

2. Спільник Ірина, Палюх Микола. Бухгалтерський облік в умовах цифрової економіки. *Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації*. 2019. Випуск 1-2. С. 83-96.

3. Рой Я. В., Мазур Н. П., Складанний П. М. Аудит інформаційної безпеки – основа ефективного захисту підприємства. *Кібербезпека: освіта, наука, техніка*. 2018. № 1. С. 86-93.

4. Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації, затверджена розпорядженням Кабінету Міністрів України від 17 січня 2018 року № 67-р. URL: <https://zakon.rada.gov.ua/laws/show/67-2018> (дата звернення: 08.05.2020).

Буганов О.В.

здобувач вищої освіти 5 курсу,
обліково-фінансовий факультет,
спеціальність 071 «Облік і оподаткування»

Науковий керівник:

канд. екон. наук, доцент Мельник О. І.

Миколаївський національний аграрний університет
м. Миколаїв

ІТ-АУТСОРСИНГ ЯК ЗАСІБ СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ОБЛІКОВОЇ ІНФОРМАЦІЇ ПІДПРИЄМСТВА

На сьогодні більшість суб'єктів господарювання проводять свою діяльність з використанням комп'ютеризованої форми ведення бухгалтерського обліку. Її застосування має не лише багато переваг, а й деякі недоліки. Так, в процесі інформатизації суспільства та поширення інформаційно-комунікативних технологій власникам підприємств потрібно перейматися інформаційною безпекою своєї установи, захищаючи облікову інформацію. Щоб забезпечити ефективну діяльність, керівникам потрібно налагодити інформаційну інфраструктуру підприємства, аби уникнути кібератак чи втрати даних через непередбачувані поломки. Для цього можна залучити ІТ-аутсорсинг, який допоможе налаштувати системи захисту облікової інформації.

ІТ-аутсорсинг – це часткова чи повна передача функції з обслуговування інформаційної інфраструктури підприємства-замовника спеціалізованій компанії. Її діяльність спрямована на:

- управління інформаційними системами щодо захисту економічної інформації;
- впровадження інформаційних баз даних, систем управління та обліку;
- проведення аудиту ІТ-інфраструктури підприємства-замовника;
- модернізація та обслуговування ІТ-систем;
- виявлення та усунення насправностей;

– відновлення даних при збої в роботі обладнання і програмного забезпечення;

- аутсорсинг бізнес-процесів;
- системна інтеграція [1, 2, 3].

Більш детально зупинимося на управлінні системами захисту облікової інформації підприємства, оскільки ця проблема є достатньо актуальною в сучасних умовах господарювання.

Обліковою інформацією є вся інформація, що зберігається та підлягає обробці в бухгалтерській службі підприємства. Вона може зберігатися такими способами:

- на електронних носіях комп'ютерної техніки;
- на електронних сховищах;
- на фізичних носіях в архівах.

Організувати захист та безпеку даних в бухгалтерській службі можна при забезпеченні комплексу організаційних, технічних заходів та кадрової роботи (рис. 1), що буде спрямована на збереження комерційної таємниці та належного контролю роботи облікових працівників.

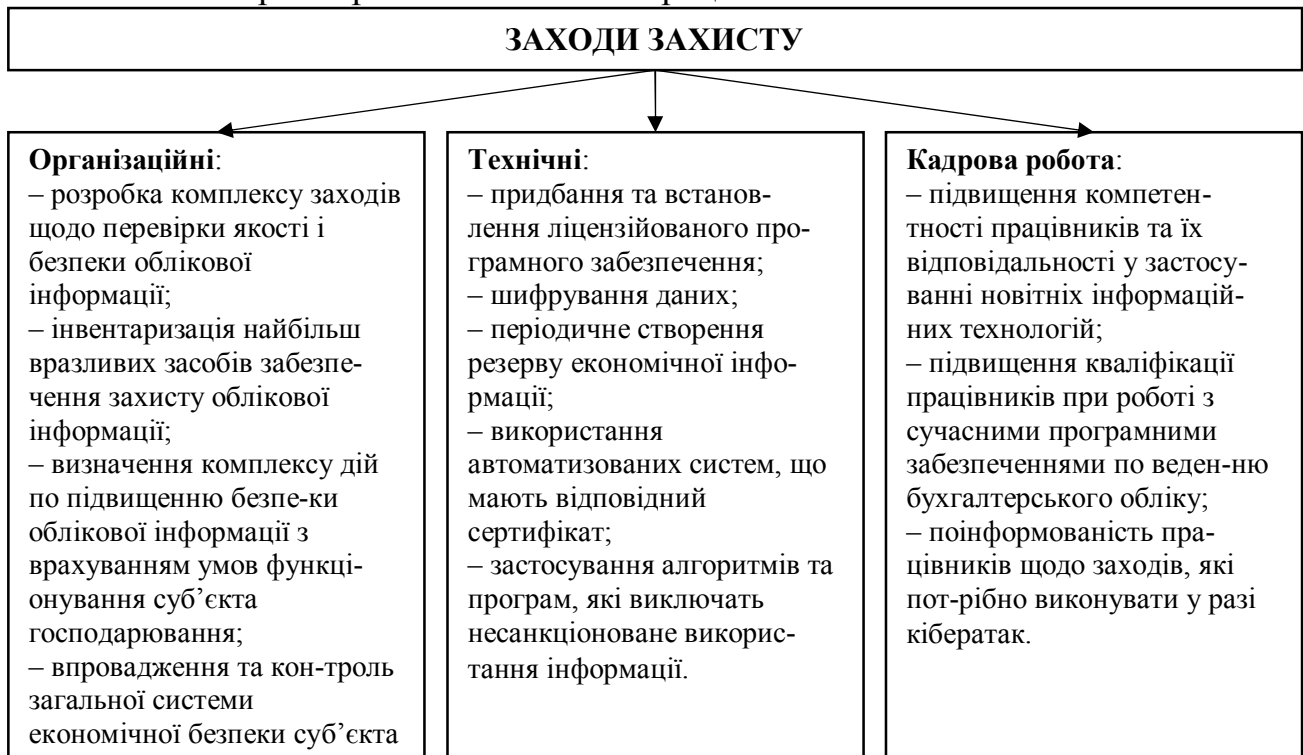


Рисунок 1 – Заходи щодо захисту облікової інформації підприємства

Джерело: побудовано автором на основі [4, 5, 6]

За допомогою фахівців сфери ІТ-аутсорсингу на суб'єкті господарювання можуть бути сформовані певні принципи, що унеможливлуватимуть неправомірне втручання в базу даних підприємства:

- підтримка програмного забезпечення (контроль за відсутністю неавторизованої зміни програм і прав доступу до них);
- охорона конфіденційної інформації (неухильне виконання персоналом бухгалтерської служби правил дотримання конфіденційності);

– ефективний контроль доступу до облікових даних (запровадження обмежень користувачів при роботі з цінною обліковою інформацією) [3].

Залучивши ІТ-аутсорсинг, суб'єкту господарювання пропонується трирівнева система управління обліковою інформацією для її захисту (табл. 1).

Таблиця 1 Засоби підвищення безпеки облікової інформації

Перелік засобів	Зміст
Перший рівень управління обліковою інформацією	
Ідентифікація, оцінка загроз	Джерела витоку та втрати інформації, окреслення кола можливих форс-мажорних загроз
Інвентаризація ресурсів	Інвентаризація інформаційних, програмних та фізичних ресурсів, які забезпечують якість облікової інформації
Контроль ризиків, які загрожують безпеці облікової інформації	Виявлення груп потенційних навмисних (шахрайство) і ненавмисних помилок в обліку
Ризик-орієнтоване керування обліковою інформацією	Керування обліковою інформацією, виходячи з принципів її ефективного захисту і зберігання
Другий рівень управління обліковою інформацією	
Моніторинг чинників загроз інформаційній безпеці	Контроль окремих випадків витоку чи втрати інформації; навмисного чи ненавмисного перекручення інформації; форс-мажорних обставин, що впливають на стан облікової інформації
Формування елементів системи протидії загрозам	Визначення переліку превентивних дій попередження, профілактики, протидії безпековим загрозам щодо облікової інформації
Розробка положень, політики і процедур в рамках системи безпеки облікової інформації	Регламентация і адміністрування системи безпеки облікової інформації
Третій рівень управління обліковою інформацією	
Контроль за дотриманням вимог безпеки облікової інформації	Моніторинг на постійній основі з наступним коригуванням дій
Оцінка операційної ефективності заходів	Проведення заходів повинно бути економічно доцільним (витрати не повинні перевищувати ефект)

Джерело: побудовано автором на основі [4]

Отже, дослідивши особливості залучення ІТ-аутсорсингу для захисту облікової інформації, обґрунтовано, що підприємство повинно перейматися безпекою своєї облікової інформації, оскільки вона є невід'ємною частиною системи управління.

Список використаних джерел

1. Що таке ІТ-аутсорсинг? URL: <https://bit.ly/2T0XEDg> (дата звернення: 11.05.2020).
2. ІТ-аутсорсинг. URL: <https://bit.ly/2Lp8y1s> (дата звернення: 11.05.2020).
3. ІТ-аутсорсинг. Обслуговування. URL: <https://bit.ly/2Tfaqyr> (дата звернення: 11.05.2020).
4. Засоби підвищення керованості безпекою облікової інформації. URL: <https://bit.ly/2AhwNwd> (дата звернення: 12.05.2020).
5. Захист облікової інформації та кібербезпека підприємства. URL: <https://bit.ly/364AFNf> (дата звернення: 12.05.2020).
6. Система захисту облікової інформації. URL: <https://bit.ly/2Lp8puV> (дата звернення: 12.05.2020).