

Облік і оподаткування

УДК 657.004.056

Антоненко Надія Василівна

*кандидат економічних наук,
доцент кафедри фінансів, обліку і аудиту
Національний транспортний університет*

Antonenko Nadiia

*Candidate of Economic Sciences,
Associate Professor at the Department of Finance, Accounting and Auditing
National Transport University
ORCID: 0000-0003-1478-6668*

Горобець Юлія Юріївна

*студентка
Національного транспортного університету*

Horobets Yuliia

*Student of the
National Transport University
ORCID:0000-0002-2725-0638*

Корнійчук Артем Володимирович

*студентка
Національного транспортного університету*

Korniichuk Artem

*Student of the
National Transport University
ORCID:0000-0003-1993-5191*

АНТИВІРУСНИЙ ЗАХИСТ ПРОГРАМ І БАЗ ДАНИХ В ОБЛІКУ

ANTI-VIRUS PROTECTION OF PROGRAMS AND DATABASES IN THE ACCOUNT

***Анотація.** Стаття присвячена проблемам захисту від вірусів та шкідливих програм комп'ютерів, електронних пристроїв та комп'ютерних мереж в облікових системах.*

Метою статті є розкриття масштабів збитків, які можуть завдати віруси, проведення аналізу та виявлення найкращих антивірусних програм, які діють сьогодні в Україні, визначення їх здатності упередити і ліквідувати можливі загрози від дії вірусів в облікових системах.

Для досягнення поставленої мети дослідження і вирішення відповідних завдань було використано набір відомих наукових методів і методик: абстрактно-логічний метод, метод логічного синтезу, методи аналізу і синтезу. Абстрактно-логічний метод був застосований для узагальнення, формулювання висновків і рекомендацій. Метод логічного синтезу використовувався для теоретичного обґрунтування важливості вивчення проблем захисту сучасних облікових систем від комп'ютерних вірусів. Методи аналізу і синтезу дозволили визначити ряд сучасних антивірусних програм, що рекомендуються для застосування в Україні, для захисту баз даних в облікових системах.

В дослідженні проведено аналіз шкоди від проникнення вірусів у комп'ютери та визначено заходи щодо припинення поширення вірусних програмних продуктів. Висвітлено проблематику зараження вірусами в різних сферах діяльності людини, в тому числі і в облікових системах. Представлено класифікацію антивірусних програм, серед яких набули найбільшого розповсюдження такі типи програм, як «детектори» (сканери), фаги, ревізори, сторожі, вакцини.

Наведено приклади найбільших за масштабами вірусних атак в історії розвитку інформаційних технологій у різних країнах світу.

Здійснено порівняльний аналіз різноманітних антивірусних програм і визначено шляхи забезпечення цілісного захисту комп'ютера від будь-яких кіберзагроз. Обґрунтовано, що найкращими антивірусами, які рекомендуються до застосування в Україні, вважаються такі програми, як: Norton 360; Avast Free AntiVirus; Avira Free Antivirus; McAfee Internet Security; F-Secure SAFE; ESET NOD32.

Доведено, що розробка заходів щодо захисту програм і баз даних в обліку – актуальна задача сьогодення. Визначено найбільш ефективні антивірусні програми та розглянуто їх механізм пошуку різних типів вірусів. Детально висвітлено інформацію щодо антивірусної профілактики комп'ютерів, комп'ютерних мереж, баз даних в облікових системах.

Ключові слова: *комп'ютерний вірус, антивірус, захист, антивірусна програма, кібератака, облікова система, база даних в обліку.*

Summary. *The article is devoted to the problems of protection against viruses and malicious programs of computers, electronic devices and computer networks in accounting systems.*

The purpose of the article is to reveal the extent of damage that viruses can cause, to analyze and identify the best anti-virus programs operating today in Ukraine, to determine their ability to prevent and eliminate possible threats from the action of viruses in accounting systems.

A set of well-known scientific methods and techniques was used to achieve the research goal and solve the relevant problems: the abstract-logical method, the method of logical synthesis, methods of analysis and synthesis. The abstract-logical method was used for generalization, formulation of conclusions and recommendations. The method of logical synthesis was used to theoretically justify the importance of studying the problems of protecting modern accounting systems from computer viruses. The methods of analysis and synthesis made it

possible to determine a number of modern antivirus programs recommended for use in Ukraine to protect databases in accounting systems.

The study analyzed the damage caused by the penetration of viruses into computers and determined measures to stop the spread of viral software products. The problem of virus infection in various spheres of human activity, including in accounting systems, is highlighted. The classification of antivirus programs is presented, among which such types of programs as "detectors" (scanners), phages, auditors, guards, and vaccines have become the most widespread.

Examples of the largest virus attacks in the history of the development of information technologies in various countries of the world are given. A comparative analysis of various anti-virus programs was carried out and ways to ensure comprehensive protection of the computer against any cyber threats were determined. It is justified that the best antiviruses recommended for use in Ukraine are such programs as: Norton 360; Avast Free Antivirus; Avira Free Antivirus; McAfee Internet Security; F-Secure SAFE; ESET NOD32.

It has been proven that the development of measures to protect programs and databases in accounting is an urgent task today. The most effective antivirus programs were determined and their mechanism of searching for different types of viruses was considered. Information on antivirus prevention of computers, computer networks, databases in accounting systems is covered in detail.

Key words: *computer virus, antivirus, protection, antivirus program, cyber attack, accounting system, accounting database.*

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями. Останнім часом спостерігається стрімкий розвиток інформаційно-комунікаційних технологій, а з кожним роком все більшого визнання отримує у світі саме процес діджиталізації – переведення різноманітної інформації у цифровий формат. Результат

діяльності компаній, підприємств, громадських закладів, державних установ напряму залежить від ефективності використання інноваційних цифрових технологій.

Сучасний стан цифрової трансформації є однією з найпопулярніших тем для обговорень на усіх рівнях суспільства, проте з розвитком інформаційних технологій особливої уваги набула проблема ураження облікових систем комп'ютерними вірусами. Комп'ютерний вірус являє собою спеціально написану програму, яка самостійно дописується до інших програм, змінюючи їх зміст, що приводить до порушень у роботі програмних продуктів та комп'ютерних пристроїв. Частіше за все віруси не просто пошкоджують певну програму або комп'ютер – вони можуть взагалі припинити їх діяльність або повністю знищити програмне забезпечення й пристрій. Саме на боротьбу з вірусами в сучасному світі націлені зусилля провідних ІТ-компаній, які створюють антивірусні програми, здатні допомогти користувачам в стабілізації та захисті робочого процесу. Антивірусна програма – це спеціальна програма, що здійснює пошук шкідливих програм і комп'ютерних вірусів, і націлена на відновлення заражених ними файлів. Тож актуальність теми захисту пристроїв і програмного забезпечення комп'ютерів від вірусів не викликає сумнівів і потребує детального висвітлення з урахуванням розвитку сучасних програм для запобігання, виявлення та видалення шкідливого програмного забезпечення.

Аналіз останніх досліджень і публікацій виявив, що на сучасному етапі розвитку ІТ-технологій створення нових антивірусних програм є важливим фактором забезпечення комфортного та безпечного функціонування програмних продуктів і комп'ютерів в цілому. Проблемами кібербезпеки програм і баз даних займалися такі науковці, як Д.О. Ричка [1], І.Л.Грабчук [2], С.А.Вітер [3], Світличин І.І. [3], В.І.Клименко [4] та ін. Питання кіберзахисту облікової інформації розглядали у своїх роботах

Ю.Ю. Мороз [5], Ю.С. Цаль-Цалко [5]. На спеціалізованих інтернет-сайтах («Наймасштабніші віруси в історії» [6], «Класифікація антивірусних програм» [7]) зроблено аналіз та визначено сутність вірусів та антивірусних програм, висвітлено проблематику зараження вірусами в різних сферах, в тому числі в облікових системах, показано необхідність використання антивірусних програм при виникненні кіберзагроз в системах обліку та відзначена актуальність захисту від кібератак в наш час.

Виділення невирішених раніше частин загальної проблеми.

Використання антивірусних програм обумовлено необхідністю захисту від несанкціонованого доступу до конфіденційної інформації, як захід боротьби зі шкідливими програмами і вірусами. На сьогоднішній день не існує науково обґрунтованих рекомендацій щодо застосування антивірусних програм, також недостатньо обґрунтовані методи захисту від шкідливого програмного забезпечення, які використовують ІТ-фахівці.

Формулювання цілей статті (постановка завдання). Метою статті є розкриття масштабів збитків, які можуть завдати віруси, проведення аналізу та виявлення найкращих антивірусних програм, які діють сьогодні в Україні, визначення їх здатності упередити і ліквідувати можливі загрози від дії вірусів в облікових системах.

Виклад основного матеріалу дослідження з повним обґрунтуванням здобутих наукових результатів. Актуальною проблемою сьогодення є масові кібератаки на адресу українських користувачів зі сторони мешканців країни-агресора. «За період війни в Україні хакерські угруповання, пов'язані з росією, здійснили 237 кібератак проти українських підприємств та державних установ. Атаки часто були спрямовані на знищення комп'ютерних систем, але деякі також були спрямовані на збирання розвідувальних даних або поширення дезінформації» – так характеризує масові кібератаки з боку росії спеціальний звіт компанії Microsoft [8]. Вторинення інтернет-злочинців нерідко координується з операціями на полі

бою. Наприклад, наприкінці лютого поточного року хакери з росії атакували комп'ютерну мережу одного із найбільших радіотелецентрів України. Того ж дня представники російської військової машини повідомили про атаки на українські «центри дезінформації» і випустили ракету по телевежі у Києві. Американська компанія Microsoft наголошує на тому, що мета цих узгоджених у часі нападів полягає у намірах підірвати довіру громадян України до інституту влади і діючих інформаційних каналів зв'язку. Тому, аби захистити свої дані та перешкодити рашистам порушити стабільність та успіх українських захисників вірним рішенням було саме встановлення захисних програм, в тому числі і антивірусних. Актуальність вищезазначених програм в Україні в період війни значно зросла.

За досить короткий час на просторах Інтернету з'явився ряд гучних імен, пов'язаних з поширенням комп'ютерних вірусів [6]. Основними діями вірусів є викрадення конфіденційної інформації, здійснення DDoS-атак шляхом об'єднання електронних пристроїв в ботнети, розсилка спам-повідомлень з комп'ютерів різних користувачів. Прикладом значної шкоди, яка була нанесена пристроям і комп'ютерним мережам внаслідок вірусних кібератак, є низка вірусних «епідемій». Однією з таких вірусних загроз була шкідлива мережева програма-хробак «Melissa», що вразила в березні 1999 року мільйони комп'ютерів. Автором цього вірусу був 31-річний колишній програміст Девід Сміт з містечка Абердин (штат Нью-Джерсі в США), що розповсюдив заражені вірусом файли на форумах з високим рівнем відвідування. Файли містили списки з переліком сайтів для дорослих і мали паролі доступу до них. Використовуючи поштовий сервіс Microsoft Outlook, протягом декількох днів вірус Melissa надіслав свої копії на сотні тисяч комп'ютерів в різних країнах. Через вірусну атаку відключили свої e-mail сервери такі компанії-гіганти, як Intel та Microsoft. З кожного ураженого вірусом комп'ютера були розіслані спам-копії на перші п'ятдесят адрес із списку e-mail-адрес користувачів. Таким чином, вірусом Melissa було

заражено близько мільйона електронних пристроїв і нанесено збитків компаніям, фірмам, а також фізичним особам на суму більше, ніж 80 млн. доларів.

Також не можна не згадати про вірус «I LOVE YOU». Це єдиний вірус, який потрапив до Книги рекордів Гіннеса, як самий руйнівний вірус у світі [6]. Написаний хакером із Філіппін хробак у 2000 році заразив більше 3 мільйонів комп'ютерів у різних країнах світу і спричинив збитків на суму 10-15 мільярдів доларів (рис.1).

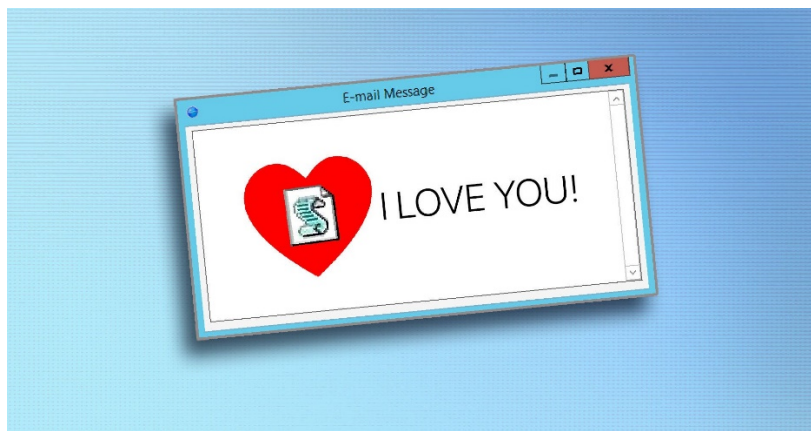


Рис. 1. Вірус I LOVE YOU

Джерело: складено авторами на основі [6]

Для свого поширення вірус ILOVEYOU використовував ті ж схеми, що і вірус Melissa. Крім того, що він розсилав через Microsoft Outlook свої копії по вкрадених адресах, він ще проявляв себе як типова троянська програма – намагався скопіювати всі знайдені паролі, які відправляв на e-mail шпигунів. Цей вірус видаляв ряд файлів із зображеннями, замість яких записував вірусний код. З кожним перезавантаженням операційної системи Windows вірус ILOVEYOU розмножувався.

Вищенаведені вірусні атаки – приклади дії масштабних, відомих на весь світ вірусів, проте крім них є ще безліч дрібних, але неприємних та небезпечних «шкідників», які заважають роботі програм та ПК в цілому. Тому, задля забезпечення захисту комп'ютерів від шкідливих або інших

небажаних програм користувачі встановлюють антивірусні програми. Найперші антивірусні продукти почав тестувати британський журнал *Virus Bulletin*. Перші тести, які журнал опублікував на своєму сайті, датуються 1998 роком [6].

Необхідно відзначити, що антивірусні програми несхожі за своєю функціональною дією, призначенням, адже відрізняються між собою й самі віруси – кожен антивірус має особливий, індивідуальний склад та сферу впливу. Найбільш відомим видом антивірусу є антивірус, що носить назву «детектор» або «сканер» [7]. Детектори перевіряють зовнішню та оперативну пам'ять комп'ютера на наявність вірусу шляхом звірки сигнатури або розрахованої контрольної суми і формують список заражених програм. Якщо сканер резидентний, то програмний продукт перевіряється і активується тільки в разі відсутності вірусів. До програм-сканерів відноситься програма MS Antivirus.

Ще одним класом антивірусних програм є програми-фаги (поліфаги), що ведуть пошук і видаляють один або декілька вірусів (фагів) [7]. Сучасні програми-поліфаги здійснюють евристичний аналіз файлу, досліджуючи його на наявність характерного для вірусу коду – вони ведуть пошук шифрування коду, аналізують додавання частини однієї програми до іншої тощо. Прикладом програм-фагів є програми DrWeb, Aidstest.

Ревізори — програми, які виявляють вірус, що невідомий для встановленої на комп'ютері програми. Програми-ревізори контролюють можливі способи зараження комп'ютера [7]. Вони перевіряють фактичний стан BOOT-сектора, заповнені FAT-таблиці, різні атрибути файлів. При виявленні хоча б незначних змін користувач отримує про це повідомлення (навіть у разі відсутності вірусів, проте при наявності змін). Прикладом програми-ревізора є програма Adinf.

Сторожі – це програми, що постійно знаходяться у пам'яті комп'ютера й в окреслений користувачем час здійснюють перевірку

оперативної пам'яті комп'ютера, файлів, BOOT-сектору, FAT-таблиці. Прикладом програми-сторожа є програма AVP, здатна виявити понад 256000 вірусів [7].

Вакцини — це програми, що застосовуються для сканування файлів та завантажувальних секторів з метою вчасного виявлення вірусів.

На ринку захисту програмних продуктів від шкідливих програм і вірусів існує багато антивірусних програм, проте серед користувачів склалися певні пріоритети і рейтинги щодо найкращих із них. Насьогодні найкращими антивірусами, що рекомендуються до застосування в Україні, користувачі вважають такі програми, як: Norton 360; Avast Free AntiVirus; Avira Free Antivirus; McAfee Internet Security; F-Secure SAFE; ESET NOD32 [7].

Norton Antivirus— це комплексне рішення для забезпечення безпеки та конфіденційності при використанні комп'ютерів з Windows або MacOS та мобільних пристроїв iOS та Android (рис.2) [9].



Рис. 2. Логотип Norton Antivirus

Джерело: складено авторами на основі [9]

Сервіс сканує систему на наявність вірусів, шпигунського та шкідливого ПЗ, а також запобігає їх проникненню через інтернет. Компонент Identity Safe захищає особисту інформацію під час роботи в мережі та включає зашифроване сховище паролів з можливістю їх генерації та автозаповнення. Продукти Norton призначені для індивідуального та сімейного використання. Вибір версії залежить від типу та кількості підключених пристроїв. Для відстеження та усунення загроз на одному персональному комп'ютері можна використовувати Security Standard. Тариф

Deluxe дозволяє підключити до 5 різних пристроїв та централізовано керувати станом їхньої безпеки через веб-консоль. Сімейна версія Premier не тільки забезпечує захист до 10 ПК, планшетів та смартфонів, а й включає інструмент для батьківського контролю та хмарне сховище від 25 гігабайт для резервного копіювання. Повне або вибіркоче сканування системи може здійснюватися як регулярно, так і на вимогу користувача. Безпека в мережі забезпечується за допомогою firewall, перевірки вмісту електронної пошти в поштовому клієнті та оцінки репутації файлів, що завантажуються. Браузерна надбудова Safe Web дозволяє визначити безпечні сайти при пошуку і допомагає запобігти спробам фішингу. Аналіз поведінки додатків виявляє невідомі загрози у часі. Для повноцінної та безперебійної роботи передбачені автоматичні оновлення вірусних баз та самозахист антивірусу від стороннього втручання.

Avast Free AntiVirus – антивірусна програма для ПК на базі операційних систем Microsoft Windows, macOS та Linux, для КПК на базі Palm та Windows CE, а також для смартфонів і планшетів на базі Android та iOS [10]. Розроблена компанією AVAST Software, яка була заснована у Чехії в 1991 році (рис. 3).



Рис. 3. Логотип Avast Free AntiVirus

Джерело: складено авторами на основі [10]

Програма Avast Free AntiVirus має наступні характеристики – це резидентний антивірусний сканер, який здійснює перевірку електронного пристрою на віруси в період показу екранної заставки; виконує перевірку комп'ютера на віруси в момент його запуску – ще до закінчення завантаження операційної системи; програма здійснює евристичний аналіз

і блокує шкідливі скрипти; програма виконує автоматичне оновлення антивірусних баз і має вбудований в програму полегшений мережевий екран. Програма Avast Free AntiVirus здійснює резидентний захист за допомогою незалежних модулів, що носять назву «екрани» і автоматично видаляє шпигунське програмне забезпечення з комп'ютера.

Avira Free Antivirus — німецький антивірусний продукт для особистого використання (рис. 4) [11].



Рис. 4. Логотип Avira Free Antivirus

Джерело: складено авторами на основі [11]

Avira Free Antivirus здійснює перевірку кожного файлу при завантаженні його на комп'ютер або відкритті на електронному пристрої, вона також моніторить жорсткий диск на предмет зараженості вірусними програмами. Удосконалена програма Avira Free Antivirus, починаючи з 9-ї версії, може знаходити програми-шпигуни та рекламні програми. За допомогою Avira Free Antivirus є можливість виявляти та знищувати руткіти – програми для приховування слідів присутності шкідливого програмного продукту в системі. Оновлення антивірусу може відбуватися щоденно, проте періодичність дозволено програмою виставляти вручну.

Антивірус **McAfee Internet Security** у своєму складі має комплекс засобів для додаткового мережевого захисту систем і пристроїв, також він здійснює антивірусний захист програм і підтримує безпеку комп'ютерів при роботі в мережі Інтернет. Антивірус McAfee Internet Security забезпечує захист пристроїв у режимі реального часу від шкідливого програмного забезпечення і зловмисників. Програма оснащена двостороннім міжмережевим екраном, що носить назву «фаєрвол», здійснює пошук

вірусів разом з програмою McAfee SiteAdvisor, виконує функцію «батьківського контролю», яка передбачає закриття доступу дітей до небажаної інформації в мережі Інтернет. Програма-антивірус McAfee Internet Security проводить також операції по безповоротному видаленню даних та налаштуванню оптимальної роботи ПК (рис. 5) [12].



Рис. 5. Логотип McAfee Internet Security

Джерело: складено авторами на основі [12]

Програма-антивірус McAfee Internet Security у своєму складі має вбудовану систему онлайн резервного копіювання, яка дає можливість зберегти і захистити від пошкодження найбільш важливі файли в мережі. Модуль програми, що носить назву QuickClean, збільшує продуктивність операційної системи за рахунок її очищення від застарілих і заражених файлів. Антивірус має функцію незворотного видалення конфіденційних файлів, яка передбачає неможливість відновлення файлів на жорсткому диску будь-якими спеціальними програмами для відновлення. Функція антивірусу McAfee Internet Security «Моя домашня мережа» дозволяє підтримувати достатньо високий рівень безпеки на комп'ютерах із встановленими антивірусами McAfee. Інформацію про безпеку відвідування веб сайтів надає вбудований модуль SiteAdvisor.

NOD32 — антивірусний пакет, що випускається словацькою фірмою ESET (рис. 6) [13].



Рис. 6. Логотип ESET NOD32

Джерело: складено авторами на основі [13]

Наприкінці 1987 року була створена перша версія антивірусу NOD32, назву якого розшифровували як «Лікарня на краю диску» (Nemocnica na Okraji Disku). Ця назва представляє собою перефразування назви популярного в Чехословаччині на той час телесеріалу «Лікарня на околиці міста». Антивірус ESET NOD32 створює ефективний захист комп'ютерних пристроїв і мереж від вірусів, а також від таких загроз, як черв'яки, троянські програми, фішинг-атаки, рекламне програмне забезпечення і шпигунське програмне забезпечення. ESET NOD32 використовує запатентовану технологію ThreatSense, яка призначена для виявлення загроз, що виникають у режимі реального часу. Для попередження дій авторів шкідливого софту пошук цих загроз здійснюється після аналізу програм, що запущені, на наявність шкідливого коду. Більша частина коду антивірусу написана мовою Assembler, для якої характерна висока швидкість перевірки і незначне використання ресурсів системи.

F-Secure Anti-Virus — антивірусне програмне забезпечення, розроблене фінської компанією F-Secure (рис.7) [14].



Рис. 7. Логотип F-Secure Anti-Virus

Джерело: складено авторами на основі [14]

Базовою розробкою антивірусу є ядро BitDefender, а також власні напрацювання компанії, серед яких DeepGuard – спеціальний засіб, що здійснює захист від невідомих вірусів. Програма F-Secure Anti-Virus виводить на екран комп'ютера інформацію про поточний стан системи F-Secure. Компонента BlackLight всебічно аналізує роботу операційної системи та виявляє руткити та заражені об'єкти, що наразі приховані від користувачів. Функція дистанційного керування допомагає адміністратору проводити антивірусну перевірку і стежити за станом корпоративної мережі. Оснащення програми F-Secure Anti-Virus механізмом автоматичного захисту від збоїв дозволяє стверджувати, що антивірусне рішення має найновіші оновлення для захисту від шкідливих програмних продуктів, навіть у тих ситуаціях, коли хмарний сервер оновлення бази даних недоступний.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Сучасний світ працює в умовах онлайн-життя, тому процес діджиталізації буде в подальшому розвиватись прискореними темпами. І скільки б не намагалися користувачі обійти можливі джерела зараження шкідливими вірусами, загроза завжди буде існувати. Віруси перешкоджають роботі користувача, проте встановлення антивірусних програм дозволяє вчасно і ефективно контролювати роботу пристроїв і програм, уникати серйозних кібератак, боротися із зараженням комп'ютерів і систем.

На сьогодні існує багато версій антивірусних програм, кожна з якої може відрізнитися від попередньої своїм функціональним складом та призначенням, проте всі ці програми мають на меті єдине – збереження спокою користувача в онлайн-середовищі. Оскільки віруси можуть приносити величезні збитки (наприклад, віруси Mellisa та ILOVEYOU) для захисту комп'ютеру і комп'ютерної мережі потрібно не тільки встановити антивірусну програму, а й вміти користуватися нею, виявляти джерела

небезпеки та максимально уникати їх. Перспективами подальших розвідок у даному напрямку є створення сучасних антивірусних програм, що усувають нові вразливості у системі безпеки.

Література

1. Ричка Д.О. Комп'ютерні віруси – шкідливі програмні засоби, рушійна сила модифікації. *Науковий вісник Херсонського державного університету*. 2018. Вип. 1. Т. 2. С. 89-93.
2. Грабчук І.Л. Організація захисту облікової інформації в умовах гібридної війни. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналіз*. 2018. Вип. 3(41). С. 20-24.
3. Вітер С.А., Світличин І.І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. Вип. 11. С. 497-502.
4. Клименко В.І. Внутрішні загрози інформаційній безпеці організації. *Вісник НБУ*. 2008. № 5. С. 62-63.
5. Цаль-Цалко Ю.С., Мороз Ю.Ю. Облікова політика підприємства та її кібербезпека. *Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства: збірник наукових праць*. Т. IV, Ч. I. Житомир: «Рута», 2017. С. 8-11.
6. Наймасштабніші віруси в історії. URL: <https://zillya.ua/index.php?q=top-10-kompyuternikh-virusiv-v-istori-chastina-1> (дата звернення 26.10.2022 р.).
7. Класифікація антивірусних програм. URL: <https://sites.google.com/site/aobdplo/pro-avtora> (дата звернення 27.10.2022 р.).
8. Кібератаки в Україні за 2022 рік. URL: <https://www.slovoidilo.ua/2022/04/28/novyna/bezpeka/rosijski-hakery->

pochatku-vijny-skoyily-majzhe-240-kiberatak-proty-ukrayiny-microsoft
(дата звернення 27.10.2022 р.).

9. Антивіруси Norton. URL: <https://onlysoft.ua/ua/antivirus/norton-antivirus/>
(дата звернення 27.10.2022 р.).
10. Avast Free AntiVirus. URL: https://uk.wikipedia.org/wiki/Avast_Antivirus
(дата звернення 27.10.2022 р.).
11. Avira Free Antivirus. URL: https://uk.wikipedia.org/wiki/Avira_Antivirus
(дата звернення 27.10.2022 р.).
12. McAfee Internet Security. URL: http://antivirus.pp.ua/mcafee_antivir_ua.html (дата звернення 27.10.2022 р.).
13. NOD32. URL: <https://www.wikiwand.com/uk/NOD32> (дата звернення 27.10.2022 р.).
14. F-Secure Anti-Virus. URL: https://uk.wikipedia.org/wiki/F-Secure_Antivirus (дата звернення 27.10.2022 р.).

References

1. Rychka D.O. (2018) Komp'juterni virusy – shkidlyvi proghramni zasoby, rushijna syła modyfikaciji [Computer viruses are malicious software, the driving force of modification]. *Scientific Bulletin of Kherson State University*, rel.1, vol. 2, pp. 89-93.
2. Ghrabchuk I.L. (2018) Orghanizacija zakhystu oblikovoji informaciji v umovakh ghibrydnoji vijny [Organization of protection of accounting information in the conditions of hybrid war]. *Problems of theory and methodology of accounting, control and analysis*, vol. 3(41), pp. 20-24.
3. Viter S.A., Svitlyshyn I.I. (2017) Zakhyst oblikovoji informaciji ta kiberbezpeka pidpryjemstva [Protection of accounting information and cybersecurity of the enterprise]. *Economy and society*, vol.11, pp. 497-502.

4. Klymenko V.I. (2008) Vnutrishni zagrozy informacijnij bezpeci orghanizaciji [Internal threats to information security of the organization]. *Bulletin of the NBU*, no. 5, pp. 62-63.
5. Calj-Calko Ju.S., Moroz Ju.Ju. (2017) Oblikova polityka pidpryjemstva ta jiji kiberbezpeka [Accounting policy of the enterprise and its cybersecurity] *Accounting, analysis and control in the context of modern concepts of managing the economic potential and market value of the enterprise: a collection of scientific papers*, vol. IV, part 1, Zhytomyr : "Ruta", pp. 8-11.
6. Naimasshtabnishi virusy v istorii [The largest viruses in history]. URL: <https://zillya.ua/index.php?q=top-10-kompyuternikh-virusiv-v-istori-chastina-1> [in Ukrainian].
7. Klasyfikatsiia antyvirusnykh prohram [Classification of antivirus programs]. URL: <https://sites.google.com/site/aobdplo/pro-avtora> [in Ukrainian].
8. Kiberatomy v Ukraini za 2022 rik [Cyber-attacks in Ukraine in 2022]. URL: <https://www.slovoidilo.ua/2022/04/28/novyna/bezpeka/rosijski-xakery-pochatku-vijny-skoyily-majzhe-240-kiberatak-proty-ukrayiny-microsoft> [in Ukrainian].
9. Antyvirusy Norton [Antiviruses Norton]. URL: <https://onlysoft.ua/ua/antivirus/norton-antivirus/> [in Ukrainian].
10. Avast Free AntiVirus. URL: https://uk.wikipedia.org/wiki/Avast_Antivirus [in Ukrainian].
11. Avira Free Antivirus. URL: https://uk.wikipedia.org/wiki/Avira_Antivirus [in Ukrainian].
12. McAfee Internet Security. URL: http://antivirus.pp.ua/mcafee_antivir_ua.html [in Ukrainian].
13. NOD32. URL: <https://www.wikiwand.com/uk/NOD32> [in Ukrainian].
14. F-Secure Anti-Virus. URL: https://uk.wikipedia.org/wiki/F-Secure_Antivirus [in Ukrainian].