7. Закон України «Про внесення змін до Закону України «Про бухгалтерський облік та фінансову звітність в Україні» щодо удосконалення деяких положень» від 05.10.2017 № 2164-VIII [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2164-19

8. Бетге Йорг. Балансоведение: Пер. с нем./Научный редактор В. Д. Новодворский; вступление А. С. Бакаева; прим. В. А. Верхова. - М.: Изд-во "Бухгалтерский учет", 2000. - 454 с.

УДК 657:004.056

Грабчук І.Л.
к.е.н., доцент
доцент кафедри обліку і аудиту
Житомирський державний технологічний університет
м. Житомир, Україна

ЗАХИСТ ОБЛІКОВОЇ ІНФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Гібридна війна передбачає поруч з використанням військових сил також і кібератак та пропаганди. 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.

Одним із найпоширеніших видів інформаційних загроз є вірусні атаки, що пошкоджують не тільки програмне забезпечення комп'ютерів та інформації, але і призводять до їх поламок та несправностей. Вірусні атаки прирівнюються до кібернетичних атак (кібератака).

Об'єктом кібернетичної атаки (кібератаки) можуть бути як комп'ютерні системи вцілому (їх нормальне функціонування), а також такі компоненти цих систем, як: інформаційні ресурси; дані, що передаються каналами зв'язку; програмні та технічні засоби тощо [2].

Яскравим прикладом кібернетичної атаки в Україні стала нещодавня подія із вірусом «Pety.A». У вівторок 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 були інфіковані 12,5 тисяч комп'ютерів [1].

Ця кібератака спровокувала зупинення роботи систем електронного документообігу та прийняття електронної звітності контролюючими органами. Після проведення низки досліджень та розслідувань, було встановлено, що вірус «Pety.A» був поширений через бухгалтерське програмне забезпечення зі 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 кібернетичним атакам технічно не уявляється можливим, незалежно від складності систем захисту. Проте, своєчасне виявлення та швидке адекватне реагування на кібернетичні атаки 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 [1].

Кібератака вірусом «Pety.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.

Вважаємо, що захист облікової інформації, значна частка якої на сьогоднішній день зберігається в електронному вигляді, повинен відбуватися з використанням таких заходів:

- ідентифікація ризиків. Захист облікової інформації повинен починатися з визначення слабких сторін діяльності підприємства, які проявляються при кібератаках.

- 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;

- 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.

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 дозволить знизити рівень інформаційних загроз.

Список використаних інформаційних джерел

1. 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 ресурс]: [Веб-сайт] // Електронний журнал «Дебет-Кредит». – Режим доступу: https://news.dtkt.ua/state/other/44158 (дата звернення 10.03.2018)

2. Шеломенцев В.П. Поняття та сутність кібернетичної атаки [Електронний ресурс] / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2011. – Вип. 25-26. – С. 337-344. – Режим доступу: 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

УДК 657.471

Демська Ю.В.
спеціаліст
Національний університет «Львівська політехніка»
м. Львів, Україна

ВИЗНАННЯ ТА ОЦІНЮВАННЯ РЕЗЕРВУ СУМНІВНИХ БОРГІВ

Важливу роль в управлінні фінансово-господарською діяльністю підприємства відіграє його інформаційне забезпечення, основою якого є система бухгалтерського обліку та фінансової звітності. Одним з важливих методів бухгалтерського обліку є оцінювання, який дає змогу узагальнити інформацію про вартісний вимір фінансового стану і результатів діяльності підприємства.

Питання оцінки резерву сумнівних боргів досліджували такі вітчизняні вчені як: Верига Ю.А., Орищенко М.М. [1], Загородній А.Г. [2]., Козлова М.О. [3] та інші. Окремі аспекти оцінки об’єктів бухгалтерського обліку, зокрема резервів, знайшли своє відображення в роботах українських вчених зокрема: Ловінської Л.Г. [4]., Пилипенка Л.М. [5], Яремка І.Й. [6] та інших. Однак питання визнання та оцінки резерву сумнівних боргів, як об’єкта бухгалтерського обліку, має проблемні аспекти, що стосуються обґрунтованого віднесення дебіторської заборгованості до сумнівної та вибору методу