

**Міністерство освіти і науки України**  
Сумський державний університет  
Навчально-науковий інститут бізнесу, економіки та  
менеджменту  
Кафедра економічної кібернетики

***ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ***  
***ФІНАНСОВИХ ПОСЛУГ***

Матеріали  
наукової онлайн-конференції

**(Суми, 07 вересня 2023)**

Суми  
Сумський державний університет  
2023

004.056.5:336(082)

B43

**Головний редактор**

доц., к.е.н., Prof., Dr. *Койбічук Віталія*, завідувачка кафедри економічної кібернетики, Сумський державний університет

*Затверджено Вченою Радою Сумського державного університету  
(протокол № 2, 14.09.2023)*

Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 07 вересня 2023. Збірник S62 матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2023. – 183 с.

Матеріали наукової онлайн-конференції " Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібезагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

© Сумський державний університет, 2023

## ЗМІСТ

<b>СЕКЦІЯ 1</b>	<b>ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ</b>	<b>6</b>
<i>Кирило Каліновський, Валерій Яценко</i>	ЕЛЕКТРОННІ ФІНАНСОВІ ПОСЛУГИ ЯК ІНСТРУМЕНТ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ	6
<i>Єлизавета Калюсенко</i>	ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ	9
<i>Сергій Миненко, Владислава Лук'янова</i>	АНАЛІЗ РІВНЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ УКРАЇНИ ТА КРАЇН ЄС	12
<i>Анастасія Самойленко, Валерій Яценко</i>	РОЗУМНІ МІСТА ТА ЇХ РОЛЬ У ЦИФРОВІЙ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ	16
<i>Аліна Сімановська</i>	ЦИФРОВІ ТРАНСФОРМАЦІЇ В БАНКІВСЬКІЙ СФЕРІ: ТЕНДЕНЦІЇ ТА МОЖЛИВОСТІ	19
<i>Ігор Бараннік, Олексій Бударін</i>	ЗРОСТАННЯ ЕКОНОМІЧНОЇ СТІЙКОСТІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ В СУЧАСНИХ УМОВАХ ДІЯЛЬНОСТІ	22
<i>Анастасія Кузченко, Валерій Яценко</i>	РОЗВИТОК ФІНТЕХ-ІНДУСТРІЇ У СВІТІ: ТЕНДЕНЦІЇ ТА ВИКЛИКИ	24
<i>Сергій Дрозд</i>	КЛЮЧОВІ АСПЕКТИ ТА ВИКЛИКИ ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ	28
<i>Сергій Миненко, Валерія Кочнєва</i>	ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ ПУБЛІЧНИХ ЗАКУПІВЕЛЬ З МЕТОЮ ВИЯВЛЕННЯ ТА УНИКНЕННЯ КОРУПЦІЇ	32
<i>Владислава Лук'янова, Валерій Яценко</i>	ПЕРСПЕКТИВИ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО І ЛЮДЕЙ	35
<i>Дмитро Діденко, Світлана Коломієць</i>	РОЗВИТОК ЕЛЕКТРОННОЇ КОМЕРЦІЇ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ	38
<i>Ілля Лубенець, Світлана Коломієць</i>	ВПЛИВ ЦИФРОВОЇ ЕКОНОМІКИ НА СТАН ГРОМАДСЬКОГО ЗДОРОВ'Я НАСЕЛЕННЯ	41

## ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

<b>СЕКЦІЯ 2</b>	<b>КІБЕРЗАГРОЗИ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ</b>	<b>44</b>
<i>Vadym Dun, Serhii Mynenko</i>	АНАЛІЗ ВПЛИВУ ВЕЛИКИХ КІБЕРІНЦИДЕНТІВ НА АКЦІЇ КОМПАНІЇ	44
<i>Kuan Zhang</i>	THE RISKS OF ELECTRONIC PAYMENTS IN CROSS-BORDER E-COMMERCE	48
<i>Анна Голопорова, Валерій Яценко</i>	МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ КІБЕРБЕЗПЕКИ: ВИКЛИКИ ТА МОЖЛИВОСТІ	50
<i>Олександр Воробйов, Валерій Яценко</i>	КІБЕРБЕЗПЕКА У МЕРЕЖАХ 5G: ПРАКТИЧНІ ВИКЛИКИ ТА РИЗИКИ	53
<i>Віталія Койбічук</i>	КІБЕРБЕЗПЕКА БІЗНЕСУ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ: ДОСВІД ЄС	56
<i>Сергій Миненко, Ксенія Могильна</i>	ПОЗИТИВНІ Й НЕГАТИВНІ СТИМУЛИ ДО ВИКОРИСТАННЯ КРИПТОВАЛЮТ У ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ	60
<i>Назар Фененко</i>	ПЕРСОНАЛ КОМПАНІЇ ЯК «БРАМА» ДЛЯ КІБЕР АТАК	64
<i>Єлизавета Литюга, Валерій Яценко</i>	ПЕРСПЕКТИВИ РОЗВИТКУ ХАКТИВІЗМУ ТА ХАКЕРСЬКИХ АТАК В СФЕРІ ФІНАНСОВИХ ПОСЛУГ: ВИКЛИКИ ТА ШЛЯХИ ПРОТИДІЇ	67
<i>Катерина Солярова, Ганна Яровенко</i>	ПРОГНОЗУВАННЯ ІНФОРМАЦІЙНИХ ТРЕНДІВ КІБЕРЗЛОЧИНІВ	71
<i>Вікторія Боженко, Олександр Росенко</i>	ОСОБЛИВОСТІ ДЕРЖАВНОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ФІНАНСОВИХ УСТАНОВ У ЄВРОПЕЙСЬКОМУ СОЮЗІ	74
<i>Вікторія Боженко, Іван Гончарук</i>	МАСШТАБИ НЕЗАКОННОГО МАЙНІНГУ КРИПТОВАЛЮТ	77
<i>Архипов Станіслав Ганна Яровенко</i>	КІБЕРФРОНТ У ВІЙНІ РОСІЇ ПРОТИ УКРАЇНИ 80 КЛЮЧОВІ АСПЕКТИ ВІДПОВІДАЛЬНОЇ ПОВЕДІНКИ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ У КІБЕРПРОСТОРІ	82

## ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

<i>Xinxin Wang</i>	ВИКЛИКИ КІБЕРБЕЗПЕКИ, ЩО СТОЯТЬ ПЕРЕД ГАЛУЗЗЮ ФІНАНСОВИХ ПОСЛУГ	85
<i>Олена Пахненко</i>	СОЦІО-ДЕМОГРАФІЧНІ ДЕТЕРМІНАНТИ ВРАЗЛИВОСТІ КОРИСТУВАЧІВ ФІНАНСОВИХ ПОСЛУГ ДО КІБЕРРИЗИКІВ	90
<b>СЕКЦІЯ 3</b>	<b>ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ</b>	<b>93</b>
<i>Альона Рапута</i>	КОНВЕРГЕНЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ ФІНАНСОВИМ ЗЛОЧИНАМ	93
<i>Анастасія Савенко, Валерій Яценко</i>	КІБЕРБЕЗПЕКА В МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВАХ: РОЗРОБКА ТА ВПРОВАДЖЕННЯ СТРАТЕГІЙ ЗАХИСТУ	97
<i>Анна Поліщук</i>	ІНВЕСТИЦІЇ В КІБЕРБЕЗПЕКУ ЯК ДРАЙВЕР РОЗВИТКУ КОМПАНІЇ	101
<i>Діана Харченко</i>	ВАЖЛИВІСТЬ ІНВЕСТИЦІЙ У КІБЕРБЕЗПЕКУ ДЛЯ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ КОМПАНІЙ	104
<i>Поліна Терляківська, Валерій Яценко</i>	РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ЦИФРОВІЙ ЕКОНОМІЦІ: ТЕХНОЛОГІЧНІ ТА ЕТИЧНІ АСПЕКТИ	107
<i>Артем Штефан</i>	ТЕХНОЛОГІЯ БЛОКЧЕЙН ДЛЯ ПРОТИДІЇ КІБЕРЗАГРОЗАМ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ	110
<i>Катерина Славгородська, Валерій Яценко</i>	ЦИФРОВІ ІННОВАЦІЇ У ФІНАНСОВИХ ПОСЛУГАХ: НОВІ МОЖЛИВОСТІ ТА ВИКЛИКИ БЕЗПЕКИ	113
<i>Христина Чуб, Валерій Яценко</i>	ЦИФРОВІ ТЕХНОЛОГІЇ ТА ІННОВАЦІЙНІ ПРОЦЕСИ У РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ	116
<i>Тетяна Доценко, Дарина Березна</i>	ТЕНДЕНЦІЇ МОДЕЛЮВАННЯ DUE DILIGENCE ДЛЯ ПРОТИДІЇ ФІНАНСОВИМ КІБЕРШАХРАЙСТВАМ	120

## СЕКЦІЯ 2 КІБЕРЗАГРОЗИ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ

### АНАЛІЗ ВПЛИВУ ВЕЛИКИХ КІБЕРІНЦИДЕНТІВ НА АКЦІЇ КОМПАНІЇ

#### ANALYSIS OF THE IMPACT OF MAJOR CYBER INCIDENTS ON THE COMPANY'S STOCKS

*Vadym Dun, student*

*Sumy State University, Ukraine*

*Serhii Mynenko, PhD*

*Sumy State University, Ukraine*

In the modern world where information reigns supreme, cyber threats pose a significant risk to the financial stability and security of organizations. Data privacy and cybersecurity issues have emerged as major drivers of business risk in recent years. Major cyber incidents such as hacking, data breaches, and malware have the potential to cause significant financial losses and impact a company's stock price. Understanding the financial impact of such cyber incidents is crucial as it enables investors, financial analysts, and regulators to develop effective risk management strategies and make informed investment decisions. This analysis also contributes to the development of cybersecurity policies and practices at a global level by identifying vulnerabilities and deficiencies in data protection systems. Measures can be developed to prevent and respond to cyber threats while improving risk management practices in this area. This paper provides a basic overview of the aftermath of the 2017 Equifax cyberattack.

There are many definitions in this field, but let us focus on the following - major cyber incidents can be defined as serious breaches of information system security that lead to unauthorized access to sensitive data, information leakage, disruption of computer networks and serious consequences for organizations and individuals (NCSC, 2023). Such incidents can include hacking attacks, viruses, phishing attacks, data breaches, attacks on critical infrastructure, and other forms of cyber threats. They can occur either within a single organization or on a national or international scale.

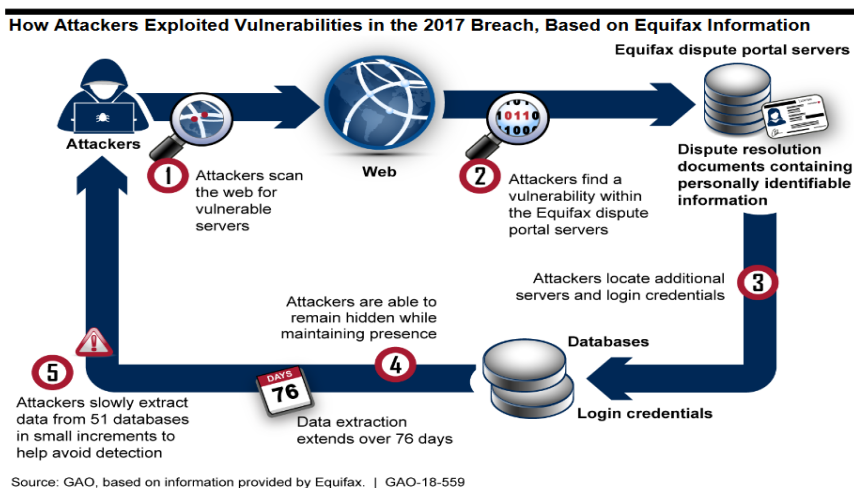
In terms of company shares, first of all, they are a tool, and I play an essential role in the financial sector. They represent shares in companies that investors can buy. Stocks allow you to invest money and benefit from growth and dividends. They also reflect the capitalization of companies, which indicates their importance and attractiveness to investors. Changes in stock prices can be an indicator of economic health and market confidence. Companies may also issue new shares to raise additional capital. Stocks provide liquidity to the market,

allowing investors to buy and sell them. In general, stocks provide an investment opportunity, access to capital and serve as an indicator of the health of the economy.

But we are going to focus on a relatively recent incident that happened to Equifax. This situation is one of the most popular - this large-scale cyberattack compromised the personal information of approximately 147 million people. In the wake of the attack, Equifax's stock plummeted and the company faced significant financial and reputational losses, but let's go in order.

Equifax is a widely recognized multinational consumer credit reporting agency based in Atlanta, Georgia. It is one of the top three largest credit reporting agencies in the world, alongside Experian and TransUnion. With millions of consumers and businesses globally, Equifax collects and analyzes credit and demographic information. It offers credit monitoring, fraud prevention services, and data insights to both individuals and businesses. Notably, Equifax is a member of the S&P 500® Index, and its common stock is traded on the New York Stock Exchange under the symbol EFX. (Investopedia, 2023)

To avoid describing the details of the attack process itself, for easier understanding we can use the illustration by Government Accountability Office, based on information provided by Equifax (GAO, 2018):



**Figure 1. Scheme How Attackers Exploited Vulnerabilities**

The announcement of the cyberattack triggered a negative reaction from investors and the market, resulting in a sharp drop in the stock price in the first two days after the announcement. The decline in the share price was more than 30%, a

significant drop. This indicates the seriousness and magnitude of the incident and caused a loss of investor confidence. The stock price continued to decline in the following weeks, with a total loss in value of approximately 35%. This share price decline reflects the serious negative impact of the cyberattack on the company's financial position and reputation in the market, and reputation is more important than anything else in our time, and investors simply do not want to take those risks and try to get out of the market as quickly as possible (Carsten Giebe, 2020). Below we can see the graphic (Investing.com, 2023):



**Figure 2. Price History - NYSE:EFX**

Following the decline in Equifax's stock price, the company faced a period of market volatility. Restoring investor and market confidence was paramount to the company's ability to halt this steep decline. According to the company's financial reports, Equifax reported a 2.7 percent decline in annual revenue compared to the previous year. The stock's drop wiped out about \$6 billion of its market value. This shows that the incident had a negative impact on the company's overall financial performance. (MarketWatch, 2017) The attack did not put the company out of business, but it did result in serious legal repercussions and a significant amount of compensation and fines - It is clear that ultimately good risk must result in increased profitability or company value. Most times this will be reflected in business and financial metrics such as profitability and company valuation. (E. Ted Prince, 2016) And until all these nuances are settled, we can't see any stability in the stock price, and it wasn't until 2019 that the company agreed to pay a \$700 million fine to the U.S. Federal Trade Commission and other regulators. In addition, a \$380.5 million restitution agreement was reached that



included cash payments to affected customers and expenses related to fraud protection and credit identity monitoring (Investopedia, 2023).

Summarizing all of the above, we can formulate a kind of prediction of the consequences of cyberattacks. The impact of these actions on stocks can be seen with the naked eye - in Equifax's experience, we can see that the company can lose up to 35% of shareholder value in an instant. Although the stock has recovered somewhat over time and with the implementation of security enhancements, the impact of the cyberattack has left a lasting impact on the company's reputation and financial performance. All of this suggests that cyberattacks can have serious financial consequences for companies, including significant losses in stock value and the emergence of a period of market volatility. It is important to note that the change in Equifax's stock price as a result of the cyberattack is only part of the complex financial impact. The company also faced high investigation and remediation costs, fines and legal fees, and a loss of customer and market confidence. This case is an example of how cyber incidents can seriously impact a company's financial position and reputation, particularly in the context of our company's specific circumstances.

### References

1. National Cyber Security Centre (2023). About NCSC: Incident Management. <https://www.ncsc.gov.uk/section/about-ncsc/incident-management>
2. Investopedia (2023). Top Three Credit Bureaus. <https://www.investopedia.com/personal-finance/top-three-credit-bureaus/>
3. Government Accountability Office. (2018). Equifax Data Breach: Actions Needed to Strengthen Response and Recovery Efforts. <https://www.gao.gov/assets/gao-18-559.pdf>
4. Carsten Giebe (Armg Publishing) (2020). Big Data & Analytics as a sustainable Customer Loyalty Instrument in Banking and Finance. <https://armgpublishing.com/wp-content/uploads/2020/01/7-2.pdf>
5. Investing.com (2023) Equifax, Inc. Stock Chart. <https://ru.investing.com/pro/NYSE:EFX/charts>
6. MarketWatch. (2017). Equifax's stock has fallen 31% since the breach disclosure. <https://www.marketwatch.com/story/equifaxs-stock-has-fallen-31-since-breach-disclosure-erasing-5-billion-in-market-cap-2017-09-14>
7. E. Ted Prince (Armg Publishing) (2016). Risk Management and Behavioral Finance. <https://armgpublishing.com/wp-content/uploads/2016/12/files/fmir/volume-2-issue-2/1.pdf>