УДК 346
DOI https://doi.org/10.32840/1813-338X-2019-3-28

Є. І. Лапінська
аспірант
Навчально-наукового інституту права
Національного університету державної фіскальної служби України

ЗАРУБІЖНИЙ ДОСВІД ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРІ ПІДПРИЄМНИЦТВА ТА ЙОГО ВИКОРИСТАННЯ В УКРАЇНІ

У статті розглянуто зарубіжний досвід захисту інформації суб'єктів господарювання під час здійснення ними своєї діяльності. Запропоновано можливі варіанти його ефективного використання в Україні. Незважаючи на розробку та впровадження у вітчизняне законодавство заходів із реалізації забезпечення інформаційної безпеки суб'єктів господарювання, вважати, що усі питання в зазначеній сфері вирішені, не можна. Так, невирішеними сьогодні, на нашу думку, залишаються проблеми суб'єктів господарювання, пов'язані з відсутністю чіткої системи захист інформації та законодавчого впровадження передового зарубіжного досвіду подолання таких проблем, у вітчизняне законодавство.

Таким чином, інформаційна безпека в сучасному світі, в якому основним товаром є інформація, є основою національної безпеки. Для України, яка прагне до Європейського Співтовариства, особливо важливим є приведення чинного законодавства у відповідність до європейських стандартів, що передбачає прийняття нових законів, вдосконалення та доопрацювання чинних законів на основі впровадження передового досвіду зарубіжних країн з урахуванням національних особливостей України.

За умов конкурентного середовища значного поширення набули такі негативні явища, як підслуховування, викрадення конфіденційної інформації на матеріально-речових носіях, зняття інформації з технічних каналів через комп'ютерні мережі. Суперечності перехідного періоду свідчать про комплекс невирішених проблем, що стримують економічний розвиток українських підприємств. Нині перед суб'єктами підприємницької діяльності гостро стоїть питання щодо вирішення спільної проблеми – інформаційної безпеки підприємств незалежно від їх форм власності. Тільки наявність достатніх сил і засобів охорони інформації може гарантувати успіхи в економічній сфері не лише окремо взятого підприємства чи установи, а й у масштабах держави. Сьогодні інформаційна безпека дедалі більше стосується саме суб'єктів підприємницької діяльності, яким потрібно захищатися від відтоку інформації. Інформаційна безпека – це здатність персоналу підприємства забезпечити захист інформаційних ресурсів і потоків від загроз несанкціонованого доступу до них. За результатами негативного впливу на основні властивості інформації (конфіденційність, цілісність, доступність) вирізняють дестабілізуючі фактори техногенного, антропогенного, природного характеру.

Останнім часом розвиток суспільства характеризується негативною динамікою не тільки зловмисних порушень роботи інформаційних систем чи мереж, а й злочинів, вчинених із використанням новітніх технологій, найсучаснішої техніки.

Ключові слова: *захист інформації, зарубіжний досвід інформаційної безпеки в підприємництві.*

Постановка проблеми. Дослідження інформаційної безпеки за сучасних умов є однією з необхідних умов нормального функціонування суб'єктів господарювання. Практика показує, що будь-яка недружня акція, спрямована проти інтересів господарського суб'єкта, починається зі збору інформації, тому питання інформаційної безпеки вже давно входить до головних пріоритетів практично всіх суб'єктів господарювання. Вивчення ж зарубіжного досвіду захисту інформації у підприємництві дозволить розв'язати ці та пов'язані з ними проблеми.

Аналіз останніх досліджень і публікацій. Питання інформаційної безпеки України, її стану і перспектив розвитку, зарубіжного досвіду в цій сфері висвітлювали у своїх наукових працях вітчизняні та зарубіжні автори І. Арістова, В. Бебик, А. Гальчинський, О. Голобуцький,

П. Друкер, Я. Жаліло, О. Зощенко, І. Колідушко, А. Колодюк, Е. Лемберг, Є. Макаренко, Н. Марсук, Г. Почепцов, А. Пшеворський та ін.

Мета дослідження – висвітлення зарубіжного досвіду захисту інформації у сфері підприємництва та його використання в Україні.

Виклад основного матеріалу. Законодавчий рівень інформаційної безпеки найбільше забезпечений у США, де нараховується близько 500 законодавчих актів. Оцінним стандартом захисту інформації є стандарт Міністерства оборони США «Критерії оцінювання довірених комп'ютерних систем».

Ця праця, звана найчастіше за кольором обкладинки «Помаранчевою книгою», була вперше опублікована в серпні 1983 р. У ній ідеться не про безпечні, а про довірені системи, тобто системи, яким можна надати певний ступінь довіри. Детальний аналіз змісту «Помаранчевої книги» підтверджує, що це основний стандарт захисту інформації, який використовується в США усередині підприємництва. Він покладений в основу системи колективної безпеки американського бізнесу, запровадженої з початку 90-х рр. XX ст. Державний департамент і понад 500 корпорацій США регулярно обмінюються інформацією з найгостріших питань загроз підприємницькій діяльності з метою захисту американських громадян.

Понад 70% американських підприємців звертаються по допомогу до відповідних охоронно-детективних агентств.

Успішні суб'єкти бізнесу, співпрацюючи з найнятими охоронно-детективними агентствами, з метою мінімізації господарських ризиків можуть створювати власні служби безпеки. Більше того, у США характерною у створенні таких служб є участь працівників ФБР та ЦРУ, що дає змогу використовувати власну базу даних, досвід відбору працівників до служби безпеки фірми та сформувати при них свої спеціалізовані відділи чи відділення, в яких працюють співробітники спеціальних служб в особі офіцерів безпеки. У такий спосіб держава, не втручаючись у виробничо-господарський процес фірми, намагається не допустити або ж мінімізувати потенційні втрати суб'єкта бізнесу.

Не менш актуальна проблема – розмежування доступу до даних, що знаходяться в пам'яті ЕОМ.

Особливу увагу хотілося б приділити інтелектуальним картам як надійному засобу контролю доступу. Провідна технологія галузі – Expocard, вироблена фірмою CHESEPEAKE (США), є маленьким пластиковим (розміром із кредитну картку) приладом, що містить вбудований комп'ютерний чіп [7]. Інформаційна ємність цієї картки приблизно у 500 разів перевищує відповідний параметр карток із магнітними мітками, а це істотно прискорює пропуск відвідувачів у разі використання їх у системах санкціонованого доступу. Пластикова картка має вбудовану напівпровідникову пам'ять, яка зберігає інформацію про користувача. Для використання таких карток застосовуються зчитувальні / записуючі пристрої, що дозволяють не тільки розшифровувати і прочитувати інформацію, занесену в картку, а й внести у неї в міру необхідності додаткову інформацію. Expocard – однин із багатьох типів карток, розроблених фірмою CHESEPEAKE. Серед можливих її застосувань можна відзначити контроль безпеки мереж комп'ютерів, будівель, охорону парковок, а також облік банківських рахунків, оплату телефонних розмов і т. д.

Дотепер не повідомлялося про жоден випадок підробки інтелектуальних карток. Витрати на експлуатацію, що важливо, теж дуже низькі.

У сфері підготовленості кадрів з питань захисту інформації Сполучені Штати є однією з передових країн. Це питання вирішується на державному рівні, і діяльність служб безпеки контролюються президентом, тому їхній позитивний досвід можна використовувати у нашій країні [1].

Проаналізуємо досвід організації системи захисту інформації у сфері підприємництва в Німеччині. Це одна з найбільш розвинутих країн Західної Європи в галузі інформаційної безпеки. Становлення системи захисту інформації відбулося в цій країні ще в XIX ст. Особливим у формуванні системи захисту інформації стало XX ст. Із середини XX ст. Німеччина багато уваги приділяла захисту такого виду інформації, як персональні дані. У 1970 р. прийнято перший у світі нормативний акт, який регулював питання захисту персональних даних, запропонований федеральною землею Гесен, ініціативу через деякий час підтримали й інші федеральні землі [2].

На підприємстві також здійснюється захист персональних даних. Навіть на маленьких підприємствах, де працює п'ять працівників, вводиться посада уповноваженого із захисту персональних даних.

Багато уваги приділено в Німеччині й технічному захисту інформації. Зокрема, в інтересах

інформаційної безпеки урядом Німеччини в 1993 р. створено федеральне відомство із забезпечення безпеки у сфері інформаційної техніки. До компетенції цього відомства належать, крім технічного захисту інформації, ще й консультації громадян із питань технічного захисту інформації, а також сертифікація та стандартизація засобів безпеки. Крім того, це відомство займається пропагандою необхідності здійснювати захист інформації на підприємствах.

Визначимо досвід Великої Британії у сфері захисту інформації на підприємствах на інших суб'єктах господарювання. Враховуючи схожість соціальної, правової й економічної систем Великої Британії та США, закономірно відзначимо схожість забезпечення безпеки бізнесу в цих країнах.

Приватні агентства виконують той перелік специфічних завдань, що їх ставлять суб'єкти бізнесу, за які не беруться правоохоронні органи держави через їх приватний або ж законом не визначений характер [3]. Більшою мірою це стосується приватних розшукових агентств, котрі обслуговують, окрім суб'єктів підприємництва, ще й осіб щодо їх приватного життя. Цікаво зауважити, що кількість таких агентств постійно зростає, позаяк зростає попит на такі послуги з боку як бізнесменів, так і приватних осіб.

Уряд Великої Британії почав займатися проблемами захисту інформації раніше за інші європейські держави. З одного боку, це дозволило країні накопичити солідний досвід у цій сфері, з іншого – вся система захисту інформації Великої Британії має серйозні недоліки.

Узяти хоч би правове забезпечення захисту інформації у Великій Британії. Основою є закони «Про державні документи» і «Про державну таємницю». Для забезпечення безпеки решти інформації використовуються кримінальний кодекс і деякі інші правові акти. Окремо варто згадати про захист комерційної таємниці. Річ у тому, що про це кожна організація повинна піклуватися самостійно, використовуючи спеціальні договори, які укладаються зі співробітниками перед наданням ним доступу до даних.

Донедавна Франція особливо не вирізнялася з-поміж інших європейських країн щодо формування системи безпеки бізнесу, хоча останніми роками власники промислово-торгівельних і фінансово-кредитних установ почали посилювати формування системи безпеки через створення власних або залучення підприємницьких детективно-охоронних агентств. Користування послугами приватних служб безпеки стало характерним і для інших осіб, зокрема представників страхового ринку, нотаріату, адвокатури, освітніх закладів тощо [4].

Фахівці приватних агентств, співпрацюючи з державними правоохоронцями, спрямовують свої зусилля на боротьбу зі зловживаннями торговою маркою, виявлення фактів недобросовісної конкуренції, на промислове шпигунство та контршпигунство, а також заходи безпеки в банківській системі.

Доцільно звернути увагу на досвід Франції у сфері безпеки персональних комп'ютерів і боротьби з комп'ютерною злочинністю. Тут в інформаційній сфері діють десятки правових актів, які детально регулюють статус суб'єктів інформаційної діяльності, режим інформаційного обміну і підключення до загальних інформаційних систем, автоматизованих банків даних.

Цікавими є системи захисту інформації у сфері підприємництва в провідних країнах Азії – Японії та Китаї.

Промислово розвинутими країнами, зокрема Японією, накопичено значний законодавчий досвід у регламентуванні відносин у сфері захисту комерційної таємниці. Роботодавець може за допомогою договору зобов'язати свого службовця не розкривати інформацію, яка була йому довірена протягом строку служби. Типова угода про службові винаходи, підготовлена патентним відомством, містить такий пункт: «Винахідники та службовці відділу з винаходів службовців повинні зберігати в таємниці суть винаходів та інших матеріалів, що належать до Інтересу компанії, на необхідний термін часу». Крім того, роботодавець може обмежити поведінку службовців після закінчення їхньої служби на визначений період. Належна увага приділяється також захисту ділових секретів у процесі конфіденційних відносин [5].

У сучасному світі Китай є однією з країн Азіатсько-Тихоокеанського регіону, що найбільш активно розвивається і є лідером в питаннях інформаційного протиборства і сучасного захисту інформації у підприємництві. У 2001 р. в Китаї було прийняте положення «Про охорону комп'ютерних програм», це був перший нормативний акт у галузі охорони безпеки комп'ютерних систем Китаю. У 2003 р. був прийнятий Закон «Про авторські права», в якому комп'ютерні програмні продукти вперше були

прирівняні до категорії охоронюваних авторськими правами. Орган громадської безпеки (міліція) несе відповідальність за забезпечення інформаційного захисту [6].

Висновки і пропозиції. Отже, розглянуті найбільш яскраві приклади організації системи захисту інформації у сфері підприємництва в різних країнах світу. Всі вони мають свої переваги і недоліки, й Україні було б добре придивитися до досвіду цих держав.

Дослідження інформаційної безпеки за сучасних умов є однією з необхідних умов нормального функціонування суб'єктів господарювання. Практика показує, що будь-яка недружня акція, спрямована проти інтересів господарського суб'єкта, починається зі збору інформації, тому питання інформаційної безпеки вже давно входить до головних пріоритетів практично всіх суб'єктів господарювання. Вивчення ж зарубіжного досвіду захисту інформації у підприємництві дозволить розв'язати ці та пов'язані з ними проблеми.

Список використаної літератури:

1. Камлик М.І. Економічна безпека підприємницької діяльності.
2. Економіка – правовий аспект : навчальний посібник. Київ : Атіка, 2005. 432 с.
3. Кормич Б.А. Інформаційна безпека: організаційно-правові основи : навчальний посібник. Київ : Кондор, 2008. 384 с.
4. Правове забезпечення безпеки суб'єктів господарської діяльності в Україні : навчально-методичний посібник / Уманський державний педагогічний університет ; уклад. О.В. Митяй. Умань : ПП Жовтий, 2013. 128 с.
5. Низенко Е.І., Калепяк В.П. Забезпечення інформаційної безпеки підприємництва : навчальний посібник. Київ : МАІП, 2006. 134 с.
6. Олійник О.Г. Інформаційна безпека США. Боротьба з організованою злочинністю і корупцією (теорія і практика), 2015.

Lapinska Ye. I. External experience in the protection of information in the field of enterprise and its use in Ukraine

The article deals with the foreign experience of protecting the information of business entities in the course of their activities. Possible variants of its effective use in Ukraine are offered. Despite significant contribution to the development and implementation in domestic legislation of measures to ensure the information security of economic entities, to assume that all issues in this area are resolved, it is impossible. So, in our opinion, today the problems of business entities are connected with the lack of a clear system of information security and the legislative implementation of advanced foreign experience in overcoming such problems in domestic legislation.

Thus, information security in the modern world, in which the main product is information, is the basis of national security. For Ukraine, which aspire to the European Community, it is especially important to bring existing legislation to European standards, which envisages adoption of new laws, improvement and revision of existing laws on the basis of implementation of best practices of foreign countries taking into account national peculiarities of Ukraine.

Under the conditions of the competitive environment, such negative phenomena as eaves dropping, the theft of confidential information on material and material carriers, and the removal of information from technical channels through computer networks became widespread. The contradictions of the transition period indicate the existence of a complex of unresolved issues hampering the economic development of Ukrainian enterprises. Today, before the subjects of entrepreneurial activity, there is an acute problem of solving a common problem – the information security of enterprises regardless of their ownership forms. Only the vailability of sufficient forces and means of protection of information can guarantee success in the economic sphere of not only one individual enterprise or institution, but also the state.

Today, information security is increasingly about the subjects of entrepreneurial activity, who need to be protected from the out flow of information. Information security is the ability of the company's staff to protect information resources and flows from threats of unauthorized access to them. According to the results of the negative influence on the basic properties of information (confidentiality, integrity, accessibility) are distinguished by destabilizing factors of anthropogenic, anthropogenic, natural nature. Recently, the development of society is characterized by a negative dynamics not only malicious violations of the work of information systems or networks, but also crimes committed using the latest technology, the most modern technology.

Key words: *information protection, foreign experience of information security in entrepreneurship.*