види кредитів; один клієнт – 1 уповноважений комерційний банк; компенсація не надається учасникам програми «Доступні кредити 5-7-9 %» [8].

Отже, кредитне забезпечення АПК, окрім інших факторів, суттєво залежить від суми коштів державного бюджету, спрямованих на програму здешевлення позик АПК. Чинний механізм здешевлення кредитів із державного бюджету є ефективним інструментом підвищення їх доступності для сільськогосподарських та інших підприємств АПК. На етапі становлення вітчизняної системи сільськогосподарського кредиту слід продовжити період дії цієї державної програми, попередньо її вдосконаливши, враховуючи можливості цифрових технологій.

***Список використаних джерел***


*1. Бондаренко Н. В. Стан пільгового кредитування поточної діяльності сільськогосподарських підприємств. Фінансово-кредитна політика. 2011. № 1. С. 216–222.*

*2. Гудзь О. Є. Удосконалення механізму кредитних субсидій підприємств АПК. Економіка АПК. 2009. № 9. С. 59–61.*

*3. Минкіна Г. О. Механізм державної підтримки підприємств АПК через удосконалення системи кредитування. Науковий вісник Національного університету біоресурсів і природокористування України : зб. наук. пр. / ред. Д. О. Мельничук. К. : НУБПУ, 2009. Вип. 142. Ч. 2. С. 260.*

*4. Непочатенко О. О. Державна підтримка підприємств АПК через удосконалення системи кредитування. Економіка АПК. 2008. № 8. С. 95–100.*

*5. Калашнікова Т. В. Стан і тенденції розвитку аграрної галузі України. Фінанси України. 2010. № 10. С. 29–37.*

*6. Ісаян А. М. Банківське кредитування підприємств АПК в умовах невизначеності. Київ, 2016. С.221.*

*7. Постанова Кабінету Міністрів України «Про порядок використання коштів, передбачених у державному бюджеті для фінансової підтримки заходів в агропромисловому комплексі шляхом здешевлення кредитів» від 29.04.2015р. № 300. URL: https://zakon.rada.gov.ua/laws/show/300-2015-п#Text (дата звернення: 12.11.2020).*

*8. Держпідтримка аграріїв 2020. Кредити, тваринництво, фермерство, техніка, садівництво. URL: https://goo-gl.su/Z0d8KAu (дата звернення: 18.11.2020).*



УДК 657:004



**Муравський Володимир Васильович,**
*д.е.н., професор кафедри обліку і оподаткування,*
*Західноукраїнський національний університет,*
*м. Тернопіль, Україна*


## ОБЛІКОВІ ФАХІВЦІ У ЗАБЕЗПЕЧЕННІ КІБЕРЗАХИСТУ ПІДПРИЄМСТВА

Організація кіберзахисту на платформі системи обліку передбачає розширення функціональних повноважень облікової служби (бухгалтерії) та відділу внутрішнього контролю або введення посади фахівця із кібербезпеки в штат підприємства. Доцільність організаційних трансформацій повинна обґрунтовуватися економічною ефективністю незалежно від розмірів та сфери

діяльності суб'єкта господарювання. За даними звіту Internet Security Threat Report у 2019 році 80 % усіх кібезлочинів адресувалися малим суб'єктам господарювання через використання поштових систем, соціальних мереж та хмарних сервісів [1]. Основним мотиватором кібератак на невеликих за розміром підприємствах є відсутність фахівців чи відділу зі забезпечення кібербезпеки. Відповідно, існує більша імовірність, що кібератаки будуть успішними на малих суб'єктах господарювання. Функції кіберзахисту на таких підприємствах можуть успішно виконувати фахівці відділу обліку чи контролю.

Відповідно, посади фахівців із кіберзахисту доцільно поділити на три групи: фахівці з інформаційного захисту (облікові фахівці), працівники служби контролю (фахівці з тестування інформаційних систем на проникнення, аналітики систем забезпечення кіберзахисту, внутрішні контролери, безпекові аудитори, інспектори з організації захисту конфіденційної інформації), персонал технічного забезпечення (системні адміністратори, адміністратори комп'ютерних мереж, програмісти з спеціалізованих комп'ютерних).

Працівників першої категорії доцільно професійно навчати в рамках освітнього процесу підготовки облікових фахівців. Особами другої групи можуть бути облікові працівники, які мають практичний досвід у сфері кіберзахисту підприємств та здобули додаткові мультидисциплінарні вміння та навички. І лише працівників третьої категорії готують за технічними напрями підготовки фахівців, що не передбачає отримання ґрунтовних знань з економічних дисциплін (у тому числі – обліку, аналізу та контролю).

Таким чином, функціональними обов'язками облікових фахівців першої та другої групи є:

– виявлення уразливих місць системи та моделювання можливої ситуації кібервпливу з позиції загроз і пов'язаних із ними ризиків;

– контроль надійності функціонування системи захисту облікової інформації, розроблення заходів безпеки на випадок непередбачуваних подій;

– віднесення облікової інформації до категорії обмеженого доступу (службової і комерційної таємниць, іншої конфіденційної інформації);

– розробка положень, політики і процедур у рамках системи безпеки облікової інформації;

– упровадження розроблених заходів безпеки та випробування системи з оцінкою її результативності, за необхідності внесення коригувань;

– встановлення користувачам комп'ютерної системи бухгалтерського обліку необхідних реквізитів захисту;

– навчання користувачів комп'ютерної інформаційної системи правилам безперервної обробки інформації;

– контроль за дотриманням користувачами комп'ютерної інформаційної системи та персоналом підприємства встановлених правил роботи з обліковою інформацією [2, с. 501].

Важливою є регламентація функціональних обов'язків із забезпечення кіберзахисту в посадових інструкціях облікових фахівців з визначенням відповідальності за порушення кібербезпеки підприємств. Така відповідальність може бути не лише адміністративною, але й кримінальною у зв'язку ймовірністю

завдання шкоди неправомірними вчинками облікових фахівців не лише кібербезпеці окремих підприємств, але й національній безпеці галузі чи сектору економіки. Додатково визнання відповідальності за реалізацію ефективного кіберзахисту підприємств рекомендовано помістити у Кодекс етики професійних бухгалтерів, який імплементується і в Україні. Зокрема, доцільно розширити зміст принципу надання облікових послуг – конфіденційність (нерозголошення третім особам облікової інформації), в якому ідентифікувати облікового фахівця також як суб'єкта організації захисту.

У фахівців служби кіберзахисту повинно бути всебічне розуміння інформаційних процесів на підприємстві, інформаційно-технічної інфраструктури, ситуації щодо взаємодії із зовнішніми стейкхолдерами та контрагентами, алгоритму функціонування спеціалізованого програмного забезпечення для автоматизації управління, юридичних аспектів функціонування суб'єкта господарювання тощо [3]. Усі ці знання в значній мірі акумульовані обліковими працівниками.

Додатково фахівці з бухгалтерського обліку, що не є їм на сьогодні властиве, зобов'язані контролювати: ефективність функціонування брандмауерів, появу новітніх технологій антивірусного програмного забезпечення, стан оновлення спеціалізованих комп'ютерних програм до актуальних версій, а також порядок використання співробітниками надійних паролів для захисту конфіденційної інформації. Комплексне поєднання зазначених вмінь та знань дасть змогу обліковим фахівцям моніторити стан внутрішніх та зовнішніх загроз.

***Список використаних джерел***

*1. Internet Security Threat Report / Symantec. Mountain View: Symantec Corporation, 2019. 61 p.*

*2. Вітер С.А. Світлишин І.І. Захист облікової інформації та кібербезпека підприємства. Економіка і суспільство: електронне фахове видання. 2017. № 11. С. 497–502.*

*3. Муравський В. В. Комп'ютерно-комунікаційна форма обліку : монографія. Тернопіль : ТНЕУ, 2018. 486 с.*

УДК 657.631.6

**Нежива Марія Олександрівна,**
*к.е.н., доцент кафедри фінансового аналізу та аудиту,*
*Київський національний торговельно-економічний університет,*
*м. Київ, Україна*

## АУДИТ В УМОВАХ ДИДЖИТАЛІЗАЦІЇ: СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

В сучасному світі процеси диджиталізації змінюють не лише повсякденне життя, а й здійснення бізнесу. Попередні бізнес-процеси вже не є достатньо ефективними, і тому постає необхідність їх вдосконалення. Адже гнучкість і