3. Czerniak, J. Innowacyjność w Polskiej i światowej gospodarce.Lublin: Uniwersytet Marii Curie – Skłodowskiej w Lublinie, 2013.S. 65-68.
4. Przyborowska, B. Fundamenty innowacyjnego społeczeństwa.Toruń: Uniwersytet Mikołaja Kopernika w Toruniu, 2014.S. 92-98.
5. Europejski Ranking Innowacyjności w 2020 roku.URL: https://ec.europa.eu/docsroom/documents/41903
6. Trading Economics. URL:tradingeconomics.com/finland/wag es.

Дишлевий Р. В.,
аспірант,
Національна академія статистики, обліку та аудиту, м. Київ

СУТНІСТЬ ТА ОСНОВНІ ХАРАКТЕРИСТИКИ КІБЕР-РИЗИКІВ

Кібербезпека – комплекс дій стратегічного характеру, направлений на захист від нанесення економічної, технічної або інформаційної шкоди внаслідок загроз, що здійснюються за допомогою програмно-технічних засобів, а також в результаті щоденної роботи з інформаційними мережевими технологіями.

Кібербезпека забезпечує захист від виникнення збитків через дій злочинців, які здійснюються за допомогою телекомунікаційних технологій, тобто бореться з проявом кібер-ризиків.

Основними характеристиками кібер-ризиків [1]:

1) IT-природа. Кібер-ризик характеризується як інформаційно-технологічна категорія, займаючи певне місце в сучасній економіці і продовжуючи все більше проникати в сферу економічної діяльності підприємств, комерційних банків та інших суб'єктів. Еволюція інформаційних технологій є головною передумовою розвитку кібер-ризиків.

2) Об'єктивність прояву. У зв'язку з тим, що в сучасному світі практично будь-яка діяльність на підприємствах і в банках супроводжується застосуванням IT-технологій, то кібер-ризик є об'єктивним явищем, тобто супроводжує всі операції. В незалежності від того, що ряд параметрів кібер-ризику залежить від суб'єктивних управлінських рішень, властивість його об'єктивного прояву залишається незмінною.

3) Імовірність виникнення. Сутність полягає в тому, що в процесі фінансово-господарської діяльності банків кібер-ризик може виникнути, а може і ні. Імовірність того, що станеться кібератака, визначається дією різних об'єктивних і суб'єктивних факторів, проте імовірнісна приналежність кібер-ризику є його стійкою характеристикою.

4) Непередбачуваність виникнення. Кібер-ризик складно прогнозувати і супроводжується труднощами в оцінці через крайню скритність кіберзлочинців. Шахраї володіють цією перевагою, яка досягається застосуванням різних механізмів шифрування і анонімності.

5) Очікувана несприятливість наслідків. Ризик в фінансово-господарській діяльності характеризується і співвідноситься з рівнем можливих негативних наслідків. Однією з основних характеристик кібер-ризику є те, що він завжди порівнюється з будь-якими несприятливими наслідками. Найчастіше кібер-ризики можуть призводити не тільки до втрати прибутку, а й капіталу підприємства (банку), що в свою чергу є причиною банкрутства.

6) Мінливість рівня. Рівень кібер-ризику не завжди однаковий. Він змінюється в часі і залежить від безлічі об'єктивних і суб'єктивних факторів (наприклад, від якості програмного забезпечення; рівня захисту від кіберзагроз банку; кваліфікації персоналу і т. п.).

7) Суб'єктивність оцінки. Незважаючи на те, що кібер-ризик є об'єктивним за своєю суттю, показник його оцінки – рівень ризику – носить суб'єктивний характер. Ця суб'єктивність (неоднозначність оцінки) характеризується різним рівнем якості інформації, її достовірності і повноти; кваліфікацією співробітників відділу ризик-менеджменту, їх компетентності та досвіду, а також іншими факторами.

8) Транскордонність. Однією з найважливіших характеристик кібер-ризику є необмеженість в просторі [2]. Таким чином, кібершахрай і постраждала від нього сторона можуть перебувати на відстані тисяч кілометрів, що не завадить скоєнню злочину.

У зв'язку з тим, що кіберзлочини охоплюють широке коло суспільних відносин, передбачають використання різного обладнання і мають безліч способів скоєння, існує кілька підходів до їх класифікації.

Конвенцією Ради Європи [3] види кіберзлочинів об'єднані в п'ять груп, представлених в таблиці 1.

Таблиця 1

Класифікація кіберзлочинів в відповідності з Конвенцією Ради Європи

Група	Зміст
1	Злочини, спрямовані проти комп'ютерних даних і систем
2	Протиправні дії, пов'язані з використанням технологій
3	Правопорушення, пов'язані зі змістом даних або контентом
4	Порушення авторських і суміжних прав
5	Дії, які посягають на громадську безпеку

Джерело: складено автором на основі [3]

Перша група включає всі комп'ютерні злочини, спрямовані проти комп'ютерних даних і систем (наприклад, незаконний доступ, втручання в дані або системи в цілому).

Другу групу складають протиправні дії, пов'язані з використанням технологій (підроблення, витяг, блокування або зміна даних, отримання економічної вигоди іншими способами).

Правопорушення третьої групи пов’язані з утриманням даних або контентом.

Порушення авторських і суміжних прав відноситься до четвертої групи, виділення певних видів злочинів в якій віднесено до законодавства конкретних держав.

Кібертероризм і використання віртуального простору для здійснення актів насильства, а також інші дії, що посягають на громадську безпеку, включаються в п’яту групу кіберзлочинів.

Згідно зі статистикою, наведеною ООН, щорічний економічний збиток від розкрадання онлайн-даних в банківському секторі становить понад 100 млрд дол. США [4]. До числа викрадених даних відносяться відомості про кредитні картки, паролі, логіни та інші особисті параметри клієнтів кредитних установ.

Таким чином, для кредитних організацій дуже важливо забезпечення кібербезпеки і ефективне управління кібер-ризиками, яке допоможе знизити кількість і ймовірність загроз з боку кібершахраїв і звести до мінімуму величину втрат від даних загроз.

Список використаних джерел:

1. Риски – понятие и виды. Классификация рисков. Основные характеристики рисков. URL: http://www.grandars.ru/student/fin-m/vidy-riskov.html

2. Gable K.A. Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. *Vanderbilt Journal of Transnational Law.* 2010. Vol. 43, № 1. P. 57-118.

3. Convention on Cybercrime – CETS 185. URL: https://rm.coe.int/1680081580

4. Доклад Конгресса ООН по предупреждению преступности и уголовному правосудию. URL: https://www.unodc.org/congress

Дмитрієва Є. В.,
студентка освітнього рівня «бакалавр»,
освітньо-професійна програма «Менеджмент зовнішньоекономічної діяльності»,
Національна академія статистики, обліку та аудиту, м. Київ

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ НЕЙРОМАРКЕТИНГУ НА РИНКУ

Сучасні ринки характеризуються перенасиченням різноманітними товарами і послугами, постійно зростаючою конкуренцією, яка призводить до посиленої боротьба за увагу споживача. Для його завоювання і успішного просування товарів, компанії використовують найрізноманітніші методи, метою яких є досягнення більшого з меншими затратами. Досягнення цієї мети