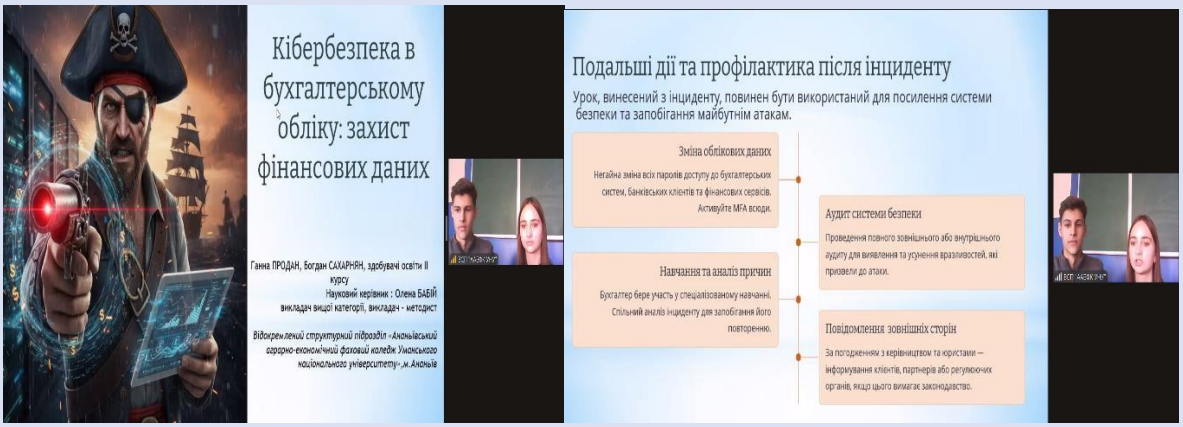
**Міністерство освіти і науки України**
**Рада директорів ЗФПО Одеської області**
**ОМК викладачів бухгалтерського обліку**

# *ІІ Обласна науково- практична конференція "Стратегія розвитку бухгалтерського обліку, аналізу й аудиту в сучасних реаліях сьогодення"*

**Одеса,2025 рік**

***Здобувачі освіти : Ганна ПРОДАН, Богдан САХАРНЯН***
***Керівник :спеціаліст вищої категорії, викладач- методист: Бабій О.М.***
***ВСП "Ананьївський аграрно-економічний фаховий коледж Уманського національного університету ", м. Ананьїв***




## КІБЕРБЕЗПЕКА У БУХГАЛТЕРСЬКОМУ ОБЛІКУ НА ПІДПРИЄМСТВАХ

У сучасному цифровому світі питання кібербезпеки стає одним із ключових факторів стабільної роботи будь-якого підприємства. Особливо це стосується бухгалтерських відділів, де зосереджена найбільш цінна фінансова та персональна інформація.

Кібератаки, фішингові кампанії, програми-вимагачі та внутрішні загрози — усе це може призвести не лише до фінансових втрат, а й до втрати репутації, витоку конфіденційних даних і навіть паралічу діяльності організації.

Саме тому мета цієї доповіді — висвітлити основні кіберзагрози, що постають перед бухгалтерськими системами, та окреслити комплекс заходів, які забезпечують їх ефективний захист.

Основні кіберзагрози для бухгалтерських відділів

Бухгалтерські відділи є одними з найпривабливіших цілей для кіберзлочинців. Тут зберігаються фінансові звіти, персональні дані працівників, інформація про банківські рахунки, платіжні документи — усе, що має реальну грошову цінність. Серед основних кіберзагроз варто виділити кілька ключових напрямів:

***1. Фішинг та соціальна інженерія.***
Шахраї надсилають електронні листи, що імітують офіційні повідомлення банків чи державних структур. Метою таких листів є викрадення облікових даних або встановлення шкідливого програмного забезпечення.
***2. Програми-вимагачі (Ransomware).***
Це особливо небезпечний вид шкідливого ПЗ, який блокує доступ до системи або шифрує дані, а потім вимагає викуп за їх розблокування. Наслідком може стати повне припинення фінансових операцій підприємства.
***3. Внутрішні загрози.***
Іноді джерелом небезпеки стають самі співробітники — як через зловмисні дії, так і через недбалість. Наприклад, використання слабких паролів, збереження конфіденційних документів на особистих пристроях або передача даних стороннім особам.
***4. Несанкціонований доступ***.
Хакери можуть зламати бухгалтерські програми або бази даних, щоб викрасти інформацію чи змінити фінансові записи. Це часто призводить до спотворення звітності та фінансових збитків.[1]
Розуміння цих загроз — перший крок до ефективного захисту.

Кібербезпека не обмежується лише програмним забезпеченням. Вона ґрунтується на поєднанні організаційних, технічних та кадрових заходів. Тільки комплексний підхід дозволяє створити надійну систему безпеки.

**1. Організаційні заходи**
Організаційна складова є фундаментом кіберзахисту.
Сюди входить:

***Розробка політики безпеки*** — документування правил поводження з фінансовими даними, визначення відповідальних осіб і процедур доступу.

***Контроль автоматизації*** — перевірка правильності роботи бухгалтерських програм і моніторинг підозрілих транзакцій.

***Розмежування доступу*** — надання працівникам лише тих прав, які необхідні для виконання їхніх обов’язків.

***Регулярний аудит*** — системні перевірки програмного забезпечення та політик безпеки для виявлення вразливостей.

Такі заходи допомагають уникнути ситуацій, коли людський фактор або організаційна недбалість стають причиною кіберінцидентів.

## 2. Технічний арсенал захисту

Технічні засоби є своєрідною «цифровою фортецею», що оточує фінансову інформацію.[2]

Серед основних технічних рішень:

Використання ліцензійного програмного забезпечення та постійне оновлення бухгалтерських систем.

Шифрування даних — як під час зберігання, так і під час передачі інформації мережею.

Багатофакторна автентифікація (MFA) — додатковий рівень захисту при вході в систему, який значно ускладнює доступ для зловмисників.

Резервне копіювання — регулярне створення копій даних і зберігання їх в окремому середовищі. Це дозволяє швидко відновити роботу у разі атаки.

Антивірусний захист і Firewall — блокування підозрілої активності, фільтрація трафіку, запобігання проникненню шкідливого ПЗ.

Роль Бухгалтера у Кібербезпеці

1) Дотримання протоколів; 2)Надійні паролі та MFA;
3)Обережна робота з поштою; 4)Повідомлення про підозри

Алгоритм дій бухгалтера: негайна реакція на атаку.

Швидка та послідовна реакція на кібератаку мінімізує збитки та запобігає її поширенню. Ефективна взаємодія з IT-службою є критичною.

- Ізоляція системи

Негайно від'єднайте скомпрометований пристрій від мережі (вийміть кабель, вимкніть Wi-Fi). Не вимикайте пристрій!

- Повідомлення керівництва та IT

Негайно інформуйте відповідальних осіб для активації плану реагування на інциденти. Не платіть викуп. У випадку атак вимагачів (Ransomware) категорично заборонено сплачувати викуп.

Після локалізації загрози починається найважливіший етап – відновлення та перевірка цілісності фінансових записів.[4]

Роль бухгалтера тут є центральною.

1. Документування інциденту: Зафіксуйте всі деталі: час, спосіб виявлення, постраждалі системи та потенційно скомпрометовані дані.
2. Відновлення з резервних копій: Співпрацюйте з IT-фахівцями для відновлення даних з актуальних, цілісних та ізольованих резервних копій

3.Перевірка цілісності: Ретельна звірка відновлених даних із первинними документами та незалежними джерелами для виявлення маніпуляцій.
4. Тимчасові рішення: Розробка процедур для продовження критичного обліку на основі паперових звітів, якщо відновлення триває довго.

Подальші дії та профілактика після інциденту:

Урок, винесений з інциденту, повинен бути використаний для посилення системи безпеки та запобігання майбутнім атакам.

- Зміна облікових даних: Негайна зміна всіх паролів доступу до бухгалтерських систем, банківських клієнтів та фінансових сервісів. Активуйте MFA всюди.
- Навчання та аналіз причин: Бухгалтер бере участь у спеціалізованому навчанні. Спільний аналіз інциденту для запобігання його повторенню.
- Аудит системи безпеки : Проведення повного зовнішнього або внутрішнього аудиту для виявлення та усунення вразливостей, які призвели до атаки.
- Повідомлення зовнішніх сторін: За погодженням з керівництвом та юристами — інформування клієнтів, партнерів або регулюючих органів, якщо цього вимагає законодавство.

**Список використаних джерел:**

1.Деньга С.М Захист інформації в комп'ютерних інформаційних системаи бухгалтерського обліку [Text] /С.М. Деньга, Ю.О. Верига // Бухгалтерський облік і аудит. 2004. № 5. - С. 59-65
2. Настанови з кібербезпеки від експертів [Електронний ресурс]. – Режим доступу:http://www.isaca.org.ua/index.php/press-center/news/191-translation-of-guidelines-on-cybersecurity
3. Про внесення змін до Закону України «Про основи національної безпеки України» : проект Закону України щодо кібернетичної безпеки України від 07.03.13р. № 2483. – Режим доступу: // www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1pf3511=45998
4. Цаль-Цалко Ю.С. Облікова політика підприємства та її кібербезпека / Ю.С. Цаль-Цалко, Ю.Ю. Мороз //Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства: збірник наукових праць, том IV, частина I, Житомир: ПП «Рута», 2017 – С. 8-11. 10. ISO/IEC 27001:2013 information security management system standardarrives [Electronicresource]. -2013-Accessedmode:http://www.reuters.com