.*

Abstract. *Protecting mobile devices is as important as protecting any other device. The number of malware, websites and phishing attacks targeting mobile phones is growing every day. Mobile devices can store large amounts of sensitive data, which poses a significant security threat. Today, any business is mobile. In this situation, secure access from mobile devices to company documents, storage of business data and protection of smartphones and tablets from cyber threats are extremely important. Some organizations provide their employees with corporate smartphones and tablets, and some allow them to use personal devices. In any case, tracking all devices and ensuring the security of the corporate environment becomes a complex and time-consuming task. Unreliable passwords, the use of potentially dangerous programs, and the denial of data encryption can cause sensitive information to fall into the hands of attackers. Attackers have many ways to implement attacks. In this case, the cost of the attack in the real environment can be very low compared to the possible benefits. The impact of criminal actions can be as insignificant, for example, expressed in the reduction of speed and spam, and significant -for example, which leads to the fact that the user can not make and receive calls or suffers financial losses. Exploiting vulnerabilities can allow hackers to infiltrate corporate networks, intercept passwords and other data, collect sensitive*

personal information or trade secrets, and install malicious devices to gain control of devices. Currently, scientists and researchers are very interested in finding new means to protect information stored on mobile devices. The aim of the article is to review the existing threats and vulnerabilities of mobile device operating platforms and the choice of mechanisms to protect information resources stored on mobile devices. The article is an overview. During the security analysis of the mobile application, the security of three main components is assessed: the communication channel, the server part and the client part.
Keywords: *information security; mobile device; protection of mobile devices; threats to personal data; data leak; malware.*

Вступ: Сьогодні Bring Your Own Device (BYOD) — це далеко не новий термін в IT-індустрії, але він дуже стрімко привернув до себе увагу на фоні пандемії COVID-19 і швидкого переходу бізнесу в «домашній» режим.

Деякі організації вже були підготовлені до непередбачуваного майбутнього — пандемії, заздалегідь прийнявши рішення про дозвіл працювати співробітникам з дому, хоч завжди, якщо вони цього тільки забажають. Це є яскравий приклад того, коли принцип BYOD став частиною щоденної рутини компаній, у даному випадку необхідністю для виживання бізнесу у такий складний час. І як показує практика, кількість користувачів даного підходу з кожним роком лише зростатиме.

Постановка проблеми: За оцінкою Міжнародного союзу електрозв'язку (ITU) абоненти мобільного зв'язку в світі ростуть набагато швидше, ніж населення. Прогнозтична модель передбачає, що обсяг світового ринку складе 8,4 млрд абонентів при 99,3 % заселення до 2025 року (8,2 млрд у 2019 році, рис. 1) [1]. Це свідчить про збільшення мобільних пристроїв, а відповідно і частоти їх застосування для потреб організацій.

До того ж повсюдне використання стратегії Bring Your Own Device у всіх сферах діяльності дозволяє прискорити бізнес-процеси, практично миттєво отримувати актуальну інформацію та спростити комунікацію з колегами. При очевидній зручності використання і мобільності співробітників виникає безліч проблем і ризиків інформаційної безпеки. Що і зумовлює актуальність обраної теми.

За даними дослідження спеціалістів ESET, у 2019 році 68 % виявлених вразливостей на Android пристроях були критичними, а 29 % з них могли бути використані для завантаження небезпечного коду. Зокрема, увагу дослідників і користувачів привернула уразливість CVE-2019-2107, яка дозволяла зловмисникам відтворювати відео на смартфоні жертви [2].

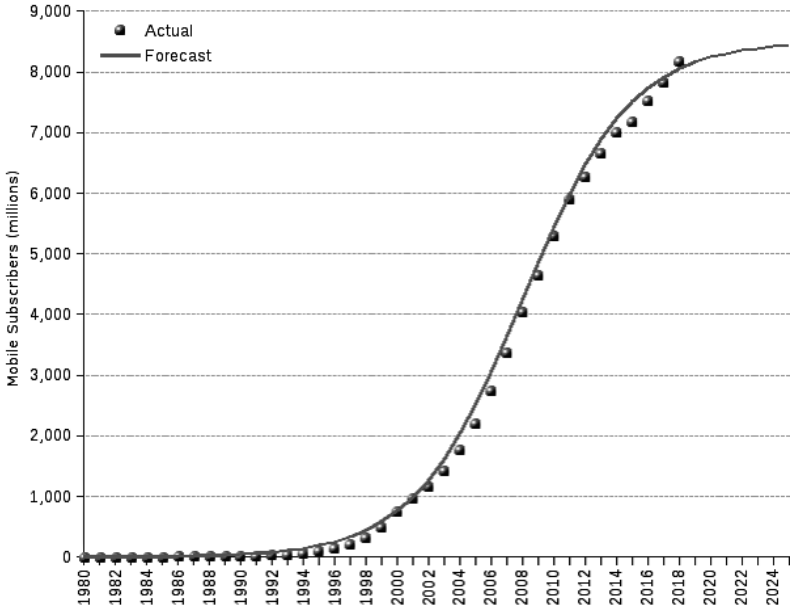

Рис. 1. Прогноз ринку мобільних телефонів ITU станом на 2019 рік

Навіть iOS пристрої — еталон надійності і безпеки — не позбавлені недоліків: у 2019 році було виявлено на 25 % уразливостей більше порівняно з 2018 роком, проте кількість критичних нижча приблизно на 20 % порівняно з Android. А отже основною ціллю кіберзлочинців, як і раніше, є пристрої Android.

Метою статті є огляд існуючих загроз і вразливостей операційних платформ мобільних пристроїв і вибір механізмів захисту інформаційних ресурсів, що зберігаються на мобільних пристроях.

Аналіз останніх досліджень і публікацій, у яких започатковано розв'язання проблеми захисту корпоративної інформації на мобільних пристроях, показав, що такі науковці як Метью Монтгомері, Кевін Курран, Вівіан Мейнс, Деклан Харкін, Нікола Благоєвич, А. В. Платоненко та інші, присвятили різним засобам захисту, таким як DLP, MDM, MAM, EMM, VPN багато уваги та часу.

Виклад основного матеріалу: Сучасні мобільні пристрої все менше відрізняються від ПК з позиції зберігання на них корпоративної інформації. Доступ до електронної пошти, корпоративних документів, спеціалізованих сервісів, ділові контакти та календа-

рі, замітки, плани і графіки робіт — це і багато іншого може отримати зловмисник, заволодівши таким пристроєм, або отримавши до нього доступ.

Величезним фактором ризику в разі втрати або крадіжки пристрою є неможливість миттєво повідомити відповідальних осіб, або заблокувати доступ до пристрою.

Також, мобільні пристрої в більшій мірі схильні до атак класу «Man-in-the-Middle», тому що змусити підключиться смартфон до «відомої» точки доступу досить легко. Після підключення до точки доступу, в більшості випадків без відома і бажання власника можна здійснювати перехоплення і підміну трафіку, а то й прямо атакувати пристрій (у випадку з Android можна скористатися спеціальними модулями Metasploit Framework).

Також, у разі Android-пристроїв велика ймовірність зараження тієї чи іншої шкідливою програмою. Це обумовлено деякими немало важливими факторами, як світова більшість користувачів, зростаюча кількість вразливостей у системі безпеки даної операційної системи та незахищений магазин додатків, через який є ймовірність скачування небезпечного ПЗ.

У разі рутованних/джейлбрекнутих* пристроїв, ризик втрати або крадіжки даних зростає ще вище: це і установка програми з невідомих джерел, необмежені і недостатньо контрольовані права — більшість користувачів не читає попереджень і підтверджує практично будь-які запити від додатків.

Найнебезпечнішою є загроза витоку інформації. У 2019 році частка витоку даних через мобільні пристрої зросла на 5 % у порівнянні з попереднім періодом. При цьому 60 % подібних інцидентів визнані великими, а інші 40 % — великими з довгостроковими наслідками [3].

Якщо ми говоримо про витік інформації, то ймовірними шляхами або причинами несанкціонованого доступу до корпоративної інформації на мобільних пристроях може бути:

- зберігання незашифрованих даних;
- необґрунтовані дозволи додаткам на використання інформаційних ресурсів;
- унікальний ідентифікатор пристрою IMEI (для Android пристроїв);
- вбудовані датчики;
- тощо.

Особлива увага має приділятися корпоративній інформації у відкритому вигляді на мобільних пристроях, так як зашифрована — вже є захищеною і надійність її безпеки залежить лише від

стійкості використовуваного криптоалгоритму. На даний час стандартом у сфері криптографії є AES — симетричний алгоритм блочного шифрування. Тож, якщо конфіденційна або важлива робоча інформація зберігаються в телефоні у відкритому вигляді, втрата або крадіжка пристрою можуть дорого обійтися компанії. Багато користувачів просто не усвідомлюють всіх ризиків своєї недбалості, наприклад, віддаючи телефон у ремонт або на обмін, чи не зачистивши пам'ять або не вилучивши доступи до акаунтів.

Дані з незашифрованого телефону можна витягти майже в 100 % випадків. «Майже» тут відноситься скоріше до випадків, коли телефон спробували фізично пошкодити або знищити безпосередньо перед зняттям даних. У багатьох пристроях Android і Windows Phone є сервісний режим, що дозволяє злити всі дані з пам'яті апарату через звичайний USB-кабель. Це стосується більшості пристроїв на платформі Qualcomm (режим HS-USB, який працює навіть тоді, коли завантажувач заблокований), на китайських смартфонах з процесорами MediaTek, Spreadtrum і Allwinner (якщо розблоковано завантажувач), а також всіх смартфонів виробництва LG [4].

Якщо мобільний пристрій належить компанії, його простіше і ефективніше захищати використовуючи загальноприйняті світові практики захисту BYOD. У корпоративних мобільних пристроях частка змішування особистих і професійних даних мала, тому деякі обмеження свободи дій користувача виправдані і доцільні. В цьому випадку баланс зміщений в сторону захисту даних, ніж зручності використання, чого не можна сказати про персональні пристрої, які більшою мірою залишаються неконтрольованими.

Перш ніж обрати технології забезпечення безпеки, компанії необхідно скласти план впровадження безпеки пристроїв, який може, наприклад, включати в себе такі кроки:

- визначити загрози і елементи ризику використання тієї чи іншої інформації на мобільному пристрої;
- необхідно скласти політику доступу до корпоративних даних поза периметром компанії;
- забезпечити додаткові заходи безпеки хмарного зберігання;
- встановити контроль додатків;
- забезпечення належної парольної політики;
- впровадження і підтримка в актуальному стані засобів захисту;
- реалізувати заходи щодо шифрування даних;
- встановити можливість віддаленого управління пристроєм;
- забезпечити заходи знищення інформації в разі втрати або крадіжки пристрою;

• прийняти заходи щодо утилізації пристрою або повернення у випадку звільнення працівника;

• впровадження адміністративних заходів щодо порушення політики BYOD.

Для захисту інформації на мобільних пристроях рекомендовано використовувати ряд таких технічних засобів: DLP-системи для контролю за конфіденційною інформацією, MDM-системи для контролю за самими мобільними пристроями та MAM-системи для контролю за програмними додатками на цих пристроях, або EEM-системи, що поєднують у собі всі попередні функції.

Сьогоденні технології DLP-продуктів використовуються головним чином для захисту інформації від витоків. Технології категоризації інформації складають ядро DLP-систем. Зазвичай на пристрої встановлюється спеціальний агент, який буде моніторити інформацію відповідно до встановлених тегів з рівнем її секретності та активізувати відповідну дію: блокування, аудит і тому подібне.

Завдяки рішенням MAM організації можуть надавати користувачам доступ до каталогу внутрішніх програм і перевірених бізнес-рішень від сторонніх постачальників, потрібних у роботі. На додачу до списку схвалених програм адміністратори також можуть створити чорний список програм, які не задовольняють необхідним критеріям. Заради зручності рішення MAM зазвичай дають адміністраторам змогу оновлювати та навіть вилучати дані віддалено, без прямого доступу до пристроїв. Це чудовий вибір для організацій із великим штатом віддалених співробітників.

Управління мобільними пристроями (MDM) — це тип програмного забезпечення для захисту, що використовується IT-відділом для моніторингу, управління та захисту мобільних пристроїв співробітників (ноутбуків, смартфонів, планшетів тощо), які розгортаються у багатьох постачальників послуг мобільного зв’язку та на декількох мобільних пристроях (рис. 2).

Рис. 2. MDM-рішення

MDM-рішення складається з двох частин: контрольного центру і клієнтського програмного забезпечення. Клієнтське програмне забезпечення може включати засоби шифрування, що дозволяють забезпечити конфіденційність робочих даних незалежно від особистої інформації користувача, а також ряд інструментів, призначених для віддаленого моніторингу та управління пристроєм. Серед найпоширеніших функцій віддаленого управління — можливість дистанційного видалення даних, установка додатків і оновлень, спливаючі оповіщення і набір інструментів «антизлодій» (що включає відстеження географічного положення пристрою, його блокування та фотографування навколишнього викрадача обстановки).

MDM-системи можуть мати вбудоване антивірусне рішенням, також можуть бути частиною мультиплатформової системи інформаційної безпеки. Рішення з управління мобільними пристроями існують для більшості популярних мобільних платформ (Android, iOS, Windows Phone, Blackberry, Symbian). Однак набір доступних функцій, залежно від операційної системи, може помітно відрізнятися. Це обумовлено відмінностями в ідеології платформ — і, як наслідок, в різному рівні доступу до даних для розробників MDM-рішень.

Мобільне управління додатками застосовує функції керування та управління політикою до окремих програм. Ця можливість необхідна, коли операційна система пристрою (наприклад, iOS, Android, Windows Phone) не надає необхідних можливостей управління або коли організації вирішили не встановлювати на пристрої профіль MDM. Існує дві основні форми управління мобільними додатками:

- попередньо налаштовані програми: До них, як правило, належать захищений менеджер персональних даних (PIM) для електронної пошти, календарів та управління контактами, а також захищений браузер, наданий постачальником послуг з управління мобільними послугами або третьою стороною;
- розширення додатків: Вони застосовують політику до програм за допомогою набору для розробки програмного забезпечення (SDK) або шляхом обгортання. Ця можливість необхідна, коли ОС не надає необхідних можливостей управління або коли організації вирішили не встановлювати агент MDM на пристрій.

Усі перераховані заходи можна застосовувати з використанням систем класу Mobile Device Management (MDM), які дозволяють віддалено (централізовано) управляти безліччю мобільних пристроїв, будь то пристрою, надані співробітникам компанією

або власні пристрої співробітників. Управління мобільними пристроями зазвичай включає в себе такі функції, як віддалений оновити регламент безпеки (без підключення до корпоративної мережі), поширення додатків і даних, а також управління конфігурацією для забезпечення всіх пристроїв необхідними ресурсами. MDM-рішення — один із засобів реалізації політики ІБ організації і, як будь-який інший інструмент, ефективні за умови використання за призначенням і правильного налаштування.

Однак і це рішення не є панацеєю від усіх загроз — можливість віддаленого управління пристроєм тільки при наявності мережі робить пристрої уразливими до фізичних атак (при відключеному мережі передачі даних або копіювання пам'яті) — клонування даних для аналізу в спеціалізованих середовищах або вилучення та можливої дешифрування даних, тому тільки дотримання контролю доступу та складу даних на мобільному пристрої може знизити ризики витоку або крадіжки критичних даних або доступу до них.

Без MDM інформація про викрадені або загублені пристрої не є захищеною, що може дозволити їй легко потрапити в чужі руки. Крім того, пристрої без MDM мають підвищений вплив шкідливих програм та інших вірусів, які можуть порушити конфіденційні дані. І після того, як конфіденційні дані скомпрометовані, легкість досягнення порушення даних або інциденту злому значно зростає –події, які можуть назавжди вплинути на репутацію компанії у споживачів та інших ділових партнерів. За даними Novell, ноутбук або планшет викрадають кожні 53 секунди, а 113 стільникових телефонів втрачають або крадуть щохвилини [5]. Оскільки витрати на відновлення після порушення корпоративних даних з кожним роком стають усе дорожчими, все більше підприємств бачать цінність комплексного рішення EMM.

Поточні пакети EMM складаються з інструментів управління політикою та конфігурацією, які поєднані з накладеним накладанням для програм і вмісту, призначеного для мобільних пристроїв, що стосуються ОС смартфонів. IT-організації та провайдери послуг використовують пакети EMM для надання IT-підтримки кінцевим користувачам мобільних пристроїв і підтримки політики безпеки.

Сучасні апартаменти EMM забезпечують такі основні функції: інвентар обладнання; інвентаризація заявок; управління конфігурацією ОС; розгортання, оновлення та видалення мобільних додатків; конфігурація мобільного додатка та управління політикою; віддалений перегляд та управління для усунення неполадок;

виконуйте віддалені дії, наприклад, віддалене форматування; управління мобільним вмістом.

Мобільні пристрої більшу частину часу підключені до Інтернету, будь то домашня мережа або загальнодоступна точка доступу Wi-Fi. Якщо не використовувати програму VPN на своєму пристрої iPhone або Android, ви автоматично стаєте привабливою мішенню для кіберзлочинців. Багато важливої корпоративної інформації стає легко доступною для злодіїв даних: повідомлення в месенджері, конфіденційні електронні листи, дані банківського рахунку та інші дані.

Мобільна VPN подібна до будь-якого іншого типу служби VPN. Вона просто пропонує захист пристрою Android або iOS через додаток, який ви можете отримати в Google Play Store та App Store.

Використання VPN гарантує захист даних під час переключення між різними мережами Wi-Fi. Частиною MDM-рішення також виступає VPN з'єдання для доступу до корпоративних ресурсів (Email, Sharepoint, Keynote, Joplin, Office) та контролю трафіка, а також його інспекції. Зі своєї сторони рішення MDM дозволяє спростити доставку сертифікату та налаштувань VPN з'єднання.

Якщо компанія вирішить налаштувати VPN вручну, то постане питання, який протокол VPN використовувати. Серед них представлені такі [6]: OpenVPN; L2TP; IPSec.

Одним з найпопулярніших і рекомендованих протоколів, OpenVPN є високозахищеною, легко налаштовуваною платформою з відкритим кодом, яка може використовувати 256-бітове шифрування AES і особливо хороша в обхід брандмауерів. OpenVPN працює на всіх основних операційних системах, включаючи Android та iOS. Однак він не підтримується на жодній платформі, а це означає, що ви повинні додати його на свій мобільний пристрій через сторонній клієнт. L2TP розшифровується як протокол тунелю рівня 2. Сам по собі L2TP — це протокол тунелювання, який не забезпечує жодного шифрування, тому, як правило, він поєднаний із IPSec-шифруванням. Разом цей дует досить простий у налаштуванні та підтримується на багатьох пристроях. Це забезпечує хороший захист, але є певна стурбованість тим, оскільки він використовує один порт (UDP-порт 500), його також легше заблокувати та не так добре обійти брандмауери, як OpenVPN. Крім того, оскільки це двоетапний процес перетворення та шифрування, він не такий швидкий. IPSec також можна використовувати самостійно і підтримується він на пристроях iOS.

Висновок: Мобільні пристрої все більше розповсюджені у світі, тому критично важливо захистити дані на всіх етапах їхнього використання. Завдяки різноманітним заходам безпеки працівники зможуть працювати, де та коли захочуть, практично з будь-якого пристрою. Щоб захист був максимальний, рішення для захисту мобільних даних зазвичай можна поєднувати. Наприклад, керуючи мобільними пристроями та програмами на них, організації можуть застосовувати захист і в хмарі, і в локальному середовищі. Корпоративні дані будуть у безпеці, незалежно від географічного розташування співробітників.

Варто зазначити, що зниження ризику витоку інформації через мобільні пристрої можна досягти, вживши нижче перераховані заходи та постійно контролювати цей процес: виключити використання корпоративних мобільних пристроїв в особистих цілях на роботі; підвищити грамотність і відповідальність працівників під час використання мобільних пристроїв; припинення навмисних витоків інформації через мобільний пристрій.

Бібліографічні посилання

1. Mobile Phone Market Forecast — 2019 [Електронний ресурс] — Режим доступу: https://stats.areppim.com/stats/stats_mobilex2019.htm
2. Аналіз безпеки мобільних пристроїв: підсумки першого півріччя 2019 [Електронний ресурс] — Режим доступу: https://eset.ua/ua/news/view/ 717/analiz-bezopasnosti-mobilnykh-ustroystv-itogi-pervogo-polugodiya-2019
3. Захист корпоративної інформації від витоку через мобільні пристрої [Електронний ресурс] — Режим доступу: https://licenziya-fsb.com/utechka-mobilnye-ustroistva
4. Афонін О. Android і шифрування даних. Про те як все погано, і навряд чи стане краще [Електронний ресурс] — Режим доступу: https://xakep.ru/2016/05/02/android-encryption/
5. What is Mobile Device Management (MDM)? [Електронний ресурс] — Режим доступу: https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm
6. Empey C. Why and how to set up a VPN on your iPhone or Android [Електронний ресурс] — Режим доступу: https://blog.avast.com/using-mobile-vpn-on-iphone-or-android

Статтю подано до редакції 29.11.2020