УДК 657.004.056
DOI: https://doi.org/10.32840/1814-1161/2021-6-26

Антоненко Н.В.
кандидат економічних наук,
доцент кафедри фінансів, обліку і аудиту
Національного транспортного університету

Пасічник П.А.
студент
Національного транспортного університету

Antonenko Nadiia
Candidate of Economic Sciences,
Associate Professor at the Department of Finance,
Accounting and Auditing
National Transport University

Pasichnyk Pavlo
Student
National Transport University

КІБЕРЗАГРОЗИ В ОБЛІКОВИХ СИСТЕМАХ

CYBER THREATS IN ACCOUNTING SYSTEMS

У статті здійснено аналіз кібернетичних загроз, які можуть зруйнувати облікові системи, та запропоновано заходи щодо кіберзахисту облікової інформації. Визначено сутність облікових систем підприємства, а також обґрунтовано актуальність впровадження на підприємствах системи кібербезпеки облікової інформації. Обґрунтовано необхідність розроблення заходів щодо захисту облікової інформації в контексті кібербезпеки та розглянуто деякі питання її організації. Акцентовано увагу на тому, що проблеми захисту від несанкціонованого доступу не лише зводяться до технічних аспектів захисту інформаційних ресурсів, але й потребують врахування людського фактору. Визначено, що найбільш значущими серед кіберзагроз для користувачів облікової інформації є комп'ютерні віруси та несанкціонований доступ до бази даних з боку осіб, які не мають на це прав. Подальші дослідження проблеми запропоновано зосередити на розробленні сучасних антивірусних засобів підтримки кібербезпеки облікової інформації.

Ключові слова: *кіберзагроза, облікова система, комп'ютерний вірус, кібербезпека, захист інформації, антивірусна програма.*

В статье осуществлен анализ кибернетических угроз, которые могут разрушить учетные системы, и предложены меры по киберзащите учетной информации. Определена сущность учетных систем предприятия, а также обоснована актуальность внедрения на предприятиях системы кибербезопасности учетной информации. Обоснована необходимость разработки мер по защите учетной информации в контексте кибербезопасности и рассмотрены некоторые вопросы ее организации. Акцентировано внимание на том, что проблемы защиты от несанкционированного доступа не только сводятся к техническим аспектам защиты информационных ресурсов, но и требуют учета человеческого фактора. Определено, что наиболее значимыми среди киберугроз для пользователей учетной информации являются компьютерные вирусы и несанкционированный доступ к базе данных со стороны лиц, не имеющих на это прав. Дальнейшие исследования проблемы предложено сосредоточить на разработке современных антивирусных средств поддержки кибербезопасности учетной информации.

Ключевые слова: *киберугроза, учетная система, компьютерный вирус, кибербезопасность, защита информации, антивирусная программа*

The article analyzes the cyber threats that can destroy accounting systems, and proposes measures to cyber protect accounting information from unauthorized access by unauthorized persons, as well as viruses. The urgency of the topic is due to the fact that the modern development of information technology has led to the emergence of cybercriminals who, through illegal actions and technologies, interfere in the work of information systems and commit theft and destruction of information. The above fact indicates a significant increase in the number of crimes in the field of information technology in the near future, especially in the accounting systems of economic entities. Thus, the relevance of the research topic is beyond doubt. The article defines the essence of accounting systems of the enterprise, as well as substantiates the relevance of the introduction of cyber security systems of accounting information in enterprises. Based on a study of the work of scientists and taking into account the situation in which businesses operate today, the threat of cyber-attacks is assessed in the context of the consequences for accounting

and reporting. Computer viruses and unauthorized access to the database by unauthorized persons have been identified as the most significant cyber threats to users of accounting information. It has been proven that the greatest threat to software users is posed by such virus programs as spyware, Trojan horse programs, worms, invisible viruses, and virus logic bombs. The implementation of measures to protect accounting information in the context of cyber security is substantiated and some aspects of its organization are considered. It is noted that to ensure the security of computer systems and networks, it is necessary to install a licensed version of the antivirus on the computer and refuse to download free programs from suspicious sites. Emphasis is placed on the fact that the problems of protection against unauthorized access are not only reduced to the technical aspects of protection of information resources, but also require consideration of the human factor. Further research on the problem is proposed to focus on the development of modern anti-virus tools to support cybersecurity of accounting information.

Keywords: *cyber threat, accounting system, computer virus, cybersecurity, information protection, antivirus program.*

Постановка проблеми. Поява у світі останнім часом величезної кількості нових ІТ-компаній та програмних продуктів свідчить про стрімкий розвиток інформаційних технологій, які посідають в економіці будь-якої держави одне з найважливіших місць. Із впровадженням у бізнес-процеси суб'єктів господарювання повної або часткової автоматизації у керівництва компаній з'являється більше свободи й ресурсів для розв'язання складних управлінських задач, що впливають на економічний розвиток країни. Дедалі активніше застосовують цифрові технології державні та місцеві органи влади. Засобами підвищення ефективності та прозорості усіх фінансових операцій, що здійснюють підприємства, є використання банками цифрових платіжних інструментів та інноваційних платіжних послуг.

Проте стрімкий розвиток інформаційних технологій зумовив появу кіберзлочинців, які за допомогою незаконних дій і технологій здійснюють розкрадання та руйнування інформації в інформаційних системах і мережах. Вищезазначений факт свідчить про те, що найближчим часом може суттєво збільшитись кількість злочинів у сфері інформаційних технологій, особливо в облікових системах суб'єктів господарювання.

З огляду на суттєву роль захисту програмного забезпечення від несанкціонованого доступу виникає необхідність визначення основних кіберзагроз, що виникають у ході роботи фахівців в облікових системах підприємств.

Аналіз останніх досліджень і публікацій. Проблемами кібербезпеки інформаційного простору займались такі науковці, як Д.О. Ричка [1], І.Л. Грабчук [2], С.А. Вітер [3], І.І. Світлишин [3], В.І. Клименко [4]. Питання визначення загроз кібербезпеки під час захисту облікової інформації розглядали у своїх дослідженнях Ю.Ю. Мороз [5], Ю.С. Цаль-Цалко [5].

Виділення не вирішених раніше частин загальної проблеми. Проте нині проблеми захисту облікової інформації від кіберзагроз, що являють собою віруси і несанкціонований доступ до баз даних, залишаються малодослідженими.

Формулювання цілей статті **(постановка завдання)**. Метою статті є аналіз кібернетичних загроз, що можуть зруйнувати облікові системи, та визначення заходів щодо кіберзахисту облікової інформації.

Виклад основного матеріалу дослідження. Невід'ємним елементом облікової політики України є облікова система, яка слугує інформаційною базою для управління господарською діяльністю суб'єктів господарювання. Більшість підприємств для здійснення облікових процесів застосовує комп'ютеризовану форму ведення бухгалтерського обліку, що передбачає використання таких програмних продуктів, як «1С:Підприємство.8», «BAS Бухгалтерія», «BAS Бухгалтерія КОРП», «BAS Комплексне управління підприємством», «Бухгалтерська програма SAP». Ці комп'ютерні системи працюють із великими обсягами інформації, і будь-яке несанкціоноване втручання у роботу вищезазначених програм може привести до втрати облікової інформації, що впливає на достовірність фінансової звітності підприємств і організацій.

З того часу як комп'ютерна техніка увійшла в усі сфери людського життя й перестала бути прерогативою великих компаній, перед розробниками програмного забезпечення і користувачами локальних та глобальних мереж гостро постало питання кібербезпеки. Про важливість захисту інформації сьогодні свідчать такі факти: у 2020 році було зафіксовано 1 120 витоків інформації і кібератак, а також зламано близько 20,1 млрд. записів, що на 50% більше, ніж у 2019 році [6]. Зазвичай кількість кібератак та інформаційних витоків приблизно однакова, але у 2020 році кількість кібератак (349) перевищила кількість витоків (771) вдвічі [6]. Причиною такого різкого скачку кіберзлочинності став COVID-19, оскільки через вірус значна кількість організацій перейшла на дистанційну форму роботи через комп'ютерну мережу Інтернет, а зловмисники отримали більше можливостей несанкціонованого доступу до баз даних. Зазвичай зловмисників цікавить приватна інформація, яка стосується управлінського обліку великих, середніх та малих підприємств і містить комерційну таємницю.

Існує багато способів викрадення інформації через комп'ютер, але найголовнішою проблемою для користувачів є віруси. Д.О. Ричка трактує поняття комп'ютерного вірусу як «спеціально створеної програми, яка сама здатна приєднуватися до інших програм і у разі запуску спричиняє різні негативні наслідки (псує файли і каталоги, перекручує інформацію) та створює інші перешкоди у роботі ЕОМ» [1]. У статті Д.О. Ричка [1] зауважує, що існують різні види вірусів, які поділяються на серйозні віруси й віруси-жарти. Віруси-жарти особливої загрози користувачеві не несуть, але можуть спричинити певні незручності. Найгірше, що можуть зробити віруси-жарти, – це зламати операційну систему, але після її переустановлення комп'ютер буде працювати, як зазвичай.

Найбільшу загрозу для користувачів програмних продуктів мають такі серйозні віруси:

– програми, що після проникнення в комп'ютер нейтралізують паролі та інші види захисту комп'ютерних програм;

– програми-шпигуни – програми, що проникають на електронно-обчислювальний пристрій і пересилають інформацію власника комп'ютера сторонній особі;

– вірусні програми «троянський кінь», які відрізняються від інших вірусів тим, що не можуть копіювати самі себе і являють собою шкідливу програму; вірус «троянський кінь» захоплює окремий файл, видозмінює або руйнує його; найнебезпечнішим є те, що цей вірус, перебуваючи у вихідному коді ліцензійної програми, може її імітувати й навіть повністю замінювати; зазвичай такі програми використовуються для викрадення паролів і надсилання їх зловмиснику задля проведення банківського шахрайства; в деяких версіях цього вірусу є система самознищення, коли програма не залишає ніяких слідів;

– програми-«хробаки» – ще один вид вірусних програм, які схожі на програми «троянський кінь», бо не можуть реплікувати самі себе: вони проникають у програму оброблення даних і можуть змінювати або знищувати дані в обліковій системі;

– вірусні програми «логічні бомби» – програми, які створені за принципом програм «троянський кінь», проте містять таймер, який запускається у визначений час;

– віруси-невидимки – віруси, що уникають антивірус і приховують усі зміни, що вносять в розділи операційної системи.

Отже, комп'ютерний вірус – це програми, що проникають до електронно-обчислювального механізму, зменшують продуктивність роботи приладу й можуть знищити або змінити інформацію на ньому [7].

Наочним прикладом нищівної дії комп'ютерного вірусу є вірус "Pety.A", який завдав шкоди 12,5 тисячам комп'ютерів у нашій державі та поширився на 64 країни світу [2]. Вірус "Pety.A" розпочав свою діяльність в Україні 27 червня 2017 року, а потім поширився на інші країни. Як показало розслідування, вірус поширився через програму "M.E.Doc". Під час установлення оновлення ця програма запрошувала дозвіл на внесення змін у комп'ютер із правами адміністратора. Зловмисники скористались цією вразливістю і вписали вірусний код у останнє оновлення програми. На рис. 1 і рис. 2 представлено сучасний процес оновлення програми "M.E.Doc".

Відмовитися від оновлення користувачі не можуть, оскільки воно містить актуальні довідники, бланки для подачі звітності та зміни до вже наявних форм документів. Таким чином, у 2017 році програма "M.E.Doc" виявила свої слабкі сторони, а дозволом її подальшого використання з боку держави стала вимога доведення рівня її захисту до рівня гарантій Г-3 [2]. Нормативний документ ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» встановлює критерії оцінки захищеності інформації. Рівень Г3 відповідає рівню EAL 4 міжнародного стандарту ISO/IEC 15408 "Common Criteria for Information Technology Security Evaluation".

Автори статті «Захист облікової інформації та кібербезпека підприємства» С.А. Вітер та І.І. Світлишин [3] рекомендують для захисту комп'ютерів установлювати антивірусні програми, але зазначають, що не від усіх шкідливих програм може захистити антивірус, адже принцип його роботи полягає в пошуку вірусного коду, який деякі програми-шпигуни маскують. Дослідники доходять висновку, що для гарантування безпеки комп'ютерних систем і мереж необхідно встановлювати на ЕОМ ліцензійну версію антивірусу і відмовитись від скачування з підозрілих сайтів безкоштовних програм. Проте абсолютного захисту від несанкціонованого доступу до інформації не існує, адже повністю захищений комп'ютер – це той, що знаходиться в броньованому сейфі і не підключений до жодної мережі, навіть

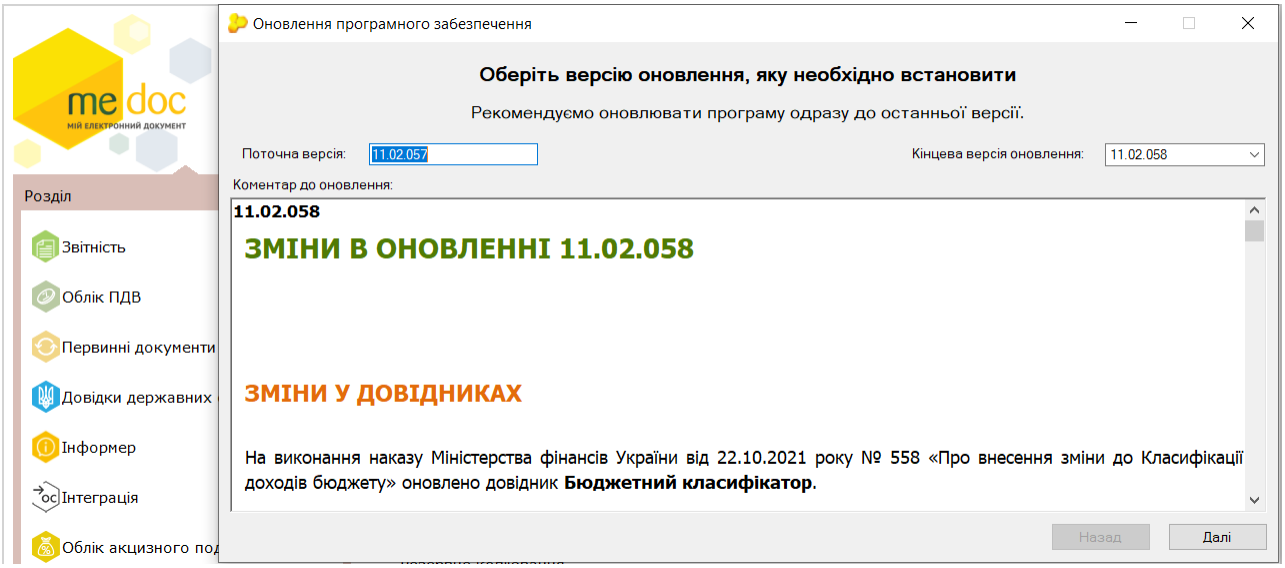

Рис. 1. Початок оновлення програмного забезпечення "M.E.Doc"

Джерело: створено авторами

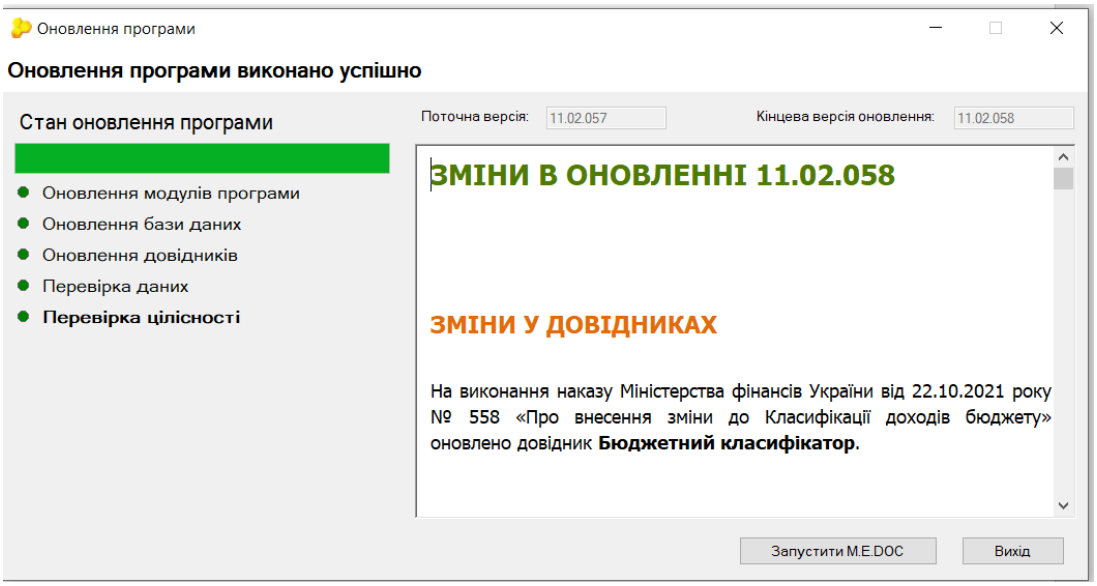

Рис. 2. Закінчення оновлення програмного забезпечення “M.E.Doc”

Джерело: створено авторами

електричної. Зазвичай таким приладом користуватися не можна. Таким чином, найкращий захист від нападу на облікові системи – недопущення його усіма способами.

Як ми вже зазначали, для хакерів найбільш привабливою є інформація щодо управлінського обліку підприємства, яка містить комерційну таємницю. Захист облікової системи потрібно здійснювати також тому, що більша частина інформації знаходиться в електронному вигляді і має високий ступінь вразливості до хакерських атак. Проте не тільки хакери становлять загрозу інформації в облікових системах. У осіб, які працюють на підприємстві, зловмисники можуть безпосередньо викрасти інформацію на цифрових носіях, здійснивши крадіжку ноутбуку, флешки, токену тощо.

Ще однією причиною витоку інформації є інсайдери – зловмисники, що знаходяться всередині організації. Для того щоб уникнути несанкціонованого доступу до конфіденційної інформації, деяким співробітникам компанії обмежують доступ до певного функціоналу програми.

Розглянемо порядок обмеження прав користувачів на прикладі організації доступу до довідників і документів у програмі «1С:Підприємство.8». Ця процедура дає змогу керівнику підприємства розмежовувати доступ до бази даних, стежити за зміною документів, організовувати ведення журналу реєстрації роботи з програмою, визначати коло користувачів, яким надано право на видалення документів і записів з бази даних підприємства.

На рис. 3 представлено скріншот екрану з програми «1С: Управління торговим підприємством для України. 8.3», який містить список користувачів і журнал реєстрації роботи з програмою. У програмі «1С:Підприємство.8» для керування доступом користувачів використовується окремий об’єкт метаданих, який називається роллю. Роль визначає набір прав користувача, які він має. Так, для кожного з об’єктів (довідників, документів) розробник установлює свій набір прав, таких як читання, запис, додавання, зміна. Набір доступних прав – це сукупність усіх дозволів у ролях користувача. Кожному користувачеві, відповідно до посади, надані певні права доступу: повні права доступу надаються адміністратору й головному бухгалтеру, а всі інші співробітники мають обмежені права доступу.

Вищезазначені заходи дають змогу під час роботи з обліковими системами уникнути несанкціонованого доступу до конфіденційної інформації з боку співробітників підприємств і організацій.

Розглянемо причини витоку інформації в банківських та фінансових секторах. Автор статті «Внутрішні загрози інформаційній безпеці організації» В.І. Клименко [4] зазначав, що більшість випадків витоку інформації, які трапилися в облікових системах банків і фінансових установ, виникла не через вразливість інформаційних систем, а через недбалість працівників. Найпопулярнішими з них є такі:

– відкриття файлів від невідомих адресатів, які надійшли через пошту або через інший вид швидкого обміну повідомленнями;

– встановлення неліцензійного програмного забезпечення;

– використання простих паролів (наприклад, 12345678 чи 11111111) або використання одного й того самого пароля впродовж тривалого часу;

– «запам’ятовування» паролів у публічних місцях (ресторанах, кафе, бібліотеках);

– робота з конфіденційними документами в публічних місцях;

– завантажування розважальних програм та відвідування розважальних сайтів;

– винесення конфіденційної інформації за межі організації.

Далі зупинимось на питаннях забезпечення кібербезпеки баз даних облікових систем. Погоджуємось із дослідниками С.А. Вітер та І.І. Світлишин, які про-

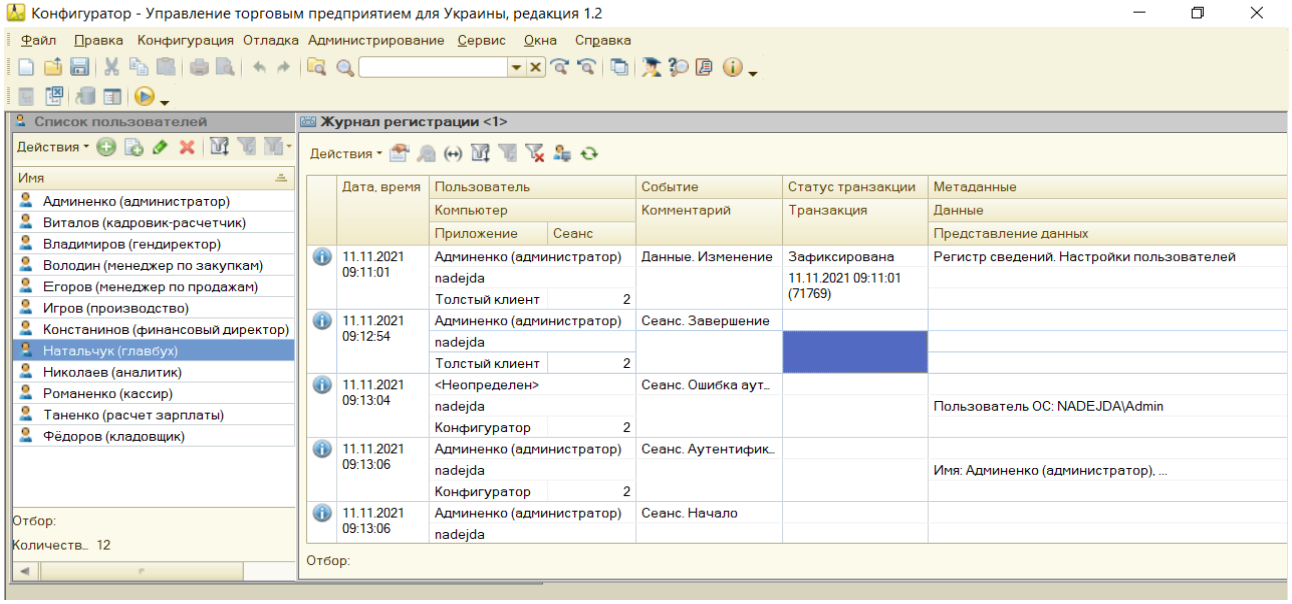

Рис. 3. Налаштування прав доступу у режимі користувача
в конфігураторі програми «1С: Управління торговим підприємством. 8.3»

Джерело: створено авторами

понують такі заходи щодо захисту облікової інформації від кіберзлочинців [3]:

– організаційні (обмеження незаконного доступу до приватної інформації);

– технічні (попередження несанкціонованих осіб щодо навмисного вторгнення в облікову інформацію за допомогою технічних засобів або програмного забезпечення);

– кадрові (підвищення компетентності та відповідальності у використанні інформаційних технологій працівниками організації).

Крім зараження облікових систем вірусами внаслідок некомпетентних дій працівників підприємств, відбувається витік, втрата або викривлення інформації [8], тому для надійного зберігання бази даних потрібно на електронно-обчислювальний пристрій установлювати якісне програмне забезпечення. Програмні продукти повинні відповідати стандарту ISO/IEC 25010 щодо забезпечення високого рівня таких характеристик якості [9]:

– придатність, точність, інтероперабельність, безпечність (невід'ємна частина існування набору функцій та їх заданих властивостей, які характеризують функціональність інформаційного простору);

– відмовостійкість, відновлюваність (складові частини надійності, що впливають на здатність програмного забезпечення підтримувати високий рівень продуктивності за певних умов протягом зазначеного періоду часу);

– зрозумілість, привабливість, працездатність (атрибути зручності, які впливають на зусилля, необхідні для використання, та на індивідуальну оцінку такого використання заявленим набором користувачів);

– утилізація ресурсів (складова частина ефективності, яка впливає на взаємозв'язок рівня продуктивності програмного забезпечення та кількості ресурсів, що використовуються за зазначених умов);

– атрибути ремонтопридатності, що впливають на зусилля, необхідні для внесення певних змін до бази даних;

– адаптивність, можливість безперешкодного встановлення програмного забезпечення (складові частини переносності, що впливають на можливість передачі програмного забезпечення з одного середовища до іншого).

В стандарті ISO/IEC 25010 наголошується на важливості постійного підвищення якості, зниження ризиків, пов'язаних із розробленням та обслуговуванням програмного забезпечення, а також на необхідності систематичного визначення якості елементів бази даних. Все програмне забезпечення, що створюється сьогодна, повинно відповідати вимогам вищезазначеного стандарту.

Висновки. В результаті здійснення аналізу кіберзагроз в облікових системах пропонується виділяти логічний та фізичний види захисту облікової інформації.

Логічна безпека реалізується за допомогою технології, яка обмежує доступ до системи та інформації суб'єкта господарювання. Фізична безпека використовує заходи, яких підприємство чи установа вживає для захисту своїх даних, об'єктів або ресурсів, що зберігаються на фізичних носіях. Логічна безпека полягає в такому:

– визначення слабких сторін діяльності підприємства для забезпечення захисту облікової інформації від кібератак;

– інформування працівників підприємств про загрози витоку інформації через доступ до їх особистих сторінок у соціальних мережах, поштових скриньок тощо; в межах цього заходу необхідно ознайомити працівників з інтернет-ресурсами, які слід використовувати на робочому місці, а надати їм інформацію щодо тих типів електронних листів та вкладень

до них, які можна відкривати без страху отримати вірус.

З точки зору фізичної безпеки слід наголосити на таких особливостях:

– найважливіша інформація повинна зберігатися у зашифрованому вигляді;

– загрозою пошкодження або доступу до конфіденційної інформації є не тільки програмне забезпечення, але й викрадення носіїв, на яких зберігають інформацію; у зв'язку з цим адміністратори внутрішніх мереж підприємств повинні використовувати фізичні засоби, що блокують доступ до бази даних.

Як висновок з дослідження необхідно зазначити, що для створення кібернетичного захисту облікової інформації на кожному підприємстві потрібно розробити відповідну програму дій, сфера застосування яких не обмежується виключно технічними аспектами, а поширюється також на людські ресурси. Перспективою подальших досліджень може бути розроблення сучасних антивірусних засобів підтримки кібербезпеки облікової інформації.

Бібліографічний список:

1. Ричка Д.О. Комп'ютерні віруси – шкідливі програмні засоби, рушійна сила модифікації. *Науковий вісник Херсонського державного університету.* 2018. Вип. 1. Т. 2. С. 89–93.
2. Грабчук І.Л. Організація захисту облікової інформації в умовах гібридної війни. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналіз.* 2018. Вип. 3 (41). С. 20–24.
3. Вітер С.А., Світлишин І.І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. Вип. 11. С. 497–502.
4. Клименко В.І. Внутрішні загрози інформаційній безпеці організації. *Вісник НБУ.* 2008. № 5. С. 62–63.
5. Цаль-Цалко Ю.С., Мороз Ю.Ю. Облікова політика підприємства та її кібербезпека. *Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства :* збірник наукових праць. Т. IV. Ч. І. Житомир : Рута, 2017. С. 8–11.
6. Статистика з кібербезпеки за 2020 рік. 10 Guards. URL: https://10guards.com/ua/articles/2020-cybersecurity-statistics (дата звернення: 10.11.2021).
7. Види комп'ютерних вірусів і способи боротьби з ними. URL: https://web-3.ru/comp/virus/?act=full&id_article=1411 (дата звернення: 12.11.2021).
8. Поняття, сутність, значення захисту інформації. ІнфоБезпека. URL: http://www.infobezpeka.com/publications/?id=102 (дата звернення: 12.11.2021).
9. ISO/IEC 25010. ISO 25000. URL: https://iso25000.com/index.php/en/iso-25000-standards/iso-25010?limit=3&limitstart=0 (дата звернення: 15.11.2021).

References:

1. Rychka D.O. (2018) Komp'juterni virusy – shkidlyvi proghramni zasoby, rushijna syla modyfikaciji [Computer viruses are malicious software, the driving force of modification]. *Scientific Bulletin of Kherson State University,* rel. 1, vol. 2, pp. 89–93.
2. Ghrabchuk I.L. (2018) Orghanizacija zakhystu oblikovoji informaciji v umovakh ghibrydnoji vijny [Organization of protection of accounting information in the conditions of hybrid war]. *Problems of theory and methodology of accounting, control and analysis,* vol. 3 (41), pp. 20–24.
3. Viter S.A., Svitlyshyn I.I. (2017) Zakhyst oblikovoji informaciji ta kiberbezpeka pidpryjemstva [Protection of accounting information and cybersecurity of the enterprise]. *Economy and society,* vol. 11, pp. 497–502.
4. Klymenko V.I. (2008) Vnutrishni zaghrozy informacijnij bezpeci orghanizaciji [Internal threats to information security of the organization]. *Bulletin of the NBU,* no. 5, pp. 62–63.
5. Calj-Calko Ju.S., Moroz Ju.Ju. (2017) Oblikova polityka pidpryjemstva ta jiji kiberbezpeka [Accounting policy of the enterprise and its cybersecurity]. *Accounting, analysis and control in the context of modern concepts of managing the economic potential and market value of the enterprise:* a collection of scientific papers, vol. IV, part 1, Zhytomyr: "Ruta", pp. 8–11.
6. Statystyka z kiberbezpeky za 2020 rik [Cybersecurity statistics for 2020]. 10 Guards. URL: https://10guards.com/ua/articles/2020-cybersecurity-statistics.
7. Vydy komp'juternykh virusiv i sposoby borotjby z nymy [Types of computer viruses and ways to fight them]. URL: https://web-3.ru/comp/virus/?act=full&id_article=1411.
8. Ponjattja, sutnistj, znachennja zakhystu informaciji [The concept, essence, importance of information protection]. *InfoSecurity*. URL: http://www.infobezpeka.com/publications/?id=102.
9. ISO/IEC 25010. ISO 25000. URL: https://iso25000.com/index.php/en/iso-25000-standards/iso-25010?limit=3&limitstart=0.