СЕКЦІЯ 2. ЕКОНОМІКА ТА УПРАВЛІННЯ НАЦІОНАЛЬНИМ ГОСПОДАРСТВОМ

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПИТАНЬ КІБЕРБЕЗПЕКИ В УКРАЇНІ

ДЕМ'ЯНЧУК М. А.
кандидат економічних наук, доцент,
доцент кафедри фінансів,
банківської справи та страхування
МАСЛІЙ Н. Д.
кандидат економічних наук, доцент,
доцент кафедри фінансів,
банківської справи та страхування
Одеський національний університет
імені І. І. Мечникова
м. Одеса, Україна

Одним із дуже помітних феноменів сучасності, які дедалі частіше привертають до себе увагу дослідників, є глобалізація та інформатизація суспільства. У цих умовах відбувається збільшення міжнародної торгівлі, зростання масштабів і темпів переміщення капіталів, інформаційного обміну тощо. Все це відбувається цілодобово в реальному часі на світових фінансових ринках завдяки сучасним технологіям і мережі інтернет, які дозволили подолати відстань, кордони і час для обміну активами, ідеями і науковими новинками. Основним ресурсом сучасних підприємств є інформація, яка, як і матеріальні ресурси, володіє якістю та кількістю, має собівартість і ціну. Порушення основних властивостей інформації може стати серйозною небезпекою для підприємств в умовах зростаючого числа загроз і вразливостей як з боку зовнішнього, так і з боку внутрішнього середовища підприємства. До числа таких загроз відносяться кіберзлочинність, яка проявляється у вигляді хакерських атак (кібератак), що позначається у втраті корпоративних даних, інтелектуальної власності або даних клієнтів чи втрата всього переліченого. Наслідки даних загроз варіюються від штрафів регулюючих органів та репутаційних втрат до повної втрати бізнесу. Тому питання забезпечення захисту інформаційних ризиків та кібербезпеки підприємств від несанкціонованого доступу до внутрішньої інформації компанії є надзвичайно важливими, основою яких є нормативно-законодавчі акти, що регулюють питання кібербезпеки.

Аналіз загроз і можливості страхового захисту від кіберзлочинів проводиться в зарубіжних країнах протягом останніх 10-15 років. Публікації зарубіжних авторів Ю. В. Бородакія, А. Ю. Добродеева і І. В. Бутусова, С. В. Бреннера і М. Д. Гудмана націлені на аналіз ризиків і страхового захисту від кіберзагроз. Такі вітчизняні автори як В. П. Прохоренко, О. В. Сергієнков, А. Устенко у своїх працях розглядають питання кіберзлочинності, правового та технічного захисту від кіберзагроз. С. Пател у своїх працях виокремлює такі ризики сучасного розвитку підприємств як кіберризик (віртуальний ризик) (cyber risk), ризик збою у бізнесі (risk of business disruption), ризики довкілля на макро рівні (macro environment risks), репутаційний ризик (reputation risk), кадровий ризик (talent risk). Наводить приклади та методи зниження деяких з них, зауважує, що страхові компанії мають активно включитись у страхування таких ризиків. Приймаючи до уваги існуючи дослідження особливої уваги потребує аналіз правового регулювання питань кібербезпеки в Україні, що і є метою роботи.

27 червня 2017 року ввійшов в історію, як день, який показав на скільки вразлива економіка країни до кібератак. За даними кіберполіції від здійсненого нападу постраждали понад 2000 компаній: серед великих компаній приватного сектору від вірусу постраждали ТОВ «Нова пошта», мережа магазинів DIY «Епіцентр», промислово-будівельна група «Ковальська», основні українські мобільні оператори – ПАТ «Київстар», ПрАТ «Vodafone» і ТОВ «Lifecell» та інші.

У липні 2018 року співробітники служби безпеки України (СБУ) відбили хакерську атаку на мережеве обладнання ТОВ «Аульськая хлоропереливна станція», яке є об’єктом критичної інфраструктури країни. Як з’ясували співробітники спецслужби, протягом декількох хвилин системи управління технологічними процесами і системи виявлення ознак аварійних ситуацій підприємства були вражені шкідливим ПЗ VPNFilter [1]. Дана кібератака потенційно могла призвести до зриву технологічних процесів і можливої аварії. Задум хакерів полягав у блокуванні сталого функціонування переливної станції, що забезпечує рідким хлором водопровідно-каналізаційні підприємства по всій території України.

Після масованих хакерських атак на український бізнес і державний сектор протягом останнього року, вітчизняні підприємці почали замислюватися про те, як перестрахувати себе від подібних ризиків. Для вітчизняного страхового ринку таке явище далеко не масове і до світових обсягів (світовий ринок кіберстрахування оцінюється в $ 3-3,5 млрд) ще дуже далеко. Українські страховики засвідчують, що затребуваність в такому продукті на вітчизняному ринку є, відзначаючи при цьому, що в першу чергу він може бути цікавий компаніям, які мають серйозні бази даних.

До сих пір в світі немає закріплених законодавством стандартів з питання страхування кіберризиків, проте серед позитивних показників галузі кібербезпеки України аналітики Міжнародного союзу електрозв'язку [2] відзначили законодавчу базу (табл. 1), професійну освіту, державне регулювання питань кібербезпеки, міжвідомче та міжнародне співробітництво у галузі, рівень державно-приватного партнерства.

Таблиця 1

Основні нормативно-правові акти, що регулюють питання кібербезпеки в Україні

Назва нормативно-правового акту / Дата прийняття	**Питання, що регулюються нормативно-законодавчим актом**
Директива 2002/58/ЄС Європейського Парламенту та Ради «Про секретність та електронні комунікації» / 12.07.2002	Директива гармонізує положення держав-членів, необхідні для забезпечення еквівалентного рівню захисту основних прав та свобод, та зокрема права на таємницю, щодо обробки персональних даних у секторі електронних комунікацій та забезпечення вільного руху таких даних та обладнання для електронних комунікацій та послуг у Спільноті.
Конвенція про кіберзлочинність / 23.11.2001	Конвенція встановлює заходи, які мають здійснюватися на національному рівні та у міжнародному співробітництві щодо правопорушень
Закон України Про основні засади забезпечення кібербезпеки України / 05.10.2017	Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.
Указ Президента України Стратегія кібербезпеки України / 15.03.2016	Метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.
Закон України «Про інформацію» / 02.10.1992	Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.
Закон України Про захист інформації в інформаційно-телекомунікаційних системах / 05.07.1994	Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах
Закон України Про авторське право й суміжні права / 23.12.1993	Закон охороняє особисті немайнові права і майнові права авторів та їх правонаступників, пов'язані із створенням та використанням творів науки, літератури і мистецтва – авторське право, і права виконавців, виробників фонограм і відеограм та організацій мовлення – суміжні права.
Закон України Про поширення екземплярів аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних / 23.03.2000	Закон визначає правові основи розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних і спрямований на захист інтересів суб'єктів авторського права і суміжних прав та захист прав споживачів

Джерело: сформовано авторами на основі даних [3-10]

Для мінімізації або усунення кіберризиків існує три основних напрямки: технологічні рішення безпеки, просвітницька робота в сфері протидії та профілактики кіберзлочинів, а також кіберстрахування.

Поняття кіберстрахування на сьогодні є доволі новим і мало дослідженим. В останні роки цей інструмент набув поширення на міжнародному ринку. І зараз його пропонує понад 60 страхових компаній по всьому світу. На даному етапі український страховий ринок істотно відстає від своїх західних колег у питанні розробки і впровадження продукту кіберстрахування.

В останні роки інструмент кіберстрахування набув широкого поширення на міжнародному ринку. І зараз його пропонує понад 60 страхових компаній по всьому світу, на відміну від українського ринку.

Основним завданням кіберстрахування є захист від великомасштабних хакерських атак. Цей вид страхування забезпечує фінансовий механізм відновлення після великих збитків, допомагаючи підприємствам повернутися до нормального функціонування, збереження стабільності, платоспроможності і зниження втрат в результаті перерви у виробництві.

Свою популярність в розвинених країнах кіберстрахування отримало завдяки розумінню того, що, впроваджуючи новітні рішення в сфері кібербезпеки і проводячи постійну роботу з персоналом, завжди залишається той 1% ризику компрометації системи, який неможливо передбачити і оцінити. Кіберстрахування характеризується широким спектром покриттів і захищає насамперед компанії від фінансових втрат.

Тому в сучасних умовах розвитку необхідним є розроблення заходів спрямованих на захист інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем підприємств різних сфер економічної діяльності і відповідних ресурсів від кібератак та кіберзагроз на основі законодавчого впровадження сутності питань з кібербезпеки. Оскільки кібербезпека є один із важливих факторів розвитку економічного потенціалу країни, основних сфер її економічної діяльності та їх підприємств: якщо держава досягає певного прогресу у сфері забезпечення кібербезпеки, то це є ознакою сприятливого інвестиційного клімату для залучення зовнішніх донорських фінансових активів, що в свою чергу сприяє більш ефективному розвитку як підприємств, так і економіки країни в цілому.

Література:

1. Братюк В. П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. Актуальні проблеми економіки. Київ, 2015. № 9. С. 421-427.
2. Міжнародний союз електрозв'язку. URL: http://www.itu.int (дата звернення: 24.10.2018).
3. Директива про секретність та електронні комунікації: Директива 2002/58/ЄС Європейського Парламенту та Ради від 12.07.2002 L 201/38. URL: https://nkrzi.gov.ua/images/upload/58/19/6f96b 8148ef15842f70cba3dd98f055b.pdf (дата звернення: 24.10.2018).
4. Конвенція про кіберзлочинність від 23.11.2001. Ратифікація від 07.09.2005 № 2824-IV. URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 24.10.2018).
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Дата оновлення: 05.10.2017. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 24.10.2018).
6. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016. Дата оновлення: 15.03.2016. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 24.10.2018).
7. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення: 01.01.2017. URL: http://zakon. rada. gov. ua/laws/show/2657-12 (дата звернення: 24.10.2018).
8. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5.07.1994 р. № 80/94-ВР. Дата оновлення: 19.04.2014. URL: http://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 24.10.2018).
9. Про авторське право й суміжні права: Закон України від 23.12.1993 № 3792-XII. Дата оновлення: 22.07.2018. URL: http://zakon.rada.gov.ua/laws/show/3792-12 (дата звернення: 24.10.2018).
10. Про поширення примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних: Закон України від 23.03.2000 № 1587-III. Дата оновлення: 04.10.2018. URL: http://zakon.rada.gov.ua/laws/show/1587-14 (дата звернення: 24.10.2018).