ХАКЕРСЬКІ АТАКИ – СУТТЄВА ЗАГРОЗА ФУНКЦІОНУВАННЮ СВІТОВОГО ФОНДОВОГО РИНКУ

HACKER ATTACKS – SUBSTANTIAL THREAT TO FUNCTIONING OF THE WORLD STOCK MARKET

УДК 336.764

Кухтин О.Б.
здобувач кафедри міжнародних економічних відносин
Тернопільський національний економічний університет

У статті описано загрози хакерських атак для учасників світового фондового ринку. Відзначено, що багаторазові спроби зломів і нападів на сервери компаній фондового ринку наносять їм серйозну фінансову та іміджеву шкоду. Визначено причини зростання кількості кібератак. Подано класифікацію хакерських атак на світовому фондовому ринку. Вказано на значне збільшення кіберзлочинності на фондовому ринку та утворення хакерських злочинних груп. Акцентовано увагу на потребі постійного вдосконалення систем забезпечення інформаційної безпеки учасників світового фондового ринку для захисту від постійно зростаючої кількості злочинних хакерських атак.

Ключові слова: *світовий фондовий ринок, хакерські атаки, інформаційна безпека, кіберзлочинність, крадіжка торгових алгоритмів.*

В статье описаны угрозы хакерских атак для участников мирового фондового рынка. Отмечено, что многократные попытки взломов и нападений на серверы компаний фондового рынка наносят им серьезный финансовый и имиджевый вред. Определены причины роста количества кібератак. Представлена классификация хакерских атак на мировом фондовом рынке. Указано на значительное увеличение киберпреступности на фондовом рынке и образования хакерских преступных групп. Акцентировано внимание на необходимости постоянного совершенствования систем обеспечения информационной безопасности участников мирового фондового рынка для защиты от растущего числа преступных хакерских атак.

Ключевые слова: *мировой фондовый рынок, хакерские атаки, информационная безопасность, киберпреступность, кража торговых алгоритмов.*

The article describes the threats of hacker attacks for participants in the world stock market. It is noted that multiple attempts at cracking and attacks on servers of stock market companies cause them serious financial and image damage. The reasons for increasing the number of cyber attacks are determined. The classification of hacker attacks on the world stock market is presented. The significant increase in cybercrime on the stock market and the formation of hacker criminal groups is indicated. The attention is focused on the need for continuous improvement of the information security systems of the participants of the world stock market in order to protect against the ever-increasing number of criminal hacker attacks.

Key words: *world stock market, hacker attacks, information security, cybercrime, theft of trading algorithms.*

Постановка проблеми. Розвиток та впровадження глобальних інформаційно-комунікаційних технологій, технологічних інновацій, глобальних комп'ютерних мереж є визначальним у нинішньому суспільстві. За словами Біла Гейтса, «коли в епоху індустріалізації машини у тисячі разів примножували мускульну силу людини, то в епоху інформатизації інформаційні технології у тисячу разів примножують інтелектуальні можливості людини» [3, с. 418]. Однак ці процеси супроводжуються й значними ризиками. Враховуючи стрімке збільшення обсягів даних, які обробляються, дуже важливим стає питання їх захисту від протизаконних посягань. Зокрема, ця проблема дуже гостро відчувається на фондовому ринку, оскільки саме ця сфера однією з перших упроваджує та активно використовує передові інноваційні технології та засоби телекомунікації. Багаторазові спроби зломів та вдалі спроби нападів на сервери фінансових установ гостро окреслюють проблему забезпечення інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Проблема зростання кількості хакерських атак на фондовому ринку певною мірою досліджувалася в різних аспектах у працях вітчизняних і зарубіжних науковців, серед них: Р. Андерсон, О. Іванов, А. Нашинець-Наумова, В. Матюшок, Ю. Мельников, А. Теренін, Д. Мельник, Е. Робертсон, С. Джонсон, Р. Лангнер, Т. Мур, Р. Клейтон та ін. Водночас існує потреба у проведенні подальшого, більш комплексного дослідження цього питання.

Постановка завдання. Метою статті є теоретичне обґрунтування сутності хакерських атак і загрози від них учасникам світового фондового ринку та визначення шляхів мінімізації їх наслідків.

Виклад основного матеріалу дослідження. Усі учасники фондового ринку в процесі своєї роботи стикаються з низкою технологічних ризиків. Їх умовно можна розділити на кілька груп. По-перше, це збої в роботі інформаційних систем. Уразливість цих систем призводить до затримок у роботі та втрати важливих даних. По-друге, стрімке зростання дезінформації у цифровому світі. Неправдива та провокаційна інформація поширюється фактично миттєво серед усіх учасників ринку та може спричинити серйозні наслідки. По-третє, це безпосередньо хакерські атаки на фондовий ринок.

Хакерські атаки спрямовані на отримання інформації обмеженого доступу, що зберігається на робочих комп'ютерах (фінансова інформація, персональні дані, документи конфіденційного

характеру), яка згодом може бути використана для розкрадання грошових коштів, кібершпигунства, вимагання та здійснення інших злочинних дій.

Загалом хакери, що здійснюють злочинні операції на фондовому ринку, є висококваліфікованими спеціалістами, які своїми діями здатні вивести з ладу сервери фінансових компаній та бірж, а також проникати у їхні системи безпеки. Хакерські атаки можуть спричиняти значні збитки, найчастіше вони носять організований характер, і досить часто серед спільників можуть бути представники власного персоналу компанії чи біржі.

Останнім часом біржові майданчики змушені приділяти багато уваги та зусиль для захисту своєї інфраструктури від хакерів. Експерти все частіше говорять про те, що кіберзлочинність стає однією з головних загроз фінансовому сектору. У доповіді Комісії із цінних паперів США, опублікованій у лютому 2016 р., повідомлялося, що 88% брокерів так чи інакше стикаються у своїй роботі з хакерськими атаками [6]. У світі кількість злочинів за участю хакерів щомісяця збільшується на 3-4%. А отже, учасники фондового ринку вимушені проводити заходи, пов'язані із захистом місць зберігання та обробки даних, а також каналів і засобів передачі даних.

Для кращого розуміння природи та загроз від хакерських атак на світовому фондовому ринку варто провести їх класифікацію (табл. 1).

Як видно з даних таблиці, кіберзлочинність характеризується різноманітністю форм та видів, а її вигадливість та зухвалість постійно зростають.

Сьогодні хакери мають можливість продавати іншим інформацію, яку вони отримали, чи навіть «продавати» свої навички на «чорному ринку» кіберзлочинності [2, с. 3].

Кібератаки стали ефективним інструментом у руках маніпуляторів, оскільки здобуту інформацію вони використовують для отримання конкурентної переваги під час торгівлі на біржі. При цьому хакерів цікавить не тільки доступ до фінансових даних бірж і фінансових компаній, а будь-яка інформація, що може вплинути на хід торгів. Особливу увагу приділяють програмному забезпеченню, що може не тільки викрадати інформацію, а й повністю зруйнувати комп'ютерну мережу. Часто в коді системи є слабкі місця, що дають змогу зловмисникам отримати «доступ до непублічної інформації». Іноді, незважаючи на всі зусилля із захисту систем і управління ризиками інформаційної безпеки, кіберзлочинцям удається отримати доступ і використовувати інформацію, яка знаходиться у системах.

Ситуація із забезпеченням цілісності та конфіденційності інформації та збільшенням загроз її втрати ускладняється ще й тим, що з розвитком техніки обробка інформації здійснюється у віддаленому доступі, тобто дистанційно, і організація

Таблиця 1

Класифікація хакерських атак на світовому фондовому ринку

За метою здійснення	отримання грошової винагороди	переважно основною метою кібератак є бажання збагатитися
	отримання певних переваг у процесі торгів	об'єктом є будь-яка інформація чи дані, здатні вплинути на хід торгів
	часткова чи повна дестабілізація діяльності окремих учасників	може здійснюватися для усунення конкурентів
За масштабом нанесених збитків	незначні	несуть за собою невеликі збитки
	середні	спричиняють більш серйозні збитки
	глобальні	спрямовані на значну і довготривалу дестабілізацію діяльності учасників фондового ринку
За складністю здійснення	прості	їх легко виявити та зменшити негативний вплив від них
	складні	їх важко виявити, віруси можуть бути у системах досить довготривалий період, перш ніж будуть виявлені та знешкоджені
За способами реалізації	викрадення актуальної інформації для продажу	здобута інформація переважно перепродується трейдерам для конкурентної переваги під час торгівлі на біржі
	викрадення алгоритмів для високочастотної торгівлі	найчастіше здійснюються, щоб повернути викрадені алгоритми за винагороду
	порушення цілісності та доступності комп'ютерних даних і систем	відбувається ушкодження комп'ютерних даних, неавторизований доступ до захищених комп'ютерів, неавторизоване використання комп'ютерних мереж
	публікація у ЗМІ інформації, здатної вплинути на хід торгів	використовується для маніпулювання інформацією
	шантаж учасників ринку	хакери-шантажисти надсилають брокерам по електронній пошті листи, у яких вимагають заплатити їм, щоб запобігти нападу, який може призвести до краху їхніх торговельних систем
	фішинг-шахрайство	спосіб шахрайства, яким користуються злочинці, щоб обманом примусити користувачів розкрити свої персональні дані

Джерело: складено автором

навіть не завжди знає, де зберігається та оброблюється її інформація [5, с. 13].

Останніми роками почастішали випадки злому систем хедж-фондів і HFT-фірм для крадіжки торгових алгоритмів. Атаки, спрямовані на крадіжку торгових алгоритмів, рідко здійснюються з метою використати їх для безпосередньої торгівлі на біржі. Куди частіше в разі успішного злому зловмисники пропонують повернути викрадені алгоритми за винагороду.

Крім того, злочинці можуть побічно управляти алгоритмами високочастотної торгівлі. За словами Натаніеля Глейхера [6], керівника стратегії кібербезпеки Illumio, «напади, націлені на джерела інформації, такі як Твіттер, The Associated Press, можуть вплинути на ціни акцій».

Нерідко об'єктом хакерських атак стають брокерські рахунки. Можливість їх злому існує завжди, оскільки злочинець може отримати доступ до брокерського рахунку, викравши ключі шифрування і пароль за допомогою шпигунських програм.

Також набуває популярності ще один вид кіберзлочинності – фішинг. Це вид хакерських атак, коли злочинці викрадають персональні дані користувачів, розсилаючи їм листи від імені відомих і шанованих брендів. Головний спеціаліст з інформаційної безпеки United Data Technologies Майк Санчес навів приклад: «Минулого тижня ми перевіряли безпеку в одній фінансовій установі. Нам надали список із 500 співробітників. Сімдесят п'ять відсотків з них, отримавши фішинговий лист, натиснули на посилання, яке запитує їх ID і пароль, та передали ці дані» [10]. У результаті дані учасників фондового ринку були викрадені в злочинних цілях.

Злочинці можуть діяти як поодинці, так і групами осіб, а стрімкий розвиток комунікаційних технологій дає їм змогу миттєво обмінюватися інформацією про слабкі місця у системах захисту серверів, поширювати програмне забезпечення для їх злому. Мережа Інтернет дає змогу хакерам об'єднуватися у віртуальному просторі в злочинні групи, але при цьому знайти і викрити їх дуже складно.

Викрадення даних, здатних вплинути на хід торгів, трапляється на біржах дуже часто. Таку інформацію легко використати або продати. Але у цьому разі атакам піддаються не тільки самі біржі, а й інші впливові у фінансовому світі компанії. Така проблема виникла й у американських ресурсів, що публікують прес-релізи компаній PRNewswire, Marketwired і Businesswire. Вони не знали, що протягом п'яти років хакери викрадали важливу для ринку інформацію ще до її публікації. Доступ до даних кіберзлочинці отримали за допомогою фішингових атак. Хакери працювали у співробітництві з трейдерами, які використовували отримані дані для торгів на біржі, а виручені кошти переводили в офшори. Збиток від дій групи оцінюється, за різними даними, від 30 до 100 млн. доларів [12].

Ті учасники ринку, на яких уже була здійснена кібератака, часто зіштовхуються з великою проблемою: повідомити публічно, що на них була здійснена атака, і залучити зовнішню допомогу під час розслідування мотивів та наслідків атаки чи провести внутрішнє розслідування і не повідомляти про атаку публічно, щоб у подальшому знизити резонанс навколо цієї події [2, с. 4]. Дуже часто компанії приховують кібератаки, виправдовуючись звичайними технологічними збоями. Частіше за все компанії вибирають другий варіант, щоб не ускладнити ситуацію репутаційною шкодою, що фактично діє на користь зловмисників. Вони приховують інформацію про хакерські атаки, боячись втратити довіру клієнтів.

Коли відбувається якийсь серйозний збій, торги просто зупиняються. Для того щоб мінімізувати можливі збитки від хакерських атак, компанії використовують спеціальне програмне забезпечення і програмно-апаратні комплекси та системи забезпечення інформаційної безпеки. Дані системи захисту інформації фінансових компаній повинні відповідати рівню важливості та секретності інформації, яка захищається.

Висновки з проведеного дослідження. Нові реалії сучасності потребують нового підходу до питання забезпечення інформаційної безпеки учасників фондового ринку. З кожним роком зростає загроза хакерських атак на сервери фінансових компаній та бірж. Хакери використовують недосконалості систем безпеки учасників фондового ринку для здійснення злочинних дій. Дії хакерів на фондовому ринку наносять серйозну шкоду компаніям як у фінансовому плані, так і шкоду їх іміджу.

Кібератаки на фондовому ринку можна розділити на декілька видів: порушення цілісності та доступності комп'ютерних систем та їхніх даних; несанкціоноване використання обчислювальних інформаційних ресурсів комп'ютерних систем; викрадення актуальної інформації; шантаж учасників ринку; фішинг-шахрайство.

Дані, отримані в результаті злочинних дій хакерів, можуть бути використані по-різному: для вимагання коштів, для перепродажу третім особам, для отримання переваг у процесі торгів, для здійснення фальсифікацій тощо.

Отже, існує потреба постійного вдосконалення систем забезпечення інформаційної безпеки учасників світового фондового ринку для захисту від зростаючої кількості злочинних хакерських атак.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Амелін О., Чумак К. Кваліфікація кіберзлочинів та її вплив на компетенцію органів правопорядку. Вісник Національної академії прокуратури України. 2017. № 2(48). С. 71-79.

2. Бочкова А.А. Киберугрозы на фондовых рынках: критерии анализа. Скиф. Вопросы студенческой науки. 2007. № 1. С. 2-5.

3. Гейтс Б. Бизнес со скоростью мысли. М.: ЭКСМО-Пресс, 2000. 480 с.

4. Гребеньков А.А. Современное состояние проблемы вредоносного программного обеспечения: основы компьютерной кримимнальной армалогии. Известия Юго-Западного государственного университета. 2014. № 6(57). С. 159-165.

5. Иванов О., Робертсон Э. Современные тенденции управления рисками в крупных компаниях. ЭТАП: экономическая теория, анализ, практика. 2012. № 1. С. 4-18

6. Защитить алгоритм: Что интересует хакеров, атакующих фондовый рынок. URL: https://geektimes.ru/company/itinvest/blog/271262/.

7. Матюшок В. Информатизация как стратегическое направление развития мировой экономики. Вестник РУДН. Серия «Экономика». 2002. № 1(8). С. 35-43.

8. Мельников Ю., Теренини А. Возможности нападения на информационные системы банка из Интернета и некоторые способы отражения этих атак. Банковские технологии. 2003. № 1.

9. Нашинець-Наумова А. Реалізація адміністративно-правових форм у сфері забезпечення інформаційної безпеки корпорації. Підприємництво, господарство і право. 2015. № 8. С. 46-48.

10. Разбор: могут ли хакеры на самом деле взломать биржу. URL: https://habrahabr.ru/company/itinvest/blog/336028/.

11. Скіцько В.І. Індустрія 4.0 як промислове виробництво майбутнього. Інвестиції: практика та досвід. 2016. № 5. С. 33-40.

12. Хакеры и биржи: как атакуют сферу финансов. URL: https://habr.com/company/iticapital/blog/332080/.

13. Can Recent Attacks Really Threaten Internet Availability? European Network and Information Security Agency. 2013. 12 Apr. URL: http://www.finanstilsynet.no/Global/Temasider/IT-tilsyn/Flash_Note_02-2013%5B1%5D.pdf.

14. Johnson C. Please Police Me. 12th Association of anti Virus Asia Researchers International Conference. URL: https://secure.eset.com/us/resources/white-papers/Please_Police_Me.pdf.

15. Langner R. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy. 2011. Vol. 9. № 3. P. 49-51.

16. Moore T., Clayton R., Anderson R. The Economics of Online Crime. The Journal of Economic Perspectives. 2009. Vol. 23. № 3. P. 3-20.

ІНСТИТУЦІЙНЕ СЕРЕДОВИЩЕ ФУНКЦІОНУВАННЯ МІЖНАРОДНИХ ФІНАНСОВИХ ЦЕНТРІВ

INSTITUTIONAL ENVIRONMENT FUNCTIONING OF INTERNATIONAL FINANCIAL CENTERS

УДК 339.926

Ліфанова М.І.
аспірант кафедри
міжнародної економіки
Тернопільський національний
економічний університет

У статті розглянуто інституційне середовище функціонування міжнародних фінансових центрів. Запропоновано авторський підхід до сутності інституційного середовища міжнародних фінансових центрів, розглянуто його складники, функції, а також інституційне забезпечення міжнародних фінансових центрів.

Ключові слова: *інституційне середовище, інституційне забезпечення, інституції, міжнародний фінансовий центр, банкострахування.*

В статье рассмотрена институциональная среда функционирования международных финансовых центров. Предложен авторский подход к сущности институциональной среды международных финансовых центров, рассмотрены его составляющие, функции, а также институциональное обеспечение международных финансовых центров.

Ключевые слова: *институциональная среда, институциональное обеспечение, институты, международный финансовый центр, банкострахование.*

In the article the institutional environment of the functioning of international financial centers is considered. The author's approach to the essence of the institutional environment of international financial centers is proposed, its components, functions, and institutional support of international financial centers are considered.

Key words: *institutional environment, institutional support, institutions, international financial center, bank insurance.*

Постановка проблеми. Головний урок, який дала економіці практика формування нових ринкових відносин, полягає у тому, що чинник інституційного середовища є надзвичайно важливим. Його ігнорування істотно обмежує можливості науки у формуванні адекватних уявлень про економічну реальність.

Ринкові перетворення в українській економіці та її входження до світового економічного простору надали нової якості й процесу розвитку вітчизняного фінансового сектору. За цих обставин його аналіз дає змогу сформулювати висновок про необхідність послідовної інституціоналізації цього сектору економіки [1, с. 92]. Величезну роль відіграє інституційне середовище, яке сприятиме ефективному функціонуванню міжнародних фінансових центрів.