УДК 657:004.056
DOI: http://dx.doi.org/10.26642/pbo-2018-3(41)-20-24

І.Л. Грабчук, к.е.н., доц.
Житомирський державний технологічний університет

Організація захисту облікової інформації в умовах гібридної війни [1]

Здійснення господарської діяльності суб'єктами господарювання відбувається в складних умовах – умовах ведення гібридної війни, яка характеризується застосуванням специфічних методів, зокрема кібератак. Доведено, що кібербезпека повинна розглядатися як розширення інформаційної безпеки та охоплювати захист підприємства, яке використовує ресурси в кіберсередовищі, та захист будь-яких інших активів, які зазнають ризику внаслідок використання інформаційно-комп'ютерних технологій. Описано наслідки кібератак для підприємств, які вибирають стаціонарне та хмарне програмне забезпечення. Обґрунтовано недоцільність використання останнього великими та середніми підприємствами в умовах гібридної війни. Описано завдання на державному рівні, яких слід дотримуватися для перевірки на шкідливість програмного забезпечення. Проведено критичний аналіз праць науковців щодо оцінки визначених ними заходів для захисту облікової інформації. Обґрунтовано заходи для мінімізації загроз бухгалтерській інформації при кібератаках в частині забезпечення логічної (ідентифікація ризиків, розгляд забезпечення інформаційної безпеки підприємства як частини корпоративної культури) та фізичної (шифрування даних, фізичний захист технічного забезпечення) безпеки.

Ключові слова: *облікова інформація; гібридна війна; кібербезпека; інформаційна безпека; безпека інформаційно-комп'ютерних технологій.*

Актуальність теми. Війни можуть приймати різні форми, які можуть бути близькими та віддаленими від класичних концепцій війн. Саме тому гібридна війна передбачає поруч з використанням військових сил також і кібератак та пропаганди. Для характеристики незаконної поведінки в кіберпросторі використовуються різні поняття, зокрема такі, як: хактивізм, кіберзлочинність, кібертерроризм.

На відміну від звичайної війни, «центр тяжіння» в гібридній війні є населенням цільової країни. Хоча військові фахівці вже кілька років обговорюють методи гібридної війни, російська агресія проти України у 2014 році підкреслила важливість інформаційної війни в новому поколінні воєн [9].

На нинішньому етапі на державному рівні приймаються заходи, які спрямовані на забезпечення інформаційної безпеки (зокрема обмеження доступу до шкідливих інтернет-ресурсів, заборона співпраці з суб'єктами господарювання, які становлять загрозу безпеці України). Проте підприємства повинні також вживати заходи щодо захисту інформації, витік якої може завдати їм збитків. Значна частина такої інформації формується саме в системі бухгалтерського обліку, а враховуючи особливості його організації в сучасних умовах, це відбувається з використанням інформаційно-комп'ютерних технологій.

Аналіз останніх досліджень та публікації, на які спирається автор. Питання захисту облікової інформації піднімалися в працях таких науковців, як, Г.І. Ляхович, В.М. Рожелюк, В.А. Шпак. Окремі аспекти щодо даного питання в контексті кібербезпеки розкривають С.А. Вітер, І.І. Світлишин, А.С. Марков, В.Л. Цирлов.

Метою статті є дослідження специфіки загроз, які виникають в умовах ведення гібридної війни, а також обґрунтування заходів захисту облікової інформації в таких умовах.

Викладення основного матеріалу. Розкриваючи особливості захисту інформації в мовах гібридної війни, слід визначитися з такими поняттями, як інформаційна безпека та кібербезпека, які часто використовуються як синоніми. Вважаємо, що кібербезпека повинна розглядатися як розширення інформаційної безпеки, вона передбачає також захист підприємства, яке використовує ресурси в кіберсередовищі, та захист будь-яких інших активів, у тому числі тих, що належать підприємству, які зазнають ризику внаслідок використання інформаційно-комп'ютерних технологій. Інформаційна безпека та кібербезпека перетинаються саме в частині застосування інформаційно-комп'ютерних технологій (рис. 1).

В межах нашого дослідження будемо приділяти увагу саме тій частині, яка пов'язана з захистом інформації, що зберігається чи передається з використанням інформаційно-комп'ютерних технологій. Адже саме така інформація на сьогодні характеризує облікову та відповідає специфіці веденню гібридної війни.

Одним із найпоширеніших видів інформаційних загроз з використанням інформаційно-комп'ютерних технологій є вірусні атаки, що пошкоджують не тільки програмне забезпечення комп'ютерів, але і призводять до їх поламок та несправностей. Вірусні атаки прирівнюються до кібернетичних атак (кібератак).

[1]* Роботу виконано в межах НДР № 48 «Трансформація соціальної відповідальності бізнесу в умовах гібридної війни»

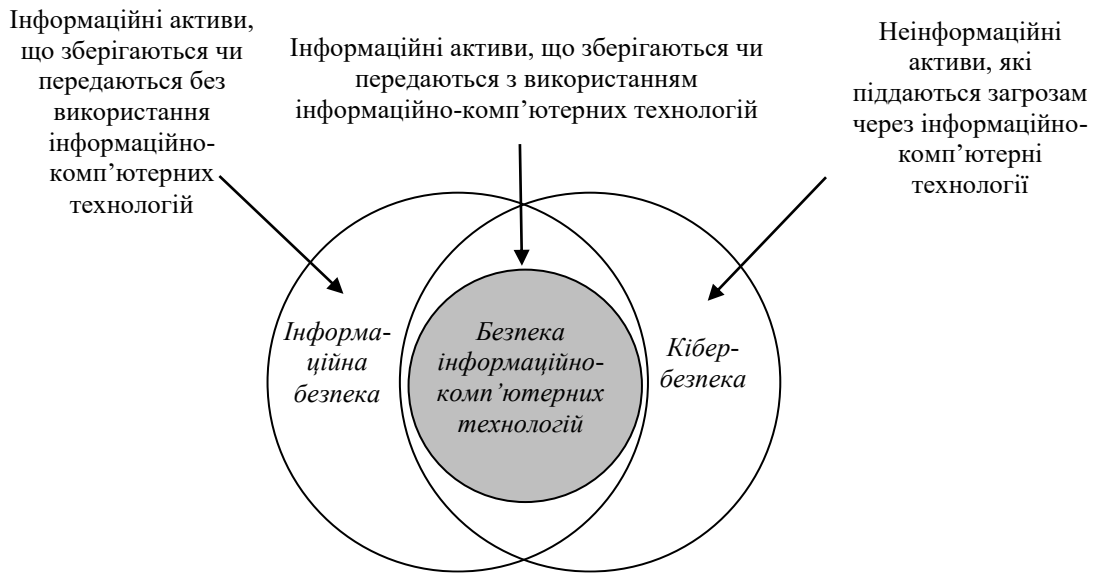

Рис. 1. Зв'язок між інформаційною безпекою, кібербезпекою та безпекою інформаційно-комп'ютерних технологій [10, p. 101]

Об'єктом кібератаки можуть бути:
- комп'ютерні системи в цілому (їх нормальне функціонування);
- такі компоненти комп'ютерних систем, як: інформаційні ресурси;
- дані, що передаються каналами зв'язку;
- програмні та технічні засоби тощо [6].

Яскравим прикладом кібернетичної атаки в Україні стала подія із вірусом «Petya.A». 27 червня 2017 року вранці відбулася цілеспрямована вірусна атака на різні установи, серед яких були «Укренерго», ДТЕК, «Нова пошта», секретаріат КМУ, «Ощадбанк», аеропорт «Бориспіль», «Укрпошта» і київський метрополітен. Через несправність систем перестали працювати банки, державні установи, приватні підприємства. Як повідомляє Microsoft у блозі компанії, хакерська атака почалася з України, а потім відбулася і в 64 інших країнах. Весь процес був запущений о 10.30 ранку 27 червня і до обіду загроза поширилася по всій Україні; всього було інфіковано 12,5 тисяч комп'ютерів [2].

Ця кібератака спровокувала зупинення роботи систем електронного документообігу та прийняття електронної звітності контролюючими органами. Після проведення низки досліджень та розслідувань, встановлено, що вірус «Petya.A» був поширений через бухгалтерське програмне забезпечення з формування та подання звітності «M.E.Doc». Вірусний код був вбудований в одне із останніх оновлень даного програмного забезпечення, яке встановили більшість користувачів. Оскільки такі оновлення зазвичай містять нові форми звітності та нові бланки документів, то їх необхідно встановлювати у програмному забезпеченні «M.E.Doc». При оновленні користувачем дається згода на доступ програми до змін налаштувань комп'ютера, що і є джерелом появи інформаційної загрози.

Запобігти кібератакам технічно не є можливим, незалежно від складності систем захисту. Проте, своєчасне виявлення та швидке адекватне реагування на кібератаки дозволяє значно мінімізувати наслідки від таких атак. Крім того, лише здійсненням кібернетичної атаки можна виявити сильні та слабкі сторони системи захисту певних комп'ютерних систем, їх уразливості, встановити елементи захисту, що потребують удосконалення [2].

Кібератака вірусом «Petya.A» показала слабкі сторони систем та програмного забезпечення. Так, слабкість захисту файлів оновлень програмного забезпечення «M.E.Doc» вказала на необхідність покращення систем захисту інформації на комп'ютерах та розробки алгоритмів дій при реалізації схожих інформаційних загроз.

Все це вимагає застосування ряду заходів захисту як на державному рівні, так і на рівні конкретного суб'єкта господарювання.

Узагальнюючи дослідження науковців [4], на державному рівні до основних завдань, які дозволяють знизити загрози, пов'язані з використанням програмного забезпечення, слід віднести:

1) підвищення контролю захищеності систем шляхом впровадження технологій аналізу захищеності, в першу чергу, тестування на проникнення;

2) підвищення контролю безпеки програмних продуктів шляхом впровадження технологій аудиту безпеки коду;

3) розробка технологій функціонування систем в умовах наявності загроз, пов'язаних з використанням недовірених програмних продуктів.

Виконання наведених завдань дозволяє виявити шкідливі програмні продукти з подальшим їх внесенням до санкційного списку, що є важливим превентивним заходом з попередження кібератак в умовах ведення гібридної війни.

В той же час, отримання розробниками експертного висновку про підтвердження відповідності комплексу засобів захисту інформації від несанкціонованого доступу програмного продукту вимогам нормативних документів з технічного захисту інформації, є своєрідною гарантією безпеки використання даної програми та одним з критеріїв її вибору серед суб'єктів господарювання. Так, в 2018 р. технічний захист програми «M.E.Doc» визнано на державному рівні, що підтверджено експертизою Державної служби спеціального зв'язку та захисту інформації України, рівня гарантій Г-3. Це, в свою чергу, був необхідний крок для заспокоєння клієнтів даного програмного забезпечення.

В контексті вибору програмного забезпечення для ведення бухгалтерського обліку та подання звітності зазначимо на наслідках кібератак та складності їх усунення. Так, для підприємств, які обрали для подачі звітності веб-сервіс «СОТА», представлений розробниками програми «M.E.Doc», наслідки кібератаки з використанням вірусу «Petya.A» були набагато складнішими, ніж для тих, хто надав перевагу власне програмі «M.E.Doc». Адже якщо на підприємстві використовувалося офф-лайн програмне забезпечення, то за умови відключення від мережі Інтернет була можливість працювати в програмному забезпеченні на основі створених попередньо архівів. Якщо ж використовувалося он-лайн програмне забезпечення, то можливість подальшої роботи в програмі до тих пір, поки не будуть усунуті наслідки кібератаки, неможливе. За такої ситуації в умовах підвищеного рівня кібератак використання веб-сервісів в Україні не є виправданим. Такі програмні продукти можуть використовуватися лише суб'єктами господарювання, які подають обмежений перелік звітності, втрата доступу до яких не нанесе значних збитків.

Отже, в умовах ведення гібридної війни вважаємо недоцільним використання хмарного програмного забезпечення для ведення обліку та подання звітності для великих та середніх підприємств. Такі програми можуть бути використані тільки малими підприємствами, для яких суттєвим є зниження рівня витрат на технічне та програмне забезпечення.

Крім наведеного критерію щодо вибору програмних продуктів, на рівнів суб'єктів господарювання дослідники визначають ряд заходів щодо захисту облікової інформації. Так, В.А. Шпак виділяє чотири групи таких заходів: правові, технічні, програмні та організаційні [7, с. 182–184]. Науковець конкретизує наведені заходи, проте в частині кібербезпеки розкриває їх тільки для технічних та програмних; всі інші групи заходів захисту відносяться до будь-якого виду інформації (не тільки облікової), яка може формуватися не тільки в умовах використання інформаційно-комп'ютерних технологій.

Рожелюк В.М, навпаки, розкриваючи заходи мінімізації загроз бухгалтерській інформації, наводить їх виключно щодо дій, які повинен забезпечити обліковий персонал. Зокрема, науковець наголошує на необхідності архівації даних, підтримці рівня професіоналізму бухгалтера, організації системи комунікації, забезпеченні умов праці бухгалтера та приділення уваги фінансуванню заходів інформаційної безпеки [5, с. 137]. Погоджуємося з тим, що дотримання розроблених В.М. Рожелюк заходів є важливим для захисту облікових даних, проте в сучасних умовах необхідно також враховувати і рівень розвитку інформаційно-комп'ютерних технологій та загрози, які він в собі несе.

В контексті кібербезпеки С.А. Вітер та І.І. Світлишин визначає три групи заходів, серед яких:

1) організаційні (обмеження несанкціонованого доступу до конфіденційної облікової інформації);

2) технічні (попередження навмисного пошкодження облікової інформації за допомогою спеціально спровокованих порушень працездатності технічних засобів або програмного забезпечення);

3) кадрова робота (підвищення компетентності працівників та їх відповідальності у застосуванні новітніх інформаційних технологій) [1, с. 500].

Проте виділена авторами остання група заходів по суті належить до організаційних, як це і розкривають більшість науковців. Так, Г.І. Ляхович [3, с. 410–411] класифікує заходи захисту облікової інформації залежно від користувачів даних в умовах аутсорсингу та виділяє саме організаційні (нормативні, кадрові, структурні) та технічні (фізичні, програмні). Про це також наголошують зарубіжні дослідники [8, p. 1177], вказуючи на такій основній тенденції в сфері безпеці, як об'єднання фізичної та логічної безпеки суб'єкта господарювання. Причому фізична безпека включає будь-які заходи, які використовує підприємство чи установа для захисту своїх об'єктів, ресурсів або власних даних, які зберігаються на фізичних носіях. А логічна безпека використовує технологію, яка обмежує доступ до систем та інформації суб'єкта господарювання лише для уповноважених осіб.

Останній підхід, на нашу точку зору, є найбільш виправданим в застосуванні на практиці, дозволяючи тим самим виділити найбільш важливі моменти, що потребують посиленої уваги в умовах використання інформаційно-комп'ютерних технологій. Саме тому вважаємо, що захист облікової інформації, значна частка якої на сьогоднішній день зберігається в електронному вигляді, повинен відбуватися з використанням таких заходів:

1) логічної безпеки:
– ідентифікація ризиків. Захист облікової інформації повинен починатися з визначення слабких сторін діяльності підприємства, які проявляються при кібератаках;
– розгляд забезпечення інформаційної безпеки підприємства як частини корпоративної культури. Працівники підприємства повинні бути проінформовані про потенційні загрози витоку інформації через доступ до їх особистих сторінок в соціальних мережах, поштових скриньок тощо. Слід ознайомити працівників з інтернет-ресурсами, які можна використовувати на робочому місці, типами електронних листів та вкладень до них, які можна відкривати. Здійснити це доцільно у вигляді спеціально підготовленого за залученням ІТ-спеціаліста розпорядчого документу;
2) фізичної безпеки:
– шифрування даних. Найбільш важлива інформація, зокрема і облікового характеру, повинна зберігатися в зашифрованому вигляді, представлення в якому можливе завдяки інструментарію більшості операційних систем;
– фізичний захист технічного забезпечення. Загрозою для витоку чи пошкодження облікової інформації може стати не тільки програмне забезпечення, а й викрадення носіїв, на яких зберігається інформація (флеш-накопичувачі, ноутбуки тощо). На підприємстві повинні повною мірою використовуватися фізичні засоби щодо перешкоджання доступу сторонніх.

Керівництво рідко приділяє значну увагу захисту облікової інформації від кібератак. Проте останні події, які відбулися в Україні в умовах ведення гібридної війни, засвідчили високий рівень інформаційних загроз, знизити який на рівні підприємства можливо завдяки впровадження наведених заходів.

Висновки та перспективи подальших досліджень. На основі дослідження праць науковців та враховуючи ситуацію, в якій сьогодні ведуть свою діяльність суб'єкти господарювання, оцінено загрози кібератак в контексті наслідків для ведення бухгалтерського обліку та подання звітності. Запропоновано заходи для їх мінімізації в частині логічної (ідентифікація ризиків, розгляд забезпечення інформаційної безпеки підприємства як частини корпоративної культури) та фізичної (шифрування даних, фізичний захист технічного забезпечення) безпеки. Врахування даних заходів дозволить значно мінімізувати наслідки кібератак.

Список використаної літератури:

1. *Вітер С.А.* Захист облікової інформації та кібербезпека підприємства / *С.А. Вітер, І.І. Світлишин* // Економіка і суспільство: електронне фахове видання. – 2017. – № 11. – С. 497–502 [Електронный ресурс]. – Режим доступа : http://www.economyandsociety.in.ua/journal/11_ukr/80.pdf.
2. Кібератака, вірус Petya.A і до чого тут M.E.Doc: усе, що нам відомо на ранок 29 червня (оновлено). – офіційний сайт «Дебет-Кредит» // Електронний журнал «Дебет-Кредит» [Електронный ресурс]. – Режим доступа : https://news.dtkt.ua/state/other/44158.
3. *Ляхович Г.І.* Захист облікової інформації в умовах аутсорсингу із використанням інформаційно-комп'ютерних технологій / *Г.І. Ляхович* // Бізнес Інформ. – 2017. – № 12. – С. 408–412.
4. *Марков А.С.* Опыт выявления уязвимостей в зарубежных программных продуктах / *А.С. Марков, В.Л. Цирлов* // Вопросы кибербезопасности. – 2013. – № 1 [Електронный ресурс]. – Режим доступа : https://cyberleninka.ru/article/n/opyt-vyyavleniya-uyazvimostey-v-zarubezhnyh-programmnyh-produktah.
5. *Рожелюк В.М.* Заходи забезпечення захисту облікової інформації / *В.М. Рожелюк* // Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації : зб. наук. праць Національної акад. статистики, обліку та аудиту. – 2013. – № 2 (12). – С. 335–340.
6. *Шеломенцев В.П.* Поняття та сутність кібернетичної атаки / *В.П. Шеломенцев* // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2011. – Вип. 25–26. – С. 337–344 [Електронный ресурс]. – Режим доступа : http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=boz_2011_25-26_39.
7. *Шпак В.А.* Організація захисту облікової інформації / *В.А. Шпак* // Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації. – 2015. – № 2. – С. 181–187.
8. *Bawaneh Shamsi S.* Information Security for Organizations and Accounting Information Systems. A Jordan Banking Sector Case / *S.Bawaneh Shamsi* // International Review of Management and Business Research. – 2014. – Vol. 3. – Iss. 2. – P. 1174–1188.
9. *Kudors A.* Hybrid War – A New Security Challenge for Europe / *A.Kudors* [Електронный ресурс]. – Режим доступа : http://www.parleu2015.lv/files/cfsp-csdp/wg3-hybrid-war-background-notes-en.pdf.
10. *von Solms R.* From information security to cyber security / *von R.Solms, van J.Niekerk* // Computers & Security. – 2013. – Vol. 38. – P. 97-102

References:

1. Viter, S.A. and Svitlyshyn, I.I. (2017), «Zahyst oblikovoi' informacii' ta kiberbezpeka pidpryjemstva», *Ekonomika i suspil'stvo: elektronne fahove vydannja*, Vol. 11, Pp. 497–502, available at: http://www.economyandsociety.in.ua/journal/11_ukr/80.pdf
2. «Kiberataka, virus Petya.A i do chogo tut M.E.Doc: use, shho nam vidomo na ranok 29 chervnja (onovleno)», oficijnyj sajt «Debet-Kredy, *Elektronnyj zhurnal «Debet-Kredyt»*, available at: https://news.dtkt.ua/state/other/44158
3. Ljahovych, G.I. (2017), «Zahyst oblikovoi' informacii' v umovah autsorsyngu iz vykorystannjam informacijno-komp'juternyh tehnologij», *Biznes Inform*, Vol. 12, Pp. 408–412.
4. Markov, A.S. and Tsirlov, V.L. (2013), «Opyt vyyavleniya uyazvimostey v zarubezhnykh programmnykh produktakh», *Voprosy kiberbezopasnosti*, Vol. 1, available at: https://cyberleninka.ru/article/n/opyt-vyyavleniya-uyazvimostey-v-zarubezhnyh-programmnyh-produktah
5. Rozheljuk, V.M. (2013), «Zahody zabezpechennja zahystu oblikovoi' informacii'», *Buhgalters'kyj oblik, analiz ta audyt: problemy teorii', metodologii', organizacii', zb. nauk. prac' Nacional'noi' akad. statystyky, obliku ta audytu*, Vol. 2 (12), Pp. 335–340.
6. Shelomencev, V.P. (2011), «Ponjattja ta sutnist' kibernetychnoi' ataky», *Borot'ba z organizovanoju zlochynnistju i korupcijeju (teorija i praktyka)*, Vol. 25–26, Pp. 337–344, available at: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=boz_2011_25-26_39
7. Shpak, V.A. (2015), «Organizacija zahystu oblikovoi' informacii'», *Buhgalters'kyj oblik, analiz ta audyt: problemy teorii', metodologii', organizacii'*, Vol. 2, Pp. 181–187.
8. Bawaneh Shamsi, S. (2014), «Information Security for Organizations and Accounting Information Systems. A Jordan Banking Sector Case», *International Review of Management and Business Research*, Vol. 3 Iss. 2, Pp. 1174–1188.
9. Kudors, A. «Hybrid War – A New Security Challenge for Europe», available at: http://www.parleu2015.lv/files/cfsp-csdp/wg3-hybrid-war-background-notes-en.pdf
10. von Solms, R. and van Niekerk, J. (2013), «From information security to cyber security», *Computers & Security*, Vol. 38, Pp. 97–102, available at: https://doi.org/10.1016/j.cose.2013.04.004.

Грабчук Ірина Леонідівна – кандидат економічних наук, доцент кафедри обліку і аудиту, Житомирський державний технологічний університет.

Наукові інтереси:

- комп'ютеризація бухгалтерського обліку;
- проблеми організації бухгалтерського обліку

Стаття надійшла до редакції 08.10.2018.