УДК 657.1.011.56:338.583(477)

Попівняк Ю.М.
кандидат економічних наук,
доцент кафедри обліку і аудиту
Львівського національного університету імені Івана Франка

КІБЕРАТАКА: НАСЛІДКИ ТА ПІДХОДИ ДО МІНІМІЗАЦІЇ ВИТРАТ В УМОВАХ АВТОМАТИЗОВАНОГО ВЕДЕННЯ БУХГАЛТЕРСЬКОГО ОБЛІКУ НА ВІТЧИЗНЯНИХ ПІДПРИЄМСТВАХ

У статті розглянуто суть кібератаки та витрати підприємств, які виникають внаслідок несанкціонованого втручання в роботу їх комп'ютерних мереж. Досліджено організаційно-методичні аспекти автоматизованого ведення бухгалтерського обліку, що впливають на інформаційну безпеку підприємства, особливості відновлення облікових даних після кібератаки. Запропоновано ряд заходів для мінімізації витрат, понесених підприємством за результатами такої атаки.

Ключові слова: автоматизація обліку, витрати, вірус, кібератака, платник податку, програмне забезпечення, форс-мажорна обставина.

Попивняк Ю.М. КИБЕРАТАКА: ПОСЛЕДСТВИЯ И ПОДХОДЫ К МИНИМИЗАЦИИ РАСХОДОВ В УСЛОВИЯХ АВТОМАТИЗИРОВАННОГО ВЕДЕНИЯ БУХГАЛТЕРСКОГО УЧЕТА НА ОТЕЧЕСТВЕННЫХ ПРЕДПРИЯТИЯХ

В статье рассмотрено сущность кибератаки и расходы предприятий, которые возникают в результате несанкционированного вмешательства в работу их компьютерных сетей. Исследовано организационно-методические аспекты автоматизированного ведения бухгалтерского учета, которые влияют на информационную безопасность предприятия, особенности возобновления учетных данных после кибератаки. Предложен ряд мер для минимизации расходов, понесенных предприятием за результатами такой атаки.

Ключевые слова: автоматизация учета, затраты, вирус, кибератака, плательщик налога, программное обеспечение, форс-мажорное обстоятельство.

Popivniak Y.M. CYBERATTACK: CONSEQUENCES AND APPROACHES TO EXPENSES MINIMIZATION IN CONDITIONS OF AUTOMATED ACCOUNTING AT DOMESTIC ENTERPRISES

The article makes a point of cyberattack essence as well as of expenses of enterprises, which appear as a consequence of tampering in work of their computer networks. The organizational and methodical aspects of automated accounting, which influence the information security of an enterprise, the features of accounting data renewal after cyberattack are discussed. A number of measures to minimize expenses incurred by an enterprise as a result of such an attack are proposed.

Keywords: accounting automatization, expenses, virus, cyberattack, taxpayer, software, force majeure event.

Постановка проблеми. Інформаційні технології відіграють ключову роль у підвищенні конкурентоспроможності підприємства, яке функціонує в умовах мінливого ринкового середовища, сприяють його розвитку і зростанню прибутковості. Широке запровадження цих технологій у практику ведення бухгалтерського обліку виправдане реалізацією у його системі процедур збирання, обробки, зберігання та передавання інформації про господарську діяльність підприємства, що потребує автоматизації цих процедур для підвищення ефективності їх здійснення. Використання автоматизованої форми обліку є вимогою часу, а застосування сучасного програмного забезпечення для його ведення – необхідною умовою економії ресурсів підприємства.

Проте автоматизована система ведення обліку завжди знаходиться під загрозою вірусів та цілеспрямованих хакерських атак. Сьогоднішня практика господарювання показала, наскільки неготовими протидіяти несанкціонованим втручанням у комп'ютерну мережу є вітчизняні підприємства і наскільки згубний вплив це може мати на облікові аспекти ведення ними господарської діяльності за умови їх автоматизації. Тому дедалі актуальнішою стає проблема зниження чутливості вітчизняних облікових систем до негативних впливів кібератак, мінімізації ризиків і витрат, пов'язаних із ними.

Аналіз останніх досліджень і публікацій. Проблеми автоматизованого ведення бухгалтерського обліку на вітчизняних підприємствах розглядали багато науковців, серед яких Ф.Ф. Бутинець, С.В. Івахненков, Я.О. Ізмайлов, Т.В. Давидюк, І.А. Касатонова, Ю.А. Кузьмінський, В.М. Костюченко, В.Д. Фролов та ін. Знаходимо в літературних джерелах також праці, які стосуються дослідження кібератак (В.М. Богуш, М.В. Захарова, А.О. Корченко, Д.О. Маріц, В.П. Шеломенцев й ін.). Проте, ці напрацювання носять, в основному, технічний характер, чи розглядають суть і наслідки кібератак з юридичної точки зору. Недостатньо висвітленими у науковій літературі залишаються питання, пов'язані з дослідженням кібератак в контексті їх впливу на функціонування системи обліку українського підприємства, пошуку механізмів зниження його витрат та шляхів уникнення цих атак.

Формулювання мети статті. Метою статті є дослідження впливу кібератак на облікову систему вітчизняних підприємств у сучасних умовах автоматизованого ведення бухгалтерського обліку для формулювання шляхів зниження негативних наслідків, зокрема, мінімізації пов'язаних з ними витрат.

Виклад основного матеріалу. Розпочнемо зі з'ясування сутності поняття «кібератака». Незважаючи на поширеність кібератак у сучасному суспільстві, в Україні відсутнє належне законодавче забезпечення, яке би регламентувало відносини у даній сфері. Згадати можна хіба Кримінальний кодекс України – розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [1].

В аналітичній записці Національного інституту стратегічних досліджень при Президентові України під кібератакою запропоновано розуміти «цілеспрямовані дії, які реалізуються в кіберпросторі (або за допомогою його технічних можливостей), що призводять (можуть

призвести) до досягнення несанкціонованих цілей» [2]. Також у документі подано підходи до розуміння цього терміну Службою зовнішньої розвідки України, Службою безпеки України та Головним управлінням розвідки Міністерства оборони України, які, за своєю суттю, аналогічні наведеному визначенню.

Попри нагальну потребу у прийнятті спеціального закону, наразі проект Закону України «Про основні засади забезпечення кібербезпеки України», який було зареєстровано ще у червні 2015 р., лише відправлено на повторне друге читання. Так, погоджуємося з викладеним у ст. 1 цього законопроекту визначенням кібератаки: «спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій», що спрямовані на «порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем» [3].

Якщо розглядати кібератаку у контексті її впливу на систему ведення бухгалтерського обліку, то витрати підприємства, яке піддалося такій атаці, є значними та різноплановими. До основних їх груп відносимо ті, що пов'язані з:

1) неможливістю здійснювати інформаційний та документальний обміни (зокрема, в системі електронного адміністрування ПДВ, подання звітності);

2) втратою даних бухгалтерського обліку та їх подальшим відновленням;

3) оновленням чи заміною програмного забезпечення (для ведення обліку та подання звітності; захисту від вірусів тощо).

Наглядовим прикладом низького рівня готовності до несанкціонованих втручань у роботу комп'ютерних мереж та вразливості інформаційно-телекомунікаційних систем як на загальнодержавному, так і на рівні окремих підприємств є масштабна кібератака за допомогою вірусу-шифрувальника Diskcoder.C (ExPetr, PetrWrap, Petya, NotPetya) наприкінці червня 2017 р. Важливо, що основним джерелом поширення вірусу стала бухгалтерська програма M.E.Doc (точніше її оновлення від 14 квітня, 15 травня та 22 червня) [4], служба підтримки якої рекомендувала користувачам вимикати антивірус при завантаженні оновлень, додавати оновлення у його «білий список» та встановлювати їх під обліковим записом адміністратора домену. При цьому представники компанії-розробника програми «M.E.Doc» були проінформовані про наявність вразливих місць у їх системах, але не відреагували на це належним чином [5]. Наголосимо, що сьогодні програмою «M.E.Doc» користується близько 500 тис. підприємств (встановленою вона є на близько 1 млн. комп'ютерах) [6]. Таким чином, всі вони опинилися під загрозою втрати облікових даних, неможливості вчасного подання податкової звітності та пов'язаних з цими проблемами витрат. Потерпіли також платники податків, які отримують електронні ключі від Акредитованого центру сертифікації ключів (АЦСК) «Україна», що виявилися скомпрометованими.

За даними опитування, проведеного Торгово-промисловою палатою України, близько 50% підприємств-респондентів не змогли своєчасно виконати зобов'язання перед контрагентами, органами Державної фіскальної служби України (ДФСУ), іншими державними органами [7]. При цьому, до проведення кібератаки Податковий кодекс України не передбачав звільнення платника податку від відповідальності за несвоєчасне виконання цих зобов'язань [8]. Лише після виникнення такої надзвичайної ситуації постала необхідність термінового внесення змін до існуючої законодавчої бази, внаслідок чого було ухвалено Закон України «Про внесення змін до підрозділу 10 розділу XX «Перехідні положення» Податкового кодексу України щодо незастосування штрафних санкцій за несвоєчасну реєстрацію податкових та акцизних накладних внаслідок несанкціонованого втручання в роботу комп'ютерних мереж платників податків» [9]. Проте, ці зміни носять тимчасовий характер і стосуються конкретного випадку (кібератаки за допомогою вірусу Diskcoder.C). Під питанням й надалі залишається багато методичних аспектів ведення обліку, складання і подання звітності за умови здійснення кібератак у майбутньому.

Наразі зміни до законодавства дозволяють підприємствам уникнути деяких витрат, пов'язаних з несвоєчасною реєстрацією податкових і акцизних накладних, а також розрахунків коригування до податкових накладних шляхом перенесення граничних строків їх реєстрації на пізніший термін (таке право стосується усіх платників податків, не залежно від того, чи постраждали вони від кібератаки, чи ні) [9]. Не втрачають підприємства і права на податковий кредит з ПДВ – його вони можуть включити до декларації за звітний період через уточнюючий розрахунок.

Надано можливість уникнути штрафу за несвоєчасне погашення податкових зобов'язань (граничний термін оплати перенесено на 30 календарних днів) [8]. Причому немає вимоги документального підтвердження наслідків кібератаки, а якщо до підприємства вже було застосовано штрафні санкції (до внесення відповідних змін в законодавство), то повідомлення-рішення про нарахування таких штрафних санкцій скасовується [10].

Законодавством встановлено й граничні терміни для відновлення облікової бази даних у випадку їх втрати чи пошкодження внаслідок кібератаки до закінчення 2017 р. Причому підприємство повинне письмово повідомити відповідний контролюючий орган про таку втрату (пошкодження), що можна зробити лише за наявності документів, які підтверджують форс-мажорну подію (обставину непереборної сили) [9; 10].

Визначеного переліку документів, які підтверджують кібератаку, і джерел їх отримання законодавчо не встановлено. Загалом треба отримати висновок Торгово-промислової палати України, до функцій якої входить засвідчення форс-мажорних обставин і видача сертифікату про них (лише для малих підприємств видається безкоштовно, величина витрат на розгляд документів і засвідчення форс-мажору для всіх інших підприємств – 422-7127 грн. залежно від виду послуги та зобов'язань суб'єкта господарювання) [10]. Незважаючи на те, що у переліку обставин непереборної сили кібератака не зазначається, ця організація надала роз'яснення, відповідно до яких таку атаку визнали форс-мажорною обставиною із подальшим документальним засвідченням згідно заяви підприємства та наявності у нього документів, наданих Департаментом Кіберполіції Національної поліції України (довідка чи витяг з Єдиного реєстру досудових розслідувань про відкриття кримінального провадження) [11].

До заяви слід додати й інші документи, які свідчать про надзвичайність, непередбачуваність та невідворотність обставин, вказують на причинно-

наслідковий зв'язок між кібератакою і неможливістю підприємства виконати свої зобов'язання, причому форс-мажорна обставина за кожним таким зобов'язанням засвідчується окремо [12].

Згідно роз'яснень, запропонованих ДФСУ, підтвердними документами пережитої кібератаки мають стати копія заяви у правоохоронні органи, повідомлення про кримінальне правопорушення (разом з документом, який підтверджує її прийняття і реєстрацію) [13] чи інша документація (наприклад, висновок експертизи комп'ютерної техніки і програмних продуктів).

Щоб повідомити податкові органи про кібератаку, на ім'я начальника відповідної Державної податкової інспекції треба надіслати листа і долучити до нього копії документів, які засвідчують несанкціоноване втручання в роботу комп'ютерної мережі підприємства.

Для відновлення облікових даних (в цілях податкового обліку достатньо відновити інформацію за останні 3 роки [8]) на підприємстві потрібно створити комісію зі встановлення переліку відсутніх документів і розслідування причин їх втрати чи знищення. Крім того, слід провести інвентаризацію [14, с. 7].

Джерелами відновлення облікової інформації після її втрати чи пошкодження за наслідками кібератаки є: друковані форми первинних документів, облікових регістрів, звітності; дані звіряння розрахунків з контрагентами, органами ДФСУ, іншими державними органами; результати інвентаризації; дані з виписок за рахунками, наданих обслуговуючими банками; відновлені дані системи Клієнт-Банк; дані, які передаються податковим органам з реєстраторів розрахункових операцій; установчі документи; договори (угоди) з контрагентами; електронні копії інформаційних баз та окремих документів на автономних носіях чи з використанням «хмарних» технологій.

Чим більше документів збережено у паперовому (електронному) вигляді, тим легше відновити пошкоджену інформацію, не втративши її достовірність. Проте зрозуміло, що присутніми будуть і похибки, суттєвість яких залежить від повноти та якості процесу відновлення даних. Особливу увагу слід звернути на розбіжності у податковому обліку. За умови їх виникнення треба відкоригувати показники минулих періодів з поданням уточнюючих розрахунків.

Поряд з такими аспектами інформаційної безпеки підприємства, як технологія обліку і зберігання інформації, правильна організація процесу електронного адміністрування ПДВ тощо, ключова роль відводиться вибору оптимального програмного забезпечення для ведення обліку і, особливо, складання і подання звітності (табл. 1).

Крім розглянутих в таблиці, для подання електронної звітності можна використовувати й наступні програми (онлайн-сервіси): Електронний кабінет платника податків, ZvitOK, E-DOC, FreeZvit, Смарт Звітність, OPZ «Податкова звітність», RePORT,

Як було описано, остання кібератака підірвала довіру користувачів до програми M.E.Doc, а після підписання Указу Президента України від 15.05.2017 р. №133/2017, відповідно до якого під економічні та обмежувальні санкції потрапили розробники і деякі дистриб'ютори програми 1С, користувачі все частіше почали задумуватися про доцільність використання й такого програмного продукту як 1С-Звіт. З іншої сторони, перехід на використання нової програми завжди супроводжується витратами, тому при виборі оптимального програмного забезпечення потрібно оцінити ключові його характеристики: вартість; види звітності й органи, у які вона може подаватися; зручність підключення і встановлення; наявність технічної підтримки, додаткових сервісів; своєчасність оновлень; зручність у користуванні; місце зберігання бази даних тощо [15]. Зокрема, дедалі популярнішими стають SaaS-рішення (Software as a service) на основі «хмарних» технологій, які є порівняно зручними і дешевими у використанні.

Спираючись на поради Департаменту Кіберполіції та Служби безпеки України, для уникнення негативних впливів і, зокрема, витрат вітчизняних підприємств від кібератаки, пропонуємо:

1) не виконувати рекомендації компаній-розробників бухгалтерського програмного забезпечення та їх партнерів щодо запуску його з підвищеними привілеями (наприклад, від імені адміністратора), внесення оновлень до «білого списку» систем захисту комп'ютера, налаштування останніх ігнорувати підозрілу активність чи код такого забезпечення, не вимикати функції евристичного аналізу антивірусної програми;

2) відключати функцію автоматичного оновлення програмного забезпечення, додатково перевіряти ці оновлення на відповідних ресурсах для аналізу підозрілих файлів;

3) регулярно робити резервні копії усієї цінної інформації на окремому, не підключеному до комп'ютера, носії (портативний жорсткий диск, флеш-пам'ять, додатковий портативний комп'ютер та ін.) та у паперовому вигляді, а також у «хмарному» середовищі;

4) з обережністю відноситися до електронної кореспонденції від контрагентів та невідомих відправників (особливо zip-архівів), налаштувати функцію «антиспаму» електронної пошти, не відкривати файли з розширеннями, характерними для вірусів, без належної перевірки;

5) встановити на всіх комп'ютерах підприємства сучасну операційну систему, антивірусні програми і регулярно їх оновлювати до актуального стану, причому з офіційних джерел;

6) не використовувати на робочих комп'ютерах програми, що не потрібні для роботи;

7) ретельно вибирати програмне забезпечення для ведення обліку, орієнтуючись, серед іншого, на кваліфікацію розробника, наявність регулярних аудиторських перевірок такого забезпечення міжнародними експертами з інформаційної безпеки та ін.;

8) проводити тренінги для бухгалтерів з основ кібербезпеки.

Якщо підприємство, все ж, піддалося кібератаці, то на цьому етапі витрати можна мінімізувати так: не перезавантажуючи інфіковані комп'ютери і не вимикаючи їх, якщо вони увімкнені та не вмикаючи, коли вимкнені; спробувавши витягти жорсткий диск і скопіювати з нього дані, підключивши до незараженого комп'ютера; заблокувавши використання облікових записів адміністраторів; не піддаючись не вимогу оплати коштів в обмін на розблокування бухгалтерської інформації; змінивши паролі та електронні цифрові підписи; вчасно звернувшись з поясненнями до відповідних державних органів для уникнення штрафних санкцій тощо.

Висновки та перспективи подальших досліджень. Побутує думка, що у сучасному світі вберегтися від кібератак вкрай важко. Водночас, кібератака завжди вказує на вразливі місця роботи системи. Завдяки проведеному дослідженню ми переконалися, що слабкими сторонами організації автоматизованого обліку на вітчизняних підприємствах, у

Таблиця 1

Програмне забезпечення для подання електронної звітності підприємством

Назва комп'ютерної програ-ми (розробник)	Характеристика комп'ютерної програми
M.E.Doc (ТОВ «Інтелект Сервіс»)	Загальна інформація. Повноцінна система електронного документообігу з модульною структурою. Дозволяє працювати з документами різних типів: звітами, податковими накладними, договорами, рахунками, актами і т.д. АЦСК. «Україна», «ІДД ДФС», «Masterkey», органів юстиції України, «ПриватБанк», «Укрзалізниця», ПАТ «УкрСиббанк». Вартість за рік. Модуль «Звітність» – 1502 грн. (локальна версія), 1802 грн. (мережева версія) (для платників єдиного податку – 902 грн. та 1202 грн. відповідно; для ФОП – 312 грн. та 512 грн. відповідно); Модуль «Корпорація» – 2002 грн.; Модуль «Зарплата» – 852 грн.; Модуль «Електронний документообіг» – 500 грн.; Модуль «Банківські рахунки» – 1002 грн. Переваги. Повноцінний сервіс документообігу, можливість підписання і відправлення документів контрагентам, створення багатьох профілів підприємств, налаштування під особливості роботи клієнта, вбудована система підказок, підтримка мережевого варіанту роботи, SaaS-сервіс, зручний інтерфейс, функціональність, складання консолідованої звітності. Недоліки. Перевантаженість функціями, робота лише в операційні системі Windows, вразливість до кібератак.
1С-Звіт (ТОВ «Інтелект Сервіс»)	Загальна інформація. Використовується для подачі електронної звітності, реєстрації податкових накладних та обміну ними між контрагентами. АЦСК. «Україна», «ІДД ДФС», «Masterkey», органів юстиції України, «ПриватБанк», «Укрзалізниця», ПАТ «УкрСиббанк». Вартість за рік. ФОП – 576 грн., юридична особа – 1200 грн. Переваги. Оперативні оновлення, розширений комплект звітності та іншої документації, зручна у використанні для тих підприємств, які ведуть облік зі застосуванням програми 1С. Недоліки. Залежить від особливостей функціонування програми 1С, працює лише з операційною системою Windows.
Єдине вікно подання електронної звітності (EDZV) (ДФСУ)	Загальна інформація. Використовується для формування і подання звітності до органів ДФСУ, статистики та Пенсійного фонду, а також накладання електронного цифрового підпису і шифрування документів. АЦСК. «ІДД ДФС», «Masterkey», ПрАТ «Інфраструктура відкритих ключів». Вартість за рік. Безкоштовно. Переваги. Можливість безкоштовного використання, конфіденційність інформації. Недоліки. Погана технічна підтримка, функціонує лише в операційній системі Windows, несвоєчасні оновлення, незручна у використанні.
ЗвітОператор (ТОВ «Оператор електронної реєстрації та звітності»)	Загальна інформація. Онлайн сервіс, який забезпечує подання звітності в режимі «Єдиного вікна» до органів ДФСУ, статистики, Пенсійного фонду. АЦСК. «ІДД ДФС», ПрАТ «Інфраструктура відкритих ключів», «Masterkey». Вартість за рік. Безкоштовно чи до 1950 грн. (залежно від пакету послуг). Переваги. Наявність інформаційної, консультаційної та технічної підтримки, надійний захист даних, зберігання інформації про стадії проходження документів у системі, відображення квитанцій, що підтверджують дату та час подання звітності, можливість подання звітності з будь-якого комп'ютера, обробка та транспортування звітів з різних бухгалтерських програм, своєчасне оновлення форм звітності. Недоліки. Функціональна обмеженість окремих пакетів, відсутність технічної підтримки та можливості зберігання архів на сервері оператора у користувачів безкоштовного пакету.
Арт-Звіт Плюс (ТОВ «Інститут математики та системного аналізу»)	Загальна інформація. Програма для обміну різними типами документів та подання електронної звітності до ДФСУ, Пенсійного фонду та інших державних контролюючих органів. АЦСК. «Masterkey», «ІВК», «ІДД ДФС», «Ключові системи», «Україна», ГП «Енергоринок», «ПриватБанк». Вартість за рік. ФОП – 320 грн., юридичні особи – 820 грн. Переваги. Хороша технічна підтримка, можливість інтеграції з програмою 1С та імпорту даних з неї і з інших програм, роботи з кількома звітами на одному екрані, працювати з декількома підприємствами і створювати кілька їх профілів, оперативне оновлення звітних форм, автоматичне заповнення полів з картки підприємства, вбудована система підказок з довідників. Недоліки. Немає можливості роботи з базами даних на різних комп'ютерах, застарілий інтерфейс, обмежений комплект звітності.
iFin (ТОВ «АйФін»)	Загальна інформація. Веб-сервіс, який забезпечує ведення бухгалтерського обліку (складського, торговельного, трудового тощо), автоматичне формування та подачу звітності в органи ДФСУ, статистики, Пенсійний фонд. АЦСК. «ІДД ДФС», органів юстиції України, «Ключові системи», «Україна», «Укрзалізниця», «Masterkey». Вартість за рік. ФОП – 280 грн., юридична особа – 849 грн. Переваги. Безпечність сервісу та конфіденційність інформації, можливість створення профілів багатьох підприємств, зберігання баз даних у «хмарі», працює з різними операційними системами та обладнанням. Недоліки. Обмежений комплект звітів і довідників, відсутність підказок зі заповнення звітності, слабка технічна підтримка.
Соната (ТОВ «СІГНІС»)	Загальна інформація. Програма для подачі електронної звітності до органів ДФСУ, Пенсійного фонду та органів статистики. Уможливлює створення, підписання та відправлення звітів й податкових накладних, перегляду отриманих квитанцій. АЦСК. «ІДД ДФС», «Ключові системи», «Masterkey», «Україна», ДП «Інформаційний центр» Міністерства юстиції. Вартість за рік. ФОП – 280 грн., юридична особа – 650 грн. Переваги. Можливість роботи з багатьма підприємствами, імпорту профілів і документів з інших програм, нагадування про закінчення термінів подання звітності, швидке її заповнення, автоматичний розрахунок та перевірка даних. Недоліки. Працює лише в операційній системі Windows, бази даних зберігаються лише на комп'ютері, немає можливості онлайн-роботи з програмою з різних комп'ютерів.

Продовження табл. 1

Приват24 для бізнесу (ПАТ КБ ПриватБанк)	Загальна інформація. Веб-сервіс для цілодобового формування і подання звітності до державних органів (ДФСУ, статистики, Пенсійного фонду). АЦСК. «ПриватБанк», «ІДД ДФС», «Україна». Вартість за рік. Безкоштовно. Переваги. Дієва служба підтримки, можливість імпорту даних з інших програм, подання звітності кількох підприємств з одного облікового запису, автоматичне заповнення в документах реквізитів підприємства, звітного періоду і суми доходу, SaaS-сервіс. Недоліки. Сервіс доступний лише корпоративним клієнтам ПриватБанку.
Taxer (ТОВ «Таксер»)	Загальна інформація. Веб-сервіс, що дозволяє відправляти електронні звіти в органи ДФСУ і Пенсійний фонд. АЦСК. «ІДД ДФС», «Masterkey», органів юстиції України, «Україна», «ПриватБанк», «Ключові системи». Вартість за рік. ФОП – 450 грн. Переваги. Наявність автоматичних нагадувань, бухгалтерської та юридичної підтримки, доступ до бази даних з будь-якого комп'ютера, автоматичне створення її копії, високий рівень захисту даних, зручний інтерфейс і висока швидкість роботи. Недоліки. Неможливість подання звітності до органів статистики, обмежений комплект звітів і довідників.
СОТА (ТОВ «Інтелект Сервіс»)	Загальна інформація. Веб-сервіс для подачі електронної звітності та обміну електронними документами між підзвітними організаціями, орієнтований переважно на малі та середні підприємства. АЦСК. «Україна», «ІДД ДФС», «Masterkey», органів юстиції України, «ПриватБанк», «Укрзалізниця», ПАТ «УкрСиббанк». Вартість за рік. ФОП – 312 грн.; юридична особа (неплатник ПДВ – 902 грн., на загальній системі оподаткування – 1502 грн). Переваги. Можливість працювати з будь-якого комп'ютера, відсутність потреби у завантаженні оновлень, здійсненні витрат на техніку і обслуговування програми, хороше співвідношення «ціна/якість», багатофункціональність, логічний і зрозумілий інтерфейс, можливість ведення необмеженої кількості підприємств з одного облікового запису, передачі прав ведення обліку на аутсорсинг. Недоліки. Працює лише в операційній системі Windows, схожість з програмою M.E.Doc аналогічного розробника.

цьому контексті, є як нормативне, так і програмне забезпечення, а також суб'єкти, що його розробляють і надають супровід, користуються ним (бухгалтери, фінансисти тощо). Проблемою є також неготовність учасників процесу до несанкціонованих втручань у їх комп'ютерні мережі, брак знань щодо того, як адекватно реагувати, щоб уберегтися від цього форс-мажору і знизити витрати підприємства у випадку, коли атака відбулася чи є така загроза у майбутньому. Тому в подальшому потрібно зосередити зусилля на детальному дослідженні структури таких витрат з метою мінімізації їх величини, як і ефективності здійснення превентивних витрат, щоб уникнути тих, які спричиняє кібератака.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Кримінальний кодекс України [Електронний ресурс] / Кодекс України від 05.04.2001 р. № 2341 – III [зі змін. та доп.]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2341-14/print1499103916333155.
2. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка [Електронний ресурс] / Національний інститут стратегічних досліджень. – Режим доступу: http://www.niss.gov.ua/articles/454/.
3. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] / Проект Закону України від 19.06.2015 р. № 2126а [зі змін. та доп.]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.
4. Кібератака через ПЗ для звітності [Електронний ресурс] // Дебет-Кредит. – 2017. – № 28. – Режим доступу: https://online.dtkt.ua/Book/%C2%AB%D0%94%D0%9A%C2%BB%20%E2%84%9628-2017.epub/navPoint-9.
5. Правоохоронці припинили другий етап кібератаки Petya. Зловмисники використовували вразливості ПЗ M.E.Doc, – Арсен Аваков [Електронний ресурс] // Дебет-Кредит. – 2017. – Режим доступу: https://news.dtkt.ua/state/other/44230?utm_source=news_10072017&utm_medium=email&utm_campaign=weeklyletter_subscribers.
6. Зануда А. Скільки коштуватиме кібератака бізнесу і що робити? [Електронний ресурс] / А. Зануда // BBC Україна. – 2017. – Режим доступу: http://www.bbc.com/ukrainian/features-40521275.
7. «Як вплинула кібератака на ваш бізнес?» – опитування від ТПП України [Електронний ресурс] / Торгово-промислова палата України. – 2017. – Режим доступу: https://www.ucci.org.ua/press-center/ucci-news/iak-vplinula-kiberataka-na-vash-biznes-opituvannia-vid-tpp-ukrayini.
8. Податковий кодекс України [Електронний ресурс] / Кодекс України від 02.12.2010 р. № 2755-VI [зі змін. та доп.]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2755-17/print1499709491287881.
9. Про внесення змін до підрозділу 10 розділу XX «Перехідні положення» Податкового кодексу України щодо незастосування штрафних санкцій за несвоєчасну реєстрацію податкових та акцизних накладних внаслідок несанкціонованого втручання в роботу комп'ютерних мереж платників податків [Електронний ресурс] / Закон України від 13.07.2017 р. № 2143-VIII [зі змін. та доп.]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2143-19.
10. Щодо форс-мажорних обставин [Електронний ресурс] / Лист Державної фіскальної служби України від 20.07.2017 р. N 19075/7/99-99-12-02-01-17. – Режим доступу: http://vobu.ua/ukr/documents/item/lyst-dfsu-vid-20072017-r-19075-7-99-99-12-02-01-17.
11. Михайло Непран: ТПП України рекомендує компаніям, постраждалим від кібератаки, звернутися до кіберполіції [Електронний ресурс] / Торгово-промислова палата України. – 2017. – Режим доступу: https://www.ucci.org.ua/press-center/ucci-news/mikhailo-nepran-tpp-ukrayini-rekomenduie-kompaniiam-postrazhdalim-vid-kiberataki-zvernutisia-do-kiberpolitsiyi-1.
12. Регламент засвідчення Торгово-промисловою палатою України та регіональними торгово-промисловими палатами форс-мажорних обставин (обставин непереборної сили) [Електронний ресурс] / Рішення Президії Торгово-промислової палати України від 18.12.2014 р. № 44(5) [зі змін. та доп.]. – Режим доступу: http://kiev-chamber.org.ua/files/articles/law/Reglament_UCCI_2014_12_18.pdf.
13. ДФС роз'яснено порядок дій платників для незастосування штрафних санкцій через кібератаку [Електронний ресурс] / Прес-служба Державної фіскальної служби України. – Режим доступу: http://sfs.gov.ua/media-tsentr/novini/304708.html.
14. Карпова В. Вірус пошкодив комп'ютер: як відновити облік / В. Карпова // Все про бухгалтерський облік. – 2017. – № 64. – С. 6-9.
15. Савко І. Яку програму вибрати для подачі звітів в електронному вигляді [Електронний ресурс] / І. Савко. – Режим доступу: http://www.buhuslugi.com.ua/ua/publikatsiji/562-yaku-programu-vibrati-dlya-podachi-zviti-v-elektronnomu-viglyadi.html.