

**СЛОБОДЯН ТЕТЯНА**, здобувач вищої освіти

Науковий керівник – **КУЧМІЙОВА ТЕТЯНА**, к.е.н., доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій

**Миколаївський національний аграрний університет, м. Миколаїв**

## КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОПОДАТКУВАННЯ: ЗАГРОЗИ ТА ЗАХОДИ ЗАХИСТУ

Кібербезпека в інформаційних системах оподаткування є дуже важливою для забезпечення стабільності та надійності фінансової інфраструктури держави. Загрози кібербезпеці в цій сфері можуть призвести до серйозних фінансових втрат, підриву довіри до державних інституцій та витоку конфіденційної інформації.

Кібербезпека забезпечує захист мереж, даних і пристроїв від несанкціонованого доступу та неправомірного використання. Надання послуг у цій сфері включає запобігання кіберзагрозам, їхнє виявлення та реагування на можливі кібератаки [1].

Основні загрози кібербезпеці в інформаційних системах оподаткування є такими [1, 2]:

1. Фішингові атаки. Кіберзлочинці використовують фішинг для отримання конфіденційної інформації, видаючи себе за надійні джерела, такі як державні установи чи банки. Це може призвести до компрометації облікових записів та несанкціонованого доступу до систем оподаткування.

2. Шкідливе програмне забезпечення (малваре). Віруси, троянці та інші види шкідливого ПЗ можуть інфікувати системи оподаткування, що призводить до викрадення даних, порушення роботи систем та фінансових втрат.

3. Атаки за типом «відмови в обслуговуванні» (DDoS). Масові атаки на сервери податкових органів можуть призвести до їх перевантаження та недоступності для користувачів, що ускладнює процеси подання та обробки податкової звітності.

4. Компрометація корпоративної електронної пошти (BEC). Зловмисники можуть отримати доступ до корпоративної електронної пошти працівників податкових органів, що дозволяє їм маніпулювати фінансовими транзакціями та викрадати кошти.

5. Використання вразливостей. Невчасне оновлення програмного забезпечення може залишити системи вразливими до відомих експлойтів, які зловмисники можуть використати для несанкціонованого доступу або пошкодження даних.

6. Внутрішні загрози. Недобросовісні співробітники або підрядники з доступом до конфіденційної інформації можуть навмисно або ненавмисно спричинити витік даних або інші інциденти безпеки.

Заходи захисту інформаційних систем оподаткування:

1. Впровадження системи управління інформаційною безпекою (СУІБ). Запровадження СУІБ на основі міжнародних стандартів, таких як ISO/IEC





27001, допомагає організаціям структурувати та систематизувати заходи з кіберзахисту.

2. Регулярне оновлення програмного забезпечення. Своєчасне оновлення ОС та прикладних програм забезпечує захист від відомих вразливостей, що можуть стати мішенню для зловмисників.

3. Використання сильних паролів та багатофакторної автентифікації. Застосування складних паролів та додаткових методів автентифікації (наприклад, одноразових кодів) значно ускладнює несанкціонований доступ до систем.

4. Навчання та підвищення обізнаності працівників. Періодичне навчання співробітників з питань кібербезпеки сприяє зниженню ймовірності успішних фішингових атак та інших методів соціальної інженерії.

5. Використання антивірусного програмного забезпечення та міжмережевих екранів. Захист систем від шкідливого ПЗ та несанкціонованого доступу забезпечується за допомогою сучасних антивірусних програм та фаєрволів.

6. Розробка планів реагування на інциденти. Детальні плани дій у разі кіберінцидентів дозволяють швидко відновити роботу систем та мінімізувати наслідки атак.

7. Співпраця з національними центрами кібербезпеки: Взаємодія з організаціями, такими як CERT-UA, сприяє обміну інформацією про актуальні загрози та отриманню рекомендацій щодо захисту.

Забезпечення кібербезпеки в інформаційних системах оподаткування вимагає комплексного підходу, який включає організаційні, технічні та освітні заходи. Лише за умови постійного вдосконалення та адаптації до нових загроз можна гарантувати надійність та безпеку податкових систем.

### Список використаних джерел:

1. Боренков А. ТОП 10 загроз кібербезпеці бізнесу у 2023 році. Міжнародна аудиторська компанія. BDO. URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023> (дата звернення 10.03.2025).
2. Кібербезпека бізнесу це не лише технічні заходи. Legal IT group. URL: <https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnicni-zahodi/> (дата звернення 10.03.2025).
3. Принципи побудови стійкої системи кіберзахисту. МОЗ. URL: <https://moz.gov.ua/uk/principi-pobudovi-stijkoyi-sistemi-kiberzahistu> (дата звернення 10.03.2025).
4. Кібербезпека під час війни: базові заходи з кіберзахисту для українських організацій. Gov.ua. URL: <https://www.kmu.gov.ua/news/kiberbezpeka-pid-chas-viiny-bazovi-zakhody-z-kiberzakhystu-dlia-ukrainskykh-orhanizatsii> (дата звернення 10.03.2025).
5. Як протидіяти кіберзагрозам та захистити системи від ворожих кібератак – важливі рекомендації та допомога CERT-UA. Gov.ua. URL: <https://www.kmu.gov.ua/news/yak-protydiaty-kiberzahrozam-ta-zakhystyty-systemy-vid-vorozhykh-kiberatak-vazhlyvi-rekomendatsii-ta-dopomoha-cert-ua> (дата звернення 10.03.2025).

