УДК 336.2
DOI: https://doi.org/10.32782/2224-6282/159-32

Яструбецька Л. С.
кандидат економічних наук, доцент,
Львівський національний університет імені Івана Франка

Yastrubetska Lesya
Ivan Franko National University of Lviv

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СУБ'ЄКТІВ ФІНАНСОВИХ ВІДНОСИН ЯК ОБ'ЄКТ ЗАХИСТУ

Інформаційна трансформація суспільства, що суттєво пришвидшилася внаслідок пандемії COVID-19, зумовила виникнення нових обставин ведення підприємницької діяльності з більш активним використанням цифрових технологій. Водночас із оптимізацією організації управління фінансами на підприємствах суттєво підвищився рівень загроз їхній інформаційній безпеці. Стрімкого розвитку та поширення набула кіберзлочинність, що реалізовується у формі несанкціонованого втручання в роботу інформаційних систем, протиправного знищення, спотворення чи оприлюднення конфіденційних фінансових даних. Це суттєво знижує рівень фінансової безпеки підприємств. Актуалізація потреби захисту фінансових даних суб'єктів господарювання зумовила необхідність розроблення та викладу у статті пропозицій щодо формування системи захисту конфіденційної фінансової інформації. З цією метою автором визначено джерела конфіденційної фінансової інформації підприємств, цілі та суб'єкти комп'ютерних злочинів, класифіковано інсайдерів відповідно до особливостей їхньої мотивації у вчиненні протиправних дій, а також розроблено організаційну модель побудови та функціонування системи захисту конфіденційної фінансової інформації суб'єкта господарювання.

Ключові слова: *конфіденційна фінансова інформація підприємств, фінансова безпека суб'єктів господарювання, інформаційна безпека ділових одиниць, кіберзлочини, система захисту конфіденційної фінансової інформації підприємств.*

INFORMATION SUPPORT OF FINANCIAL RELATIONS AS A OBJECT OF PROTECTION

The information transformation of society, which has significantly accelerated as a result of the COVID-19 pandemic, has led to the emergence of new circumstances for doing business with a more active use of digital technologies. Simultaneously with the optimization of the organization of financial management in enterprises, the level of threats to their information security has significantly increased. Cybercrime, which is realized in the form of unauthorized interference in the work of information systems, illegal destruction, distortion or disclosure of confidential financial data, has gained rapid development and spread. Disclosure of trade secrets of companies and leakage of important information can cause significant moral and material damage to business units and significantly reduce the level of their financial security. The actualization of the need to protect the financial data of economic entities has necessitated the development and presentation in the article of proposals for the formation of a system for the protection of confidential financial information. To this end, the author identifies sources of confidential financial information of enterprises, targets and subjects of computer crimes. The article proposes the classification of insiders and identifies the features of their motivation in committing illegal acts. When building a system of protection of confidential financial information at the enterprise, the author proposes to take into account a number of principles. These include the principle of financial feasibility, the principle of legal regulation, the principle of internal regulation, the principle of balancing the interests of the enterprise and its economic environment, the principle of integration with international standards for the protection of confidential financial information. The formation of an effective information security policy at both the state and enterprise levels, as well as the development and implementation of appropriate measures can eliminate or significantly reduce financial losses from information threats, which will increase the level of financial security of economic entities.

Keywords: *confidential financial information of enterprises, financial security of business entities, information security of business units, cybercrime, system of protection of confidential financial information of enterprises.*

JEL classification: *F38, G19*

Постановка проблеми. Інформатизація суспільства, поглиблена пандемією COVID-19, зумовила виникнення нових викликів та загроз фінансовій безпеці суб'єктів господарювання. Адже нині успішна підприємницька діяльність практично не є можливою без використання сучасних інформаційних технологій. Це оптимізує вирішення ділових завдань та створює ефективні механізми для економічної співпраці. Водночас зростає рівень загроз інформаційній безпеці суб'єктів господарювання, що може завдати вагомих моральних та матеріальних збитків підприємствам та унеможливити захист їхніх фінансових інтересів. Це актуалізує потребу захисту конфіденційної фінансової інформації суб'єктів господарювання та обґрунтовує необхідність пошуку та розроблення ефективних способів протидії кіберзлочинності в діяльності суб'єктів фінансових відносин.

Аналіз останніх досліджень і публікацій. Над проблемами інформаційної безпеки працювали вітчизняні та зарубіжні дослідники, зокрема В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко, О.Й. Жабинець, М.Ю. Журавель, В.К. Задірака, О.С. Олексюк, Т.В. Полозова, О.В. Стороженко, Л.Дж. Хоффман та інші. Взаємозв'язок фінансової та інформаційної безпеки досліджували у своїх працях О.М. Підхомний, С.В. Кавун, А.А. Пилипенко, Д.О. Ріпка.

Формулювання цілей статті. Водночас чимало аспектів цієї проблематики залишаються ще не досить вивченими та потребують ґрунтовного аналізу. Крім того,

стрімкість зростання загроз інформаційній та фінансовій безпеці в умовах пандемії COVID-19 передбачає пошук та розроблення цілком нових методів захисту конфіденційної фінансової інформації та протидії дезінформації, з якою стикнулися суб'єкти фінансових відносин. Адже розсекречення конфіденційної фінансової інформації чи її спотворення генерує загрозу заволодіння цією інформацією конкурентами, здатними на несумлінну боротьбу на ринку, та рейдерами, що прагнуть заволодіти активами суб'єктів господарювання.

Виклад основного матеріалу дослідження. Щороку кіберзлочинність завдає державі, суб'єктам господарювання та приватним особам значних збитків. Впродовж 2018 року працівники Департаменту кіберполіції були залучені до розслідування більше 11 тисяч кримінальних проваджень та викрили понад 800 осіб, причетних до вчинення злочинів у сфері високих інформаційних технологій [2].

Однією з таких кібератак був запуск у 2017 році різновиду вірусу Petya, який спричинив порушення функціонування багатьох українських суб'єктів господарювання та державних установ. Зокрема, внаслідок кібератаки була заблокована діяльність таких підприємств, як ДП «Міжнародний аеропорт "Бориспіль"», ПАТ «Концерн Галнафтогаз», ПАТ «Укртелеком», ПАТ «Укрпошта», АТ «Державний ощадний банк України», ПАТ «Укрзалізниця».

За результатами дослідження Pricewaterhouse, у якому взяло участь 3877 компаній із 79 країн світу (23% становили фінансові організації), комп'ютерні атаки є одним із п'яти найпоширеніших економічних злочинів в Україні. Понад 25% організацій не мають відповідних механізмів реагування на кіберзлочини; 36% респондентів в Україні розглядають кіберзлочинність як зовнішню загрозу, 24% – як внутрішню загрозу, а 34% вважають, що загроза є як ззовні, так і всередині організації. На думку 67% опитаних, відділ інформаційних технологій (IT) є найбільш ризиковим підрозділом з погляду кіберзлочинності як внутрішньої загрози. Адже співробітники відділу IT мають необхідні навички та можливості для скоєння злочинів із використанням комп'ютерних технологій. Серед інших підрозділів, які наражають організації на ризики кіберзлочинності, респонденти зазначили відділ фінансів (47%), відділ маркетингу та продажів (37%), юридичний відділ (27%), підрозділи вертикалі операційної діяльності (22%), а також представників вищого керівництва (29%). Найменш ризиковими були визнані відділ інформаційної та фізичної безпеки (16% опитаних), а також відділ з управління персоналом (10%) [1].

Виділяють такі категорії джерел конфіденційної інформації суб'єктів господарювання (рис. 1).

Працівники підприємства та суб'єкти його економічного оточення є одним із найважливіших джерел конфіденційної фінансової інформації, оскільки вони можуть одночасно бути джерелом конфіденційної інформації та суб'єктом зловмисних дій. Це керівники всіх рівнів управління, обслуговуючий персонал, партнери, постачальники, покупці тощо.

Документи містять усі дані про склад, стан і діяльність будь-якого суб'єкта господарювання, що привертає до них підвищену увагу зловмисників.

Важливим джерелом конфіденційної інформації про суб'єкт господарювання можуть бути *публікації* в різному вигляді, зокрема статті, матеріали конференцій, брошури, рекламні проспекти, які поширюють на ярмарках і виставках, тощо.

До групи *технічних засобів* забезпечення функціонування підприємства належать телефони і телефонний зв'язок, телевізори і промислові телевізійні установки, радіоприймачі, радіотрансляційні системи, системи гучномовного зв'язку, підсилювальні системи, кіносистеми, системи часофікації, охоронні й пожежні системи та інші, які за параметрами можуть бути джерелами перетворення акустичної інформації в електричні й електромагнітні поля, здатні утворювати електромагнітні канали витоку конфіденційної інформації.

Технічні носії як джерела конфіденційної інформації зумовлені високим темпом зростання парку технічних засобів, що перебувають в експлуатації, їх широким застосуванням у всіляких сферах.

Продукція, особливо нова, яку готують до серійного виробництва, є особливим джерелом інформації. Адже кожний етап життєвого циклу продукції – від задуму та макета до серійного виробництва – супроводжується специфічними даними, що в разі витоку їх із підприємства до конкурентів може завдати значних збитків суб'єкту господарювання.

Документальні, промислові й виробничі відходи можуть містити дані про матеріали, їхній склад, особливості виробництва, технології, фінансові розрахунки тощо.

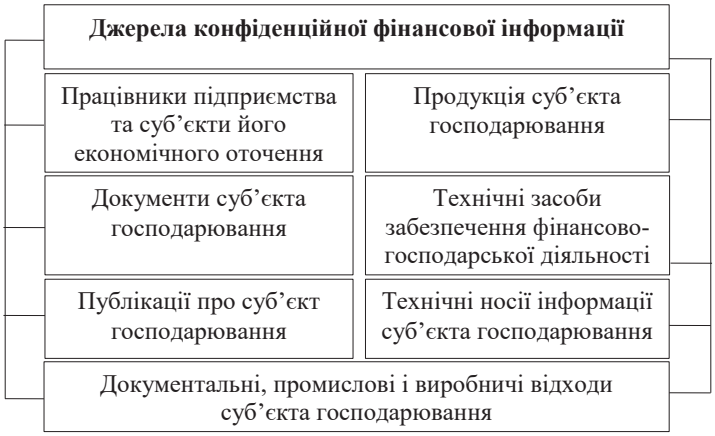

Рис. 1. Джерела конфіденційної фінансової інформації суб'єктів господарювання [4, с. 192]

Злочини в інформаційній сфері пов'язані із порушенням ключових властивостей інформації (див. рис. 2).

Основними причинами, що призводять до порушень, є безвідповідальність, самоствердження і корисливий інтерес користувачів інформаційних систем. Втрати від кожного виду порушень обернено пропорційні до їхньої частоти. Від порушень, зумовлених недбалістю, потрібний мінімальний захист, від зондування системи – жорсткіший, від проникнень – найбільш жорсткий, поєднаний із постійним контролем.

Комп'ютерні злочини характеризуються низкою особливостей (рис. 3):

Для керівників підприємств важливим є усвідомлення, що загроза витоку конфіденційної інформації найчастіше пов'язана з їхнім власним персоналом, тобто з інсайдерами. Згідно з

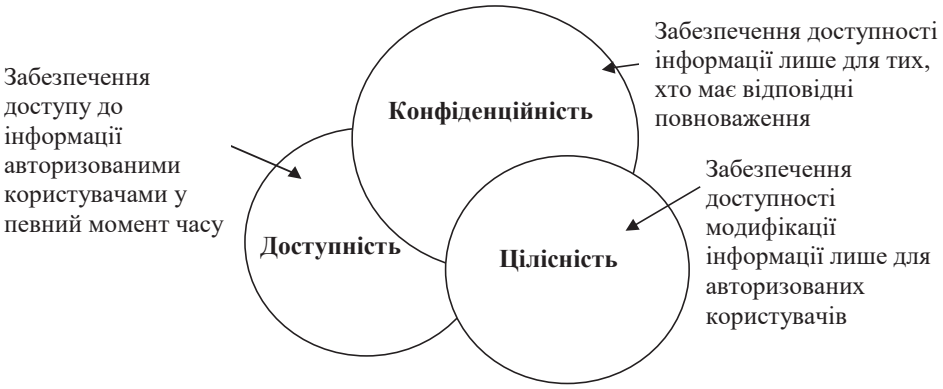

Рис. 2. Властивості інформації [4, с. 203]

класифікацією міжнародної науково-дослідної компанії IDC, система інсайдерів має чотири рівні (рис. 4).

Верхній рівень становлять «громадяни» – лояльні службовці, які зрідка порушують корпоративну політику і загалом не загрожують інформаційній безпеці підприємства. На другому рівні – «порушники», що становлять велику частку усіх працівників суб'єкта господарювання.

Вони здебільшого дозволяють собі в робочий час відволікатися на особисті справи, зокрема працюють із персональною вебпоштою, комунікують у соціальних мережах тощо. Представники цього рівня інсайдерів генерують загрозу інформаційній безпеці підприємства, проте ці інциденти є випадковими і ненавмисними. На наступному рівні – «відступники», що зловживають своїми привілеями з доступу до Інтернету і можуть передавати конфіденційну інформацію суб'єкта господарювання зовнішнім адресатам. «Відступники» становлять вагому загрозу інформаційній безпеці підприємства. На нижньому рівні знаходяться «зрадники» – службовці, які умисно і регулярно чинять зловживання з конфіденційною інформацією з корисливою метою, зазвичай за фінансову винагороду від зацікавленої сторони. Такі співробітники становлять найбільшу загрозу інформаційній безпеці підприємства.

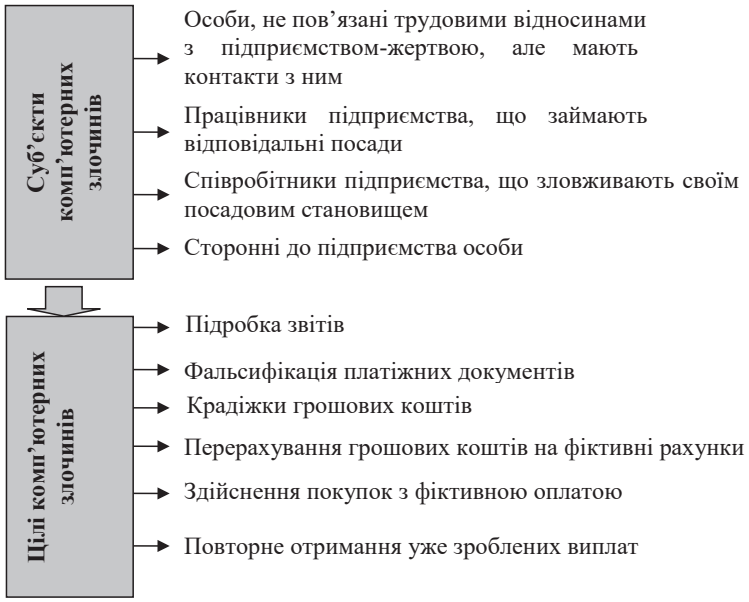

Рис. 3. Особливості комп'ютерних злочинів [4, с. 196]

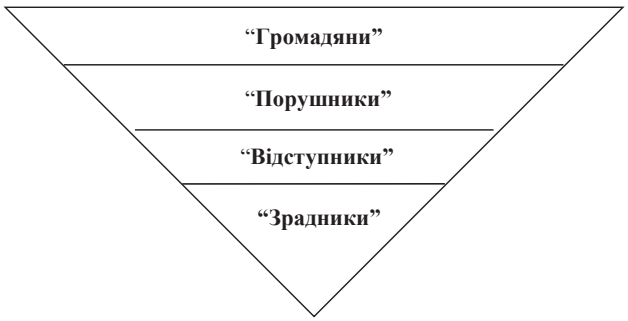

Рис. 4. Класифікація інсайдерів [5, с. 36–40]

Вивчення типів інсайдерів дає змогу розробити методи боротьби з ними, враховуючи їхню індивідуальну специфіку.

Система захисту конфіденційної фінансової інформації – це сукупність спеціальних служб та заходів адміністративно-правового, соціально-психологічного й організаційно-технічного характеру, що забезпечують її збереження, цілісність та належний порядок доступу. Вона покликана забезпечити надійну й ефективну протидію зловмисникам та вирішити сукупність таких завдань, як:

– захист законних прав та інтересів суб'єкта господарювання;

– вивчення партнерів, клієнтів і конкурентів підприємства;

– своєчасне виявлення інтересу до суб'єкта господарювання та його співробітників із боку осіб, які можуть стати джерелом загроз безпеці;

– недопущення проникнення на підприємство представників структур економічного шпигунства, рейдерів, організованої злочинності тощо;

– протидія технічному проникненню на підприємство зі злочинними намірами.

На наш погляд, організаційна модель побудови та функціонування системи захисту конфіденційної фінансової інформації суб'єкта господарювання повинна включати такі етапи (рис. 5):

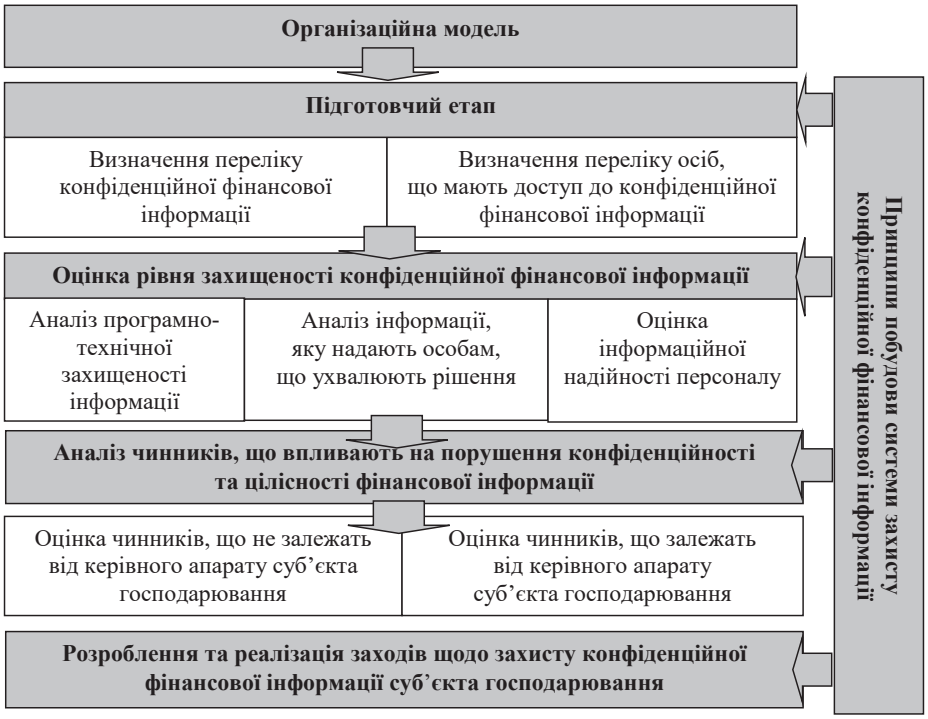

Рис. 5. Організаційна модель побудови та функціонування системи захисту конфіденційної фінансової інформації суб'єкта господарювання [4, с. 204]

На першому етапі необхідно визначити перелік конфіденційної фінансової інформації та осіб, що повинні мати доступ до неї. Наступний етап передбачає оцінку наявного рівня захищеності конфіденційної фінансової інформації, яку виконують із використанням індикаторів інформаційної безпеки. Після оцінювання наявного рівня захищеності конфіденційної фінансової інформації необхідно дослідити чинники, що впливають на порушення її конфіденційності чи цілісності.

З'ясування основних причин порушення конфіденційності фінансової інформації дає змогу створити систему заходів щодо її захисту.

На рівні держави заходи захисту конфіденційної фінансової інформації передбачають розроблення ефективної нормативно-правової бази, що регламентує правила використання інформації, визначає права й обов'язки учасників інформаційних відносин у процесі роботи з конфіденційною фінансовою інформацією, а також відповідальність за порушення цих правил.

На рівні підприємства система заходів щодо захисту конфіденційної фінансової інформації повинна охоплювати адміністративні (визначення переліку конфіденційної фінансової інформації та посадових осіб, що матимуть доступ до неї, і закріплення цього порядку в письмовій формі у відповідних інструкціях підприємства), соціально-психологічні (бесіди з персоналом щодо безпеки фінансової інформації) та організаційно-технічні засоби (застосування захищених технічних засобів і спеціальних програм, призначених для створення перешкод на можливих шляхах проникнення і доступу потенційних порушників до конфіденційної фінансової інформації).

Становлення та функціонування системи захисту конфіденційної фінансової інформації передбачає врахування низки принципів, зокрема: системності (сприйняття системи захисту фінансової інформації нерозривне з іншими системами управління підприємством), фінансової доцільності (оптимальне співвідношення між ефективністю системи захисту інформації та витратами на її становлення і функціонування), законодавчого регулювання (розроблення ефективної законодавчої бази, яка б забезпечувала захист інформації і створення на державному рівні дієвих механізмів та інституцій, які б забезпечували контроль за дотриманням захисту фінансової інформації на підприємствах), внутрішньогосподарського регламентування (затвердження основних правил захисту конфіденційної фінансової інформації на рівні підприємства у відповідних інструкціях), збалансування інтересів підприємства та суб'єктів його економічного оточення (пошук компромісу між конфіденційністю фінансової інформації та необхідним обсягом даних, що підлягають оприлюдненню), інтеграції з міжнародними стандартами захисту конфіденційної фінансової інформації.

Висновки. Формування ефективної політики з інформаційної безпеки як на рівні держави, так і на рівні підприємств, а також розроблення і впровадження відповідних заходів дають змогу ліквідувати чи значно скоротити фінансові втрати від інформаційних загроз, що сприятиме підвищенню рівня фінансової безпеки суб'єктів господарювання.

Список використаних джерел:

1. Всесвітній огляд економічних злочинів PwC : Звіт. URL: https://www.pwc.com/ua/uk/press-room/assets/gecs_ukraine_ua.pdf (дата звернення: 25.10.2018).
2. Підсумки 2018 року в цифрах : Звіт Департаменту кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/results/2018/ (дата звернення: 21.09.2020).
3. Про інформацію : Закон України № 2657-XII від 02.10.1992. Дата оновлення: 16.06.2020. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 12.09.2020).
4. Крупка М.І., Яструбецька Л.С. Фінансова безпека суб'єктів господарювання : підручник. Львів : ЛНУ імені Івана Франка, 2018. 320 с.
5. Шульга І.П. Роль інсайдерської інформації у забезпеченні економічної безпеки акціонерних товариств. *Інвестиції: практика та досвід*. 2010. № 17. С. 36–40.

References:

1. Vsesvitniy ohlyad ekonomichnykh zlochyniv PwC (2018) [World Review of Economic Crimes PwC]. Retrived from: https://www.pwc.com/ua/uk/press-room/assets/gecs_ukraine_ua.pdf (in Ukrainian)
2. Pidsumky 2018 roku v tsyfrakh: Zvit Departamentu kiberpolitsiyi Natsional′noyi politsiyi Ukrayiny (2018) [Results of 2018 in figures: Report of the Cyberpolice Department of the National Police of Ukraine]. Retrived from: https://cyberpolice.gov.ua/results/2018/ (in Ukrainian)
3. Pro informatsiyu: Zakon Ukrayiny № 2657-XII vid 02.10.1992 [On information: Law of Ukraine № 2657-XII of October 2, 1992]. Retrived from: https://zakon.rada.gov.ua/laws/show/2657-12#Text (in Ukrainian)
4. Krupka M.I., Yastrubets′ka L.S. (2018) Finansova bezpeka subyektiv hospodaryuvannya [Financial security of business entities]. Lviv: Lvivskyy natsional′nyy universytet imeni Ivana Franka. (in Ukrainian)
5. Shul′ha I.P. (2010) Rol insayderskoyi informatsiyi u zabezpechenni ekonomichnoyi bezpeky aktsionernykh tovarystv [The role of insider information in ensuring the economic security of joint stock companies]. *Investytsiyi: praktyka ta dosvid*, 17, 36–40. (in Ukrainian)