using digital tools for the development of farming and the modernization of the agro-industrial complex of Ukraine.
Keywords: *digital agriculture, mobile applications, farming, agro-industrial complex, farm management, digital technologies.*

Науковий керівник:
Співак В.В.,
асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій
Миколаївський національний аграрний університет

УДК 004.056:338.43

Роль систем фільтрації електронної пошти у забезпеченні інформаційної безпеки аграрного сектору

Чепурненко Владислав,
здобувач вищої освіти спеціальності 122 «Комп'ютерні науки»
Миколаївський національний аграрний університет
м. Миколаїв, Україна

Анотація: *Електронна пошта в агробізнесі є основним каналом обміну договорами, рахунками, логістичними повідомленнями та службовими документами, тому саме вона часто стає точкою входу для фішингу, спаму і шкідливих вкладень. Для аграрних підприємств такі атаки означають не лише технічний інцидент, а й ризик зриву поставок, підміни платіжних реквізитів, втрати доступу до корпоративних сервісів і витоку комерційної інформації. У тезах доведено, що сучасні системи фільтрації пошти мають розглядатися як повноцінний елемент кіберзахисту, ефективність якого забезпечується поєднанням перевірки автентичності відправника, аналізу вкладень, поведінкових моделей та машинного навчання.*
Ключові слова: *електронна пошта, фішинг, спам, інформаційна безпека, аграрний сектор, машинне навчання.*

Вступ. Цифрова трансформація аграрного сектору змінює не лише виробничі процеси, а й логіку управління підприємством. Агрокомпанії, фермерські господарства, елеватори, трейдери, логістичні оператори, постачальники насіння, добрив і техніки дедалі більше покладаються на електронні канали комунікації. Саме через електронну пошту узгоджуються умови контрактів, пересилаються рахунки та специфікації, надходять повідомлення від банків, державних органів, митних і контролюючих служб. За таких умов поштовий сервіс стає не просто засобом листування, а критичною точкою доступу до управлінської, фінансової та комерційної інформації. Цим

активно користуються зловмисники: під виглядом листів від контрагентів вони надсилають фішингові повідомлення, заражені вкладення, посилання на підроблені сторінки входу або прохання терміново змінити реквізити для оплати. Для аграрного бізнесу, де помилка в один день посівної чи збирання врожаю може мати відчутні фінансові наслідки, навіть короткочасна компрометація пошти здатна спричинити ланцюгові збої.

Аналіз проблеми. Традиційне уявлення про захист електронної пошти часто зводиться до базового антиспам-фільтра та антивіруса. Однак цього вже недостатньо. Сучасні фішингові кампанії стали значно точнішими: листи пишуться без явних мовних помилок, імітують стиль реальних партнерів, посилаються на актуальні господарські процеси – постачання пального, погодження видаткових накладних, бронювання перевезень, оформлення сертифікатів якості чи фітосанітарних документів. Окрему небезпеку становить компрометація ділового листування, коли зловмисник не просто надсилає випадковий лист, а вбудовується у вже наявний діалог між працівником підприємства та контрагентом. У такому разі повідомлення виглядає максимально правдоподібно, а традиційні фільтри, що орієнтуються лише на ключові слова або відомі шкідливі адреси, можуть не спрацювати. До того ж аграрні підприємства нерідко мають розгалужену структуру, сезонних працівників, віддалені виробничі майданчики та нерівномірний рівень цифрової грамотності персоналу. Це створює середовище, у якому людський фактор посилює технічні ризики. Проблема полягає і в тому, що електронний лист сьогодні є не самою атакою, а лише початковою ланкою більш складного сценарію: через нього викрадають облікові дані, запускають шкідливий код, отримують доступ до хмарних сервісів, бухгалтерських систем або внутрішніх документів підприємства.

Пропоновані рішення. За таких умов системи фільтрації електронної пошти мають працювати як багаторівневий механізм відбору ризиків. Перший рівень – перевірка автентичності відправника за допомогою SPF, DKIM і DMARC, що дозволяє виявляти підміну домену та зменшує ефективність листів, які імітують надійного партнера. Другий рівень – репутаційний аналіз адрес, доменів, IP-джерел, а також виявлення аномальної активності, наприклад нетипової масової розсилки або листів із технічно підозрілими заголовками. Третій рівень – контентний аналіз: перевірка вкладень, сканування архівів, макросів, виконуваних файлів, вебпосилань і QR-кодів, які дедалі частіше використовуються для обходу класичних засобів захисту. Особливо важливим стає застосування «пісочниць», у яких підозрілий файл або посилання перевіряється в ізольованому середовищі до того, як його побачить користувач. Четвертий рівень – інтелектуальний аналіз повідомлення. Саме тут ефективними є алгоритми машинного навчання, що враховують не лише формальні ознаки листа, а й його семантику, тональність, нетипові мовні конструкції, раптові прохання про оплату, зміну банківських реквізитів, передачу паролів або відкриття вкладення «терміново». Сучасні моделі можуть виявляти неочевидні

залежності між текстом листа, історією взаємодії з відправником і поведінкою користувача, підвищуючи точність відсікання небезпечних повідомлень.

Для аграрного сектору доцільно доповнювати типові поштові фільтри галузевим контекстом. Наприклад, лист із вкладенням про нібито зміну умов постачання мінеральних добрив у розпал посівної кампанії має оцінюватися з урахуванням того, чи є такий контрагент у реєстрі партнерів підприємства, чи листування з ним уже велося, чи відповідає стиль повідомлення попереднім контактам. Аналогічно повідомлення про термінову оплату транспортних послуг, яке надходить бухгалтерії з нової адреси, повинно автоматично отримувати підвищений ризиковий бал. Тобто ефективна система фільтрації – це не просто бар'єр на вході, а інструмент контекстного аналізу бізнес-комунікації. Вона має бути інтегрована з корпоративною інфраструктурою: каталогом користувачів, політиками доступу, журналами подій, SIEM-платформами, сервісами резервного копіювання та механізмами швидкого реагування на інциденти. Не менш важливою є і правильна організаційна складова: навіть найкращий фільтр не замінить регламенту подвійної перевірки фінансових вказівок, правил роботи з вкладеннями, обмеження прав доступу та навчання персоналу без створення атмосфери покарання за помилки.

Висновки. Отже, системи фільтрації електронної пошти відіграють у забезпеченні інформаційної безпеки аграрного сектору значно ширшу роль, ніж просте відсіювання небажаної кореспонденції. У сучасних умовах вони є першою лінією захисту від фішингу, шкідливих вкладень, компрометації ділового листування та витоку даних. Їхнє значення особливо зростає для аграрного бізнесу, де електронна комунікація безпосередньо пов'язана з поставками ресурсів, рухом коштів, логістикою та стабільністю виробничого циклу. Базових засобів захисту вже недостатньо, тому пріоритет слід надавати багаторівневим системам, що поєднують протоколи автентифікації, поведінковий аналіз, машинне навчання, перевірку вкладень і тісну інтеграцію з внутрішніми процесами підприємства. Саме такий підхід дає змогу не лише зменшити кількість успішних атак, а й підвищити стійкість аграрних організацій до кіберінцидентів, зберегти фінансову стабільність і довіру партнерів.

Список використаних джерел:

1. ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

2. Kulkarni, A., Wang, Y., Gopinath, M., Sobien, D., Rahman, A., & Batarseh, F. A. (2025). A review of cybersecurity incidents in the food and agriculture sector. Journal of Agriculture and Food Research, 22, 102245. https://doi.org/10.1016/j.jafr.2025.102245

3. Alhuzali, A., Alloqmani, A., Aljabri, M., & Alharbi, F. (2025). In-depth analysis of phishing email detection: Evaluating the performance of machine learning and deep learning models across multiple datasets. Applied Sciences, 15(6), 3396. https://doi.org/10.3390/app15063396

Анотація: *The article examines the role of email filtering systems in protecting the information infrastructure of the agricultural sector. It is shown that phishing, spam, malicious attachments, and business email compromise create direct risks for payments, logistics, contracts, and confidential data in agribusiness. The paper argues that effective defense requires multi-layer filtering based on sender authentication, attachment inspection, behavioral analysis, and machine learning.*
Ключові слова: *email security, phishing, spam, information security, agricultural sector, machine learning.*

Науковий керівник:
Коломієць А.М.,
асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій,
Миколаївський національний аграрний університет

УДК 004.8:004.773.6

Класифікація спаму в електронній пошті з використанням машинного навчання

Чепурненко Владислав,
здобувач вищої освіти спеціальності 122 «Комп'ютерні науки»
Миколаївський національний аграрний університет
м. Миколаїв, Україна

Анотація: *у тезах доповіді розглянуто підходи до автоматичної класифікації небажаної електронної кореспонденції (спаму) з використанням методів машинного навчання. Проаналізовано традиційні та сучасні алгоритми фільтрації спаму, методи представлення текстових даних, а також ключові набори даних для навчання та оцінювання моделей. Запропоновано практичну реалізацію класифікатора на основі наївного баєсівського алгоритму та методу опорних векторів засобами Python.*
Ключові слова: *машинне навчання, фільтрація спаму, класифікація тексту, наївний баєс, метод опорних векторів, NLP, Python.*

Електронна пошта залишається одним із ключових інструментів ділової та особистої комунікації в цифровому суспільстві. Водночас значна частка поштового трафіку припадає на небажані повідомлення – спам, що становить серйозну загрозу для інформаційної безпеки, продуктивності користувачів та стабільності поштових систем. За даними аналітичних компаній, частка спаму у глобальному електронному трафіку стабільно перевищує 40–45%, а його типи охоплюють рекламні розсилки, фішингові атаки, розповсюдження шкідливого програмного забезпечення та соціальну інженерію [1]. У цьому контексті