

УДК 331.108

*Шкуренко М.І.,
«ФЕтаУ», III курс,
Науковий керівник - Красножон С. В.,
к.е.н., доцент кафедри
корпоративних фінансів і контролінгу
ДВНЗ «КНЕУ імені Вадима Гетьмана»*

Кібернетичні атаки та їх роль у бізнесі

Проблема кібернетичних атак у наш час є досить актуальним, особливо якщо ця проблема чіпляє наш бізнес, а в основному його захищеність від втручання із зовнішнього середовища. Паралельно з нею постають важливі питання:

- Що ж собою взагалі уявляють кібер – атаки?
- Які ж методи і наслідки з'явилися, щоб боротись із цим явищем?

Кібернетичну атаку в загальному вигляді можна розглядати як рішучу дію, яка для досягнення певної мети використовує методи технічної кібернетики й спрямована проти об'єкта, здатного сприйняти цілеспрямований вплив кібернетичного характеру. Дане визначення не є єдиним у своїй історії, існують безліч напрямків трактування цього поняття над яким працювали Д. В. Дубов, О. А. Ільяшов, О. О. Климчук, С. В. Мельник, Н. А. Ожеван, О. О. Тихомиров та інші науковці[1, с. 2].

Кібер-ризика є найбільш недооціненими ризиками в довгостроковій перспективі в Україні. Яскравим прикладом цього є те, що у 2017 році під час кібератаки вірусу Petya постраждали понад 1500 компаній, а 13 тисяч комп'ютерів були заражені. За рік український бізнес втратив від кібератак мільярди гривень [2].

Проведення кібер – атак в організаціях малого та середнього бізнесу призводить до настання таких наслідків, як ліквідація бізнесу або його уповільнення, що несуть збитки конкурентоспроможності на ринку і як наслідок – втрата клієнтів та прибутку; зниження вартості бізнесу, яка породжується через втрату репутації та знеславлення бренду; судові розгляди та позови, що

несуть витрати на усунення наслідків, штрафи й санкції органів, що регулюють це питання.

Задля уникнення таких наслідків, необхідно залучити певні заходи стосовно ізоляції свого бізнесу від кібернетичних атак. У всьому світі використовують ряд таких методів:

- побудова урядової моделі, спрямованої на забезпечення кібербезпеки;
- встановлення схеми у вигляді суспільно – державного партнерства, задля обговорення та затвердження політики, що пов'язана з проблемами кібербезпеки;
- планування та встановлення політик та механізмів, що їх регулюють, точне визначення ролей, прав та відповідальності для приватного та державного секторів у сфері розвитку кібербезпеки;
- встановлення цілей та методів розвитку можливостей, які може надати держава та розширення законодавчої бази з метою міжнародної боротьби з кіберзлочинністю;
- визначення ключових інформаційних інфраструктур, у тому числі – основних активів, сервісів та взаємозалежностей;
- підвищення рівня готовності, зменшення часу на реакцію на інциденти, які можуть виникнути, розробка плану відновлення після збоїв та розробка механізмів захисту для ключових інформаційних інфраструктур;
- розробка системного та інтегрованого підходу до державного управління ризиками;
- засвоєння користувачами нової моделі поведінки та роботи, шляхом визначення цілей інформаційних програм та затвердження їх в якості пріоритетних;
- розробка нової програми освіти з акцентом на навчання ІТ – фахівців та професіоналів в рамках кібербезпеки;
- розвиток співпраці з іншими країнами[3].

Отже, кібер – ризики сьогодні виходять далеко за межі крадіжки та шахрайства, що включає втрату конкурентної переваги внаслідок вкраденого інтелектуального майна, втрату клієнта чи бізнесу, довіри партнера та загальний збиток для репутації та бренду організацій малого та середнього бізнесу. Складність кібер – ризиків в Україні та світі, на жаль, надалі буде тільки зростати. Більше підключених пристроїв, більше джерел даних, більше автоматизації процесів, сторонні стосунки створюють нові можливості для кібератак та інцидентів.

Список використаних джерел:

1. Наукова стаття – Шеломенцев В. П. Поняття та сутність кібернетичної атаки / Шеломенцев Володимир Петрович, 2011. – 8 с.
2. Волосович С. Детермінанти виникнення та реалізації кібер-ризиків / С. Волосович, Л. Клапків // Зовнішня торгівля: економіка, фінанси, право. – 2018. № 3. С. 101–115.
3. Йон О. О. СВІТОВІ ТЕНДЕНЦІЇ БОРотьБИ З КІБЕРЗЛОЧИННІСТЮ / О. О. Йон, Н. Ф. Казаков. // ВІСНИК СХІДНОУКРАЇНСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ імені Володимира Даля. – 2013. – С. 59–61.

УДК 336.743

Шуплат О.М.,

к.е.н., доцент кафедри

корпоративних фінансів і контролінгу

ДВНЗ «КНЕУ імені Вадима Гетьмана»

Глобальні інвестиції у фінтех-сектор

Світ технологій, фінансів та інвестицій, коли впроваджуються нові фінансові інструменти та принципово інші бізнес-моделі, що функціонують також на основі фінтех-сервісу, зазнає бурхливого розвитку. Швидке зростання числа стартапів та паралельний розвиток екосистеми будуть сприяти