

ОСОБЛИВОСТІ КІБЕРАТАК НА ФУТБОЛЬНІ КЛУБИ КРАЇН СВІТУ

Кулик Сергій Михайлович,

кандидат політичних наук,

доцент кафедри міжнародних відносин і регіональних студій

Волинського національного університету імені Лесі Українки

ORCID ID: 0000-0001-7520-7426

Від атак хакерів все частіше страждають міжнародні та національні спортивні організації, спортивні клуби, стадіони, спортсмени, а також уболівальники і глядачі. Автор обрав для дослідження футбольні клуби, бо футбол – це «спорт № 1» у більшості країн Європи і має мільйони шанувальників і фанатів. За допомогою структурно-функціонального, порівняльного, біхевіористичного методів розглянуто особливості здійснення кібератак на клуби та їхні наслідки. Метод теорії груп дав можливість трактувати хакерську активність як боротьбу за політичну владу, тиск, вплив на прийняття політичних рішень. Виявлено, що кібератак зазнають системи життєзабезпечення населення міст, у яких відбуваються важливі матчі. Встановлено, що РФ і Китай підтримують кібертероризм на державному рівні. Різні російські хакерські групи діють в інтересах уряду РФ. Тому досить складно винести доказове судове рішення з цих справ. Кібератаки все частіше є причиною погіршення двосторонніх відносин між країнами. Водночас у футбольних клубах запроваджено розширений протокол і план дій у випадку виявлення кіберзагроз. Контролюючі органи країн запроваджують штрафні санкції до клубів за сплату ними викупу хакерам і надання представникам державної влади недостовірної інформації про масштаби втручання.

Увага звернута на політичний підтекст хакерських атак на українські футбольні клуби під час збройної агресії РФ проти України. Приводом для цього є їхня чітка державницька позиція, відстоювання національних інтересів України. Від незаконного втручання страждають сайти клубів, трансляції матчів. Так, у червні 2022 р. під час фіналу плей-офф відбору чемпіонату світу-2022 Уельс – Україна хакери підмінили трансляцію матчу кадрами з російського пропагандистського каналу «Известия». Він транслював інтерв'ю президента РФ В. Путіна та сюжет про нібито обстріли Донецька українськими військовими. Все це підтверджує думку про гібридний характер цієї війни і остаточно спростовує тезу про «спорт поза політикою».

Ключові слова: кібератаки, національна безпека, футбольні клуби, міжнародні спортивні організації, хакери "Fancy Bear", збройна агресія Росії.

Kulyk Serhii. Features of cyber attacks on football clubs of the countries of the world

International and national sports organizations, sports clubs, stadiums, athletes, as well as fans and spectators are increasingly affected by hacker attacks. The author chose football clubs for research, because football is the «№ 1 sport» in most European countries and has millions of fans and fans. With the help of structural-functional, comparative, behavioral methods, the peculiarities of cyberattacks on clubs and their consequences are considered. The group theory method made it possible to interpret hacker activity as a struggle for political power, pressure, influence on political decision-making. It was revealed that the life support systems of the population of the cities where important matches take place are subjected to cyber attacks. It was established that the Russian Federation and China support cyber terrorism at the state level. Various Russian hacker groups act in the interests of the Russian government. Therefore, it is quite difficult to make an evidentiary judgment in these cases. Cyber attacks are increasingly the cause of deterioration of bilateral relations between countries. At the same time, football clubs have introduced an extended protocol and an action plan in case of detection of cyber threats. Controlling bodies of countries are imposing fines on clubs for paying ransom to hackers and providing state authorities with unreliable information about the extent of the interference.

Attention is drawn to the political subtext of hacker attacks on Ukrainian football clubs during the armed aggression of the Russian Federation against Ukraine. The reason for this is their clear statesmanship position, defense of the national interests of Ukraine. Club websites and match broadcasts suffer from illegal interference. So, in June 2022, during the Wales-Ukraine World Cup 2022 playoff final, hackers replaced the broadcast of the match with footage from the Russian propaganda channel "Izvestia". It broadcast an interview with the President of the Russian

Federation V. Putin and a story about the alleged shelling of Donetsk by the Ukrainian military. All this confirms the opinion about the hybrid nature of this war and finally refutes the thesis about "sport outside of politics".

Key words: *cyber attacks, national security, football clubs, international sports Organizations, "Fancy Bear" hackers, armed aggression of Russia.*

Актуальність дослідження. Від атак хакерів все частіше страждають міжнародні та національні спортивні організації, спортивні клуби, спортивні споруди, спортсмени, відомі представники спорту, а також уболівальники і глядачі. Автор обрав для дослідження саме футбольні клуби, адже футбол – це «спорт № 1» у країнах Європи і має мільйони шанувальників та величезний комерційний успіх. Найбільш активно ці атаки відстежують відповідні державні структури та організації США та Об'єднаного Королівства Великої Британії та Північної Ірландії.

Мета – проаналізувати особливості здійснення кібератак на футбольні клуби країн світу.

Стан вивчення проблеми в науковій літературі. Наукових публікацій із тематики дослідження поки що небагато. Ці питання досліджують переважно фахівці із захисту інформаційних мереж [1], журналісти. Широкого розголосу набули кібератаки на міжнародні спортивні організації – МОК, Всесвітнє Антидопінгове агентство (ВАДА), Антидопінгове агентство США (USADA), Канадський центр спортивної етики, Міжнародну Асоціацію легкоатлетичних федерацій, Спортивний Арбітражний суд, Міжнародну федерацію футболу (ФІФА) [2]. Значну увагу звертають на кібер-безпеку проведення Олімпійських і Паралімпійських ігри, щоб унеможливити спроби зловмисників зірвати головну спортивну подію у світі. Однак окремих досліджень щодо хакерських атак на футбольні клуби поки що немає.

Методи дослідження. Автор використав системний підхід. Тобто з'ясував, яку актуальну важливу інформацію зберігають у своїх ІТ-системах футбольні клуби; які мотиви і вимоги переслідують хакери; загрози і наслідки кібератак; як керівництво клубів взаємодіють із відповідними державними органами для мінімізації несанкціонованих втручань.

Структурно-функціональний метод передбачив вивчення функціональних зв'язків, взаємодію елементів, функціональне призначення служб, департаментів, відповідальних за кібербезпеку спортивних клубів. За допомогою порівняльного методу автор зіставив шпигунські атаки із метою виявлення спільних рис та їх специфіки. Психологічний метод був ефективний при з'ясуванні особистісних мотивів організаторів атак, їх позиціонування. Метод теорії груп дав можливість розглянути хакерську діяльність як боротьбу за політичну владу, тиску, вплив на прийняття політичних рішень.

Виклад основного матеріалу дослідження. Футбольні клуби – вигідні цілі для атак хакерів. У ІТ-системах клубів зберігається значна кількість важливої інформації про сотні тисяч осіб – фанатів, співробітників, гравців, конфіденціальні ділові і платіжні дані. У випадку несанкціонованого проникнення зловмисники можуть отримати інформацію про трансферні плани клубів, контракти гравців і комерційні угоди. Крім того, кібератаки спрямовані проти конкретних гравців, керівників та уболівальників клубів з метою завдання їм репутаційних втрат. Хакери публікують медичні дані спортсменів, у яких йдеться про «вживання» ними заборонених препаратів, і у такий спосіб створюють історію щодо тих спортсменів, хто із них перебуває у «чорному» списку. На стадіонах клубів як на публічних цивільних об'єктах, потенційну загрозу становить не проникнення і крадіжка інформації, а виведення з ладу життєвоважливих систем. Проблему посилює те, що на стадіонах усі системи працюють всередині однієї мережі. Хакери обирають для атак популярні, найтитулованіші і найдорожчі футбольні клуби. Наприклад, «Манчестер Юнайтед» і «Барселона» входять до трійки найдорожчих футбольних клубів світу, «Барселона» займає

четверте місце у списку кращих футбольних клубів ХХ ст. за версією ФІФА. Тому кібератаки на футбольні клуби та їхню інфраструктуру спричиняють значний суспільно-політичний резонанс.

Автор виділив такі особливості здійснення шпигунських атак на футбольні клуби країн світу:

1. *Використання хакерами тактики «подвійного вимагання» і сплати викупу у криптовалюті.* Фахівці з кібербезпеки переконані, що саме так трапилось із ФК «Манчестер Юнайтед», під час якої зловмисники закодували важливі файли і системи, заважаючи роботі, і викрали

конфіденційні дані. Вони погрожували опублікувати внутрішню інформацію на загальнодоступному ресурсі у випадку несплати викупу. Футбольні клуби найбільше піддаються ризику атаки з боку хакерів, які вимагають криптовалюту як викуп за зашифровану корпоративну інформацію.

2. *Причетність до кібератак хакерів, яким надана державна підтримка, зокрема Китаю і Росії.* Про це свідчить складність кібератак. За інформацією Служби державної безпеки Швеції, до проникнення у комп'ютерні системи національної конфедерації спорту при-

Таблиця 1

Кібератаки на футбольні клуби країн світу*

Дата, об'єкт атаки	Дії хакерів та керівництва клубу
Липень 2018 р., ФК «Ліверпуль»	Хакери отримали доступ до ІТ-мережі, що призвело до крадіжки даних про уболівальників клубу.
Листопад 2020 р., ФК «Манчестер Юнайтед»	Хакери атакували ІТ-системи клубу: отримали доступ у дані, пов'язані з симпатиками або покупцями магазинів "MU", вебсайт і мобільні додатки не постраждали. Атака відбулась напередодні зустрічі з командою «Вест Бромвіч Альбїон» у Прем'єр-лізі на стадіоні «Олд Траффорд». Про крадіжку особистих даних уболівальників і замовників керівництво клубу не повідомляло.
Протягом 2019 р., Велико-британія	За даними Національного центру кібербезпеки Великобританії, від кібератак постраждало 70 % найбільших британських спортивних організацій, що вдвічі перевищує показники серед інших організацій. 30 % з цієї кількості повідомили як мінімум про п'ять інцидентів порушення кібербезпеки, стільки ж зазнали понад 12 тис. дол. США збитків. У липні хакери зламали корпоративну базу даних неназваного клубу Англійської футбольної ліги й зашифрували інформацію. За повернення доступу до неї, вони вимагали викуп у сумі 400 біткойнів (~4 млн. дол. США). Клуб відмовився, тоді хакери відновили атаки, що завдало збитків на сотні тисяч доларів США. Вірус заблокував роботу турнікетів і камер відеоспостереження стадіону.
Липень 2020 р., ФК «Барселона» і президент клубу Ж. Бартомеу	Мета кібератаки – завдати репутаційних втрат клубу шляхом критики Ж. Бартомеу, ради директорів ФК, уболівальників, які їх підтримують. Для цього використали масові коментарі в Інтернеті: 3281 бота створили 19359 повідомлень, 23200 згадувань з негативним відтінком на адресу «Барселони». У соціальних мережах 12,5 % коментарів щодо «Барси» стосувалися кібератаки, 5 % коментарів зробили автоматичні аккаунти. Ці аккаунти постили також посилання на веб-сайт elnacional.cat, який виступає за незалежність Каталонії. Пізніше Х. Бартомеу запідозрили у масштабних репутаційних кібератаках проти своїх опонентів – футболістів Л. Мессі і Ж. Піке. Також жертвами кібератак могли бути колишні гравці ФК «Барселона» Хаві, К. Пуйоль і колишній головний тренер Х. Гвардіола [3].
2017–2018, 2021 рр., Шведська конфедерація спорту	Мета кібератаки – отримати особисту інформацію шведських спортсменів, їх медичні записи, й завдати шкоди їхній репутації. Одна з жертв атаки – футболістка О. Шуг, яка зіграла 72 матчі за збірну Швеції (9 голів) і є срібною призеркою Олімпійських ігор у Ріо-де-Жанейро. Вона отримала помилковий статус відстороненої через допінг [4].

* складено автором самостійно

четне Головне управління Генштабу збройних сил Росії – Головного розвідувального управління Росії (ГРУ), а саме військова частина № 26165 Міністерства оборони. Хакери **“Fancy Bear”** (дослівно «модний ведмідь»), відомі ще як «APT28» і **“Sofacy”**, **“Tsar Team”**. Назва команди різна у зв'язку із застосуванням ними різних інструментів під час атак. **“Sofacy”** працюють із 2008 р. Хакери з групи **“Sofacy”** переважно атакують сектори оборони, енергетики, урядові установи, засоби масової інформації США і європейських країн. Список атак команди зазвичай збігається зі списком інтересів уряду РФ, тому це дає підстави вважати про належність хакерів до ГРУ [5]. Для злому ВАДА вони використали логотип білого ведмедя з маскою джокера.

Відомо, що ці хакери неодноразово здійснювали атаки на міжнародні та національні спортивні організації. Так, у серпні 2016 р. російські хакери зламали базу ВАДА і виклали в мережу Інтернет документи зі списком атлетів, яким організація дозволила використовувати у зв'язку з лікуванням захворювань препарати із переліку заборонених (т. зв. терапевтичні винятки). Серед них були американські тенісистки С. і В. Вільямс і гімнастка С. Байлз. Мотивом для кібератак росіянами, зокрема на ВАДА, Міністерство юстиції США назвало помсту за антидопінгове розслідування проти РФ. У серпні 2016 р. хакери атакували Спортивний арбітражний суд Лозанни, а у січні 2018 р. опублікували вкрадені документи із МОК та Олімпійського комітету США, а також виклали в мережу дані листування працівників МОК та ВАДА. Ці порушення були частиною кампанії РФ, спрямованої проти національних та міжнародних антидопінгових організацій, таких як ВАДА, USADA і ФІФА.

Агент ФБР і директор Національного центру контррозвідки і безпеки США У. Еваніна порадив американцям, які відвідають в Росії Чемпіонат Світу з футболу 2018 р., не брати з собою телефони, ноутбуки та інші гаджети. «Будь-які дані на цих пристроях, особливо ваша особиста інформація, можуть стати

доступні російському уряду або кіберзлочинцям». При цьому на найбільший ризик наражають себе «посадовці корпорацій і урядовці», – заявив фахівець [6]. Профільні відомства США випустили аналогічні попередження перед іншими міжнародними спортивними заходами, наприклад, Зимовими Олімпійськими іграми у Пд. Кореї, Японії. У зв'язку із збільшенням кількості кібератак, британські спецслужби – Національний центр з кібербезпеки, що входить до складу Центру урядового зв'язку, попередили підданих Об'єднаного Королівства і футбольну команду Англії, яка брала участь у ЧС–2018 у Росії, не брати з собою електронні гаджети, тому що вони можуть бути зламані злочинцями або особами, пов'язаними із урядом РФ. На думку експерта у сфері кібербезпеки Н. Дойла, «Росія володіє величезними можливостями зі здійснення хакерських атак, які часто здійснюють через посередників, для того, щоб уряд міг все правдоподібно заперечувати. Мета Росії – викликати хаос і розкол у країнах, які вона вважає ворожими» [7]. Мотивом для кібератак, зокрема на ВАДА, американський Мін'юст назвав помсту за антидопінгове розслідування проти Росії та відсторонення її від Олімпійських ігор.

Як заявляв Президент Росії В. Путін, під час проведення Чемпіонату світу з футболу 2018 р. російським фахівцям вдалось знешкодити майже 25 млн кібератак. Безпосередньо моніторингом кібератак займався національний координаційний центр з комп'ютерних інцидентів та регіональні центри моніторингу. Серед серйозних атак вони назвали шість спроб DDoS NTP-amplification в Калінінграді. Це відбувалось під час перших матчів ЧС. Небезпечними вважали атаки на системи зображення на полі, публічний Wi-Fi, і особливо критичні інженерні системи: системи контролю доступу (вхідні турнікети), пожежна сигналізація, оповіщення, відеоспостереження, ліфти. На той час на кожному стадіоні було більше 20 IT-підсистем. Частина даних зберігалась у зовнішніх системах, у випадку

з ФІФА – це всі персональні дані вболівальників, квитки, медіаконтент та ін. Стадіони відповідають за дані з камер відеоспостереження, все, що пов'язано з фізичною безпекою відвідувачів. Зауважимо, що після ЧС кількість атак різко знизилася [1]. Однак, більш детальної інформації влада РФ не надала.

3. У футбольних клубах запроваджено розширений протокол і план дій у випадку виявлення кіберзагроз. Вони відразу інформують національні організації із кібербезпеки, поліцію, співпрацюють з експертами-консультантами над розслідуванням інцидентів і мінімізацією збоїв в роботі ІТ-систем, ініціюють розслідування.

4. Контролюючі органи країн запроваджують штрафні санкції до клубів за сплату ними викупу хакерам і надання представникам державної влади недостовірної інформації про масштаби втручання. Наприклад, ФК «Манчестер Юнайтед» котується на Нью-Йоркській фондовій біржі, і законодавство США має право застосувати санкції до англійського клубу. Управління контролю за іноземними активами США, підрозділ казначейства, попередило, що сплата викупу лише призведе до збільшення фінансування кіберзлочинців і спонукає їх атакувати інші організації. Тому у випадку задоволення вимог хакерів клубу загрожував багатомільйонний штраф. Крім того, «манкуніанцям» загрожував ще один штраф – від Департаменту інформації Великобританії (ICO) – у випадку доведення порушення захисту даних уболівальників [8].

5. Складність розгляду справ і винесення доказового судового рішення. 13 квітня 2021 р. шведська прокуратура припинила розслідування хакерських атак на Шведську спортивну конфедерацію, які тривали з грудня 2017 р. до травня 2018 р. Це рішення було прийняте через брак умов для судового розгляду або екстрадиції до Швеції [9]. Відомі й інші випадки. Х. Бартомеу – президент найтитулованішого футбольного клубу Іспанії «Барселона», одного із символів Каталонії, змушений був подати у відставку у 2020 р. після того, як його

запідозрили у масштабних репутаційних кібератаках проти своїх опонентів [3].

6. Кібератаки на системи життєзабезпечення населення міст, у яких відбуваються важливі матчі. Хакер зламав комп'ютерну мережу водоочисної системи у м. Олдзмер (штат Флорида, США) і намагався отруїти воду. Він зміг на короткий час у сто разів підняти кількість їдконого натру, хімікату, що додають до системи для контролю кислотності води. Олдзмер (15 тис. населення) розташований неподалік м. Тампа, у якому напередодні – 7 лютого – відбувся фінальний матч за звання чемпіона Національної футбольної ліги – Супербоулі-2021. Суперкубок з американського футболу – це подія, яка приваблює значну кількість глядачів [10].

7. Погіршення двосторонніх відносин між країнами внаслідок кібератак на спортивні організації. У квітні 2021 р. посла Росії викликали до МЗС Швеції в зв'язку з розслідуванням кібератак на Шведську спортивну конфедерацію. Як заявила прокурор М. Люнгквіст: «Розслідування показало, що російська військова розвідка, ГРУ, яка через свій 85-й центр, також відомий як підрозділ 26165, планувала та здійснювала серйозні порушення секретності даних проти Шведської конфедерації спорту. У період з грудня 2017 р. до травня 2018 р. Шведська федерація спорту була об'єктом неодноразових та всебічних порушень кібератак на систему. Злочин кваліфікували як серйозне порушення таємниці даних [11]. Від дипломата очікували пояснень «неприйнятних та серйозних порушень» конфіденційності даних здійснених Росією у 2017–2018 рр. Однак Росія традиційно заперечує причетність до будь-яких кібератак.

Окремо виділимо політичний підтекст хакерських атак на українські спортивні клуби під час збройної агресії РФ проти України. Але перед цим автор зверне увагу на такий випадок. Ймовірно, з метою «лагідної українізації» футбольних клубів Сходу України, у січні 2014 р. було заблоковано роботу порталів ФК «Металург» (Донецьк) і «Зоря»

(Луганськ). На їхніх стартових сторінках розмістили банер з емблемою ВО «Свобода» і зображенням С. Бандери, Р. Шухевича і О. Тягнибока. Подаємо текст банера мовою оригіналу: «Ми прийшли назавжди! Нам не потрібна Конституція 2004 року! Далі ми підемо без Кличка і Яценюка! Ми підемо до кінця! Слава Україні! Героям слава! Смерть ворогам!» [12]. Автор не має певності, що це здійснили «націоналістично налаштовані» представники Західної України, але наголошує на тому, що внутрішньополітичні суперечності виявляють себе і у вітчизняному футболі.

Вдень 27 червня 2017 р. Україна пережила наймасштабнішу кібератаку у своїй історії. Унаслідок вірусу Petya. А постраждало багато великих компаній. Серед них сайти двох ФК: «Шахтар» (Донецьк), «Дніпро» (Дніпропетровськ). Перший швидко відновив свою роботу, другий – було заблоковано, сторінку звітано як нападницьку, тобто таку, яка може викрасти конфіденційну інформацію та пошкодити комп'ютерну систему [13]. 5 червня 2022 р. під час фіналу плей-офф відбору чемпіонату світу-2022 Уельс – Україна виникли проблеми з трансляцією матчу. На сервісі Oll.tv хакери підмінили його кадрами з російського пропагандистського каналу «Известия». Він транслював інтерв'ю президента РФ В. Путіна та сюжет про нібито обстріли Донецька українськими військовими. Згідно повідомлення Центру протидії дезінформації РНБО, місто обстрілювали окупаційні війська. Хакери були в ефірі майже 10 хв. Кіберзлочинці отримали доступ до мережі, що відповідає за доставку контенту – Content Delivery Network, – та перенаправили трафік на пропагандистський російський канал. Виявивши втручання у систему, компанія тимчасово відключила сервіс та перенаправила трансляцію на свій YouTube-канал «Футбол News». Росіяни атакували інші українські телеканали, в ефірі багатьох із них почали з'явилась картинка пропагандистських ЗМІ. На думку експертів, це вказувало на кіберзлочинців, яких контролюють російські спецслужби.

Адже хактивісти, як правило, хизуються своїми атаками, а інформації про цей злам у відомих групах не було [14]. Окрім фейкової трансляції, тут є очевидний спортивно-політичний підтекст: збірну Росії у зв'язку з агресією проти України відсторонили від футбольних змагань під егідою УЄФА та ФІФА, тому вона не брала участі у ЧС-2022 у Катарі. Натомість, українська збірна вийшла у раунд плей-офф, який наші гравці мали зіграти у березні. Але у зв'язку із війною Росії проти України, матч України проти Шотландії перенесли на 1 червня. У фіналі кваліфікації за путівку на ЧС-2022 Україна зустрічалася з Уельсом.

У лютому 2023 р. хакерської атаки зазнав офіційний сайт «Мінаю». Футболісти ужгородського клубу напередодні в турецькому готелі побилися з гравцями російського «Шинника» (Ярославль). «Причиною сутички була ганебна поведінка футболістів російської команди стосовно працівниці готелю та провокаційні вигукі у бік закарпатців», – йшлося у повідомленні пресслужби. Клуб також спростував інформацію-фейк російських ЗМІ, що нібито українські футболісти змушували росіян співати гімн України та побили гравця у ліфті [15]. На офіційній сторінці «Міная» у соціальних мережах після цього з'явилось повідомлення: «Наші хлопці зламали вашим ребра, а ви нам – сайт? Які ж ви жалюгідні!» [16].

8 липня 2023 р. хакери атакували офіційний сайт ФК «Динамо» (Київ). Для відновлення доступу клубу знадобилося 10 хв. [17]. Цього дня «Динамо» зробило заяву щодо рішення турецького «Фенербахче» брати участь у товариському турнірі в російському Санкт-Петербурзі за участю місцевого ФК «Зеніт»: «Жодні гроші не компенсують вам цю ганебну поведінку, цю поїздку до вбивць без моралі та людських якостей [...] Ми не боїмося сказати на весь світ: ви допомагаєте вбивцям продовжувати криваві жнива на українській землі. Ви підіграєте їм та легітимізуєте головне зло 21 ст.» [18].

Отже, приводом для хакерських атак на українські футбольні клуби була їхня

чітка державницька позиція, відстоювання національних інтересів України. При цьому напади здійснювали на сайти футбольних клубів, трансляцію їхніх матчів, поширюючи нарativi «русского мира».

Висновки. Футбольні клуби постійно посилюють свої системи захисту від несанкціонованого втручання. Незважаючи на це, кіберзлочинці з інформаційних баз даних футбольних клубів, спортивних організацій викрадають особисту інформацію про спортсменів, їхні медичні дані, публікують у вільному доступі корпоративну інформацію, вчиняють дії, спрямовані на завдання репутаційних втрат гравцям та керівництву клубів. Зловмисники також виводять з ладу сис-

теми, необхідні для забезпечення проведення матчів на стадіонах, системи функціонування міст, у яких вони відбуваються. Значну кількість атак на відомі футбольні клуби країн світу здійснюють хакерські групи, які пов'язані із Головним управлінням розвідки Росії. При цьому вони поширюють фейки, ідеологію «русского мира». Атаки на футбольні клуби можуть бути поодинокими або частиною більш масштабних операцій, як це трапилось з поширенням вірусу Petya.A в Україні. Якщо в Європі від атак хакерів страждають передусім топ-клуби, то в умовах збройного вторгнення РФ на територію України, починаючи із 2014 р., під загрозою опинились вітчизняні футбольні клуби різних ліг.

ЛІТЕРАТУРА:

1. Столяров А. Сергей Купцов: Хакерские атаки на стадионы ЧМ по футболу шли из Европы. URL: https://www.cnews.ru/reviews/security2018/interviews/sergej_kuptsov (дата звернення: 12.08.2023).
2. Літвінчук Т. «Незграбні аматори». Як російські розвідники здійснювали кібератаки по всьому світу і що про них відомо. URL: <https://gordonua.com/ukr/publications/-nezgrabni-amatori-jak-rosijski-rozvidniki-zdijsnjuvali-kiberataki-po-vsomu-svitu-i-shcho-pro-nih-vidomo-402070.html> (дата звернення: 12.08.2023).
3. Президент футбольного клубу «Барселона» об'явив о своей отставке после обвинений в коррупции. URL: <https://polit.ru/news/2020/10/28/bartomeu/> (дата звернення: 14.08.2023).
4. Мороз Є. «Швеція звинуватила Росію в кібератаці на місцеву конфедерацію спорту. Що трапилось». URL: <https://suspilne.media/122039-svecia-zvinuvatila-rosiu-v-hakerskij-ataci-na-federaciju-sportu-so-trapilosa-ta-aki-naslidki/> (дата звернення: 16.08.2023).
5. Пашинська А. Нова кібератака на Україну: що таке вірус VPNFilter і як з ним боротися. URL: https://espreso.tv/article/2018/05/29/nova_kiberataka_na_ukrayinu_scho_take_virus_vpnfilter_i_yak_z_nym_borotysya (дата звернення: 15.08.2023).
6. Аросев Г. Спецслужбы США рекомендуют любителям футбола не брать в Россию гаджеты. URL: <https://www.dw.com/ru/%D1%81%D0%BF%D0%B5%D1%86%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D1%8B-%D1%81%D1%88%D0%B0-%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D1%83%D1%8E%D1%82-%D0%BB%D1%8E%D0%B1%D0%B8%D1%82%D0%B5%D0%BB%D1%8F%D0%BC-%D1%84%D1%83%D1%82%D0%B1%D0%BE%D0%BB%D0%B0-%D0%BD%D0%B5-%D0%B1%D1%80%D0%B0%D1%82%D1%8C-%D0%B2-%D1%80%D0%BE%D1%81%D1%81%D0%B8%D1%8E-%D0%B3%D0%B0%D0%B4%D0%B6%D0%B5%D1%82%D1%8B/a-44192908> (дата звернення: 16.08.2023).
7. "Sun: эксперты заподозрили российский или китайский след в кибератаке на «Манчестер Юнайтед»». URL: <https://russian.rt.com/inotv/2020-11-22/Sun-eksperti-zapodozrili-rossijskij-ili> (дата звернення: 17.08.2023).
8. Чекабаев А. «Мощная кибератака на «МЮ»: хакеры шантажируют, а государство грозит штрафом до 18 млн за слив данных о фанатах». URL: <https://www.sports.ru/tribuna/blogs/greatness/2860573.html> (дата звернення: 18.08.2023).
9. Губенко Д., Мильников П. Посла Росії викликали до МЗС Швеції через кібератаки. URL: [http://dw.com/uk/%D0%BF%D0%BE%D1%81%D0%BB%D0%B0-%D1%80%D0%BE%D1%81%D1%96%D1%97-%D0%B2%D0%B8%D0%BA%D0%BB%D0%B8%D0%BA%D0%B0%D0%BB%D0%B8-%D0%B4%D0%BE-%D0%BC%D0%B7%D1%81-%D1%88%D0%B2%D0%B5%D1%86%D1%96%D1%97-%D1%87%D0%B5%D1%80%D0%B5%D0%B7](http://dw.com/uk/%D0%BF%D0%BE%D1%81%D0%BB%D0%B0-%D1%80%D0%BE%D1%81%D1%96%D1%97-%D0%B2%D0%B8%D0%BA%D0%BB%D0%B8%D0%BA%D0%B0%D0%BB%D0%B8-%D0%B4%D0%BE-%D0%BC%D0%B7%D1%81-%D1%88%D0%B2%D0%B5%D1%86%D1%96%D1%97-%D1%87%D0%B5%D1%80%D0%B5%D0%B7-%D1%80%D0%B5%D0%B7)

%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8/a-57192371 (дата звернення: 17.08.2023).

10. Рої дронів, хакерське отруєння води і кібератаки на урядові установи: як протистояти новим загрозам. URL: <https://www.radiosvoboda.org/a/viina-droniv-kiberzagrozyzahyst/31094308.html> (дата звернення: 11.08.2023).

11. Швеція звинувачує Росію в кібератаках на федерацію спорту. URL: <https://www.pravda.com.ua/news/2021/04/14/7290103/> (дата звернення: 12.08.2023).

12. Сайти футбольних клубів зі Сходу України «закрилися» через хакерську атаку. URL: https://lb.ua/sport/2014/01/31/253946_bandera_shuhevich_tyagnibok.html (дата звернення: 12.08.2023).

13. Хакерські атаки: Шахтар ненадовго постраждав, сайт Дніпра заблоковано. URL: https://football24.ua/hakerski_ataki_shahtar_nenadovgo_postrazhdav_vid_virusu_sayt_dnipra_zablokovano_n392363/ (дата звернення: 18.08.2023).

14. Антонюк Д. «Горить у пеклі». Хакери замінили на Oll.tv трансляцію футболу на російську пропаганду. Чи серйозна це атака і які збитки може принести компанії Ахметова. URL: <https://forbes.ua/innovations/gorit-v-pekli-khakeri-zaminili-na-olltv-translyatsiyu-futbolu-na-rosiysku-propagandu-chi-seryozna-tse-ataka-06062022-6436> (дата звернення: 15.08.2023).

15. Некрасов А. Бійка з російськими футболістами: у «Мінаї» зробили офіційну заяву. URL: <https://www.stopcor.org/ukr/section-suspilstvo/news-bijka-z-rosijskimi-futbolistami-u-minai-zrobili-ofitsijnu-zayavu-15-02-2023.html> (дата звернення: 16.08.2023).

16. Клубний сайт «Міная» піддався російській кібератаці. URL: <https://terrikon.com/uk/posts/429395> (дата звернення: 17.08.2023).

17. Хакери атакували офіційний сайт «Динамо». Клубу знадобилося 10 хвилин для відновлення доступу. URL: <https://ua.tribuna.com/uk/football/1000000079612-hakery-atakovali-oficialnyj-sajt-dinamo/> (дата звернення: 15.08.2023).

18. «Клуб без совісті та честі». Динамо засудило поїздки Фенербахче до росії. URL: <https://sport.ua/uk/news/633161-klub-bez-sovisti-ta-chesti-dinamo-zasudilo-poizdku-fenerbahche-do-rosii> (дата звернення: 18.08.2023).

REFERENCES:

1. Stoljarov A. Sergej Kupcov: Hakerskie ataki na stadiony ChM po futbolu shli iz Evropy. URL: https://www.cnews.ru/reviews/security2018/interviews/sergej_kuptsov (data zvernennja: 12.08.2023).

2. Litvinchuk T. "Nezgrabni amatory". Yak rosiiski rozvidnyky zdiisniuvaly kiberataky po vsomu svitu i shcho pro nykh vidomo. URL: <https://gordonua.com/ukr/publications/-nezgrabni-amatori-jak-rosijski-rozvidniki-zdijsnjuvali-kiberataky-po-vsomu-svitu-i-shcho-pro-nih-vidomo-402070.html> (data zvernennia: 12.08.2023).

3. Prezident futbol'nogo kluba "Barselona" ob"javil o svoej otstavke posle obvinenij v korrupciiju. URL: <https://polit.ru/nevs/2020/10/28/bartomeu/> (data zvernennja: 14.08.2023).

4. Moroz Ye. "Shvetsiia zvynuvatyla Rosiiu v kiberatatsi na mistsevu konfederatsiiu sportu. Shcho trapylosia". URL: <https://suspilne.media/122039-svecia-zvynuvatyla-rosiu-v-hakerskij-ataci-na-federaciju-sportu-so-trapilosa-ta-aki-naslidki/> (data zvernennia: 16.08.2023).

5. Pashynska A. Nova kiberataka na Ukrainu: shcho take virus VPNFilter i yak z nym borotysia. URL: https://espresso.tv/article/2018/05/29/nova_kiberataka_na_ukrayinu_scho_take_virus_vpfilter_i_yak_z_nym_borotysya (data zvernennia: 15.08.2023).

6. Arosev G. Specscluzhby SShA rekomendujut ljubiteljam futbola ne brat' v Rossiju gadzhety. URL: <https://www.dw.com/ru/%D1%81%D0%BF%D0%B5%D1%86%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D1%8B-%D1%81%D1%88%D0%B0-%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D1%83%D1%8E%D1%82-%D0%BB%D1%8E%D0%B1%D0%B8%D1%82%D0%B5%D0%BB%D1%8F%D0%BC-%D1%84%D1%83%D1%82%D0%B1%D0%BE%D0%BB%D0%B0-%D0%BD%D0%B5-%D0%B1%D1%80%D0%B0%D1%82%D1%8C-%D0%B2-%D1%80%D0%BE%D1%81%D1%81%D0%B8%D1%8E-%D0%B3%D0%B0%D0%B4%D0%B6%D0%B5%D1%82%D1%8B/a-44192908>. (data zvernennja: 16.08.2023).

7. "Sun: jeksperty zapodozrili rossijskij ili kitajskij sled v kiberatke na "Manchester Junajted"». URL: <https://russian.rt.com/inotv/2020-11-22/Sun-eksperti-zapodozrili-rossijskij-ili> (data zvernennja: 17.08.2023).

8. Chekabaev A. "Moshhnaja kiberataka na "MJu": hakery shantazhirujut, a gosudarstvo grozit shtrafom do 18 mln za sliv dannyh o fanatah". URL: <https://www.sports.ru/tribuna/blogs/greatness/2860573.html> (data zvernennja: 18.08.2023).

9. Hubenko D., Mylnikov P. Posla Rosii vyklykaly do MZS Shvetsii cherez kiberataky. URL: <http://dw.com/uk/%D0%BF%D0%BE%D1%81%D0%BB%D0%B0-%D1%80%D0%BE%D1%81%D1%96%D1%97-%D0%B2%D0%B8%D0%BA%D0%BB%D0%B8%D0%BA%D0%B0%D0%BB%D0%B8-%D0%B4%D0%BE-%D0%BC%D0%B7%D1%81-%D1%88%D0%B2%D0%B5%D1%86%D1%96%D1%97-%D1%87%D0%B5%D1%80%D0%B5%D0%B7-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8/a-57192371> (data zvernennia: 17.08.2023).

10. Roi droniv, khakerske otruiennia vody i kiberataky na uriadovi ustanovy: yak protystoiaty novym zahrozam. URL: <https://www.radiosvoboda.org/a/viina-droniv-kiberzagrozy-zahyst/31094308.html> (data zvernennia: 11.08.2023).

11. Shvetsiia zvyuvachuie Rosiiu v kiberatakakh na federatsiiu sportu. URL: <https://www.pravda.com.ua/news/2021/04/14/7290103/> (data zvernennia: 12.08.2023).

12. Saity futbolnykh klubiv zi Skhodu Ukrainy "zakrylysia" cherez khakersku ataku. URL: https://lb.ua/sport/2014/01/31/253946_bandera_shuhevich_tyagnibok.html (data zvernennia: 12.08.2023).

13. Khakerski ataky: Shakhtar nenadovho postrazhdav, sait Dnipra zablokovano. URL: https://football24.ua/hakerski_ataki_shahtar_nenadovgo_postrazhdav_vid_virusu_sayt_dnipra_zablokovano_n392363/ (data zvernennia: 18.08.2023).

14. Antoniuk D. "Horit u pekli". Khakery zaminily na Oll.tv translyatsiiu futbolu na rosiisku propahandu. Chy seriozna tse ataka i yaki zbytky mozhe prynesty kompanii Akhmetova. URL: <https://forbes.ua/innovations/gorit-v-pekli-khakeri-zaminili-na-olltv-translyatsiyu-futbolu-na-rosiysku-propagandu-chi-seryozna-tse-ataka-06062022-6436> (data zvernennia: 15.08.2023).

15. Nekrasov A. Biika z rosiiskymy futbolistamy: u "Mynai" zrobyly ofitsiinu zaiavu. URL: <https://www.stopcor.org/ukr/section-suspilstvo/news-bijka-z-rosijskimi-futbolistami-u-minai-zrobili-ofitsijnu-zayavu-15-02-2023.html> (data zvernennia: 16.08.2023).

16. Klubnyi sait "Minaia" piddavsia rosiiskii kiberatatsi. URL: <https://terrikon.com/uk/posts/429395> (data zvernennia: 17.08.2023).

17. Khakery atakuvaly ofitsiinyi sait "Dynamo". Klubu znadobylosia 10 khvylyn dlia vidnovlennia dostupu. URL: <https://ua.tribuna.com/uk/football/1000000079612-xakery-atakovali-oficijnyj-sajt-dinamo/> (data zvernennia: 15.08.2023).

18. "Klub bez sovisti ta chesti". Dynamo zasudylo poizdku Fenerbahche do rosii. URL: <https://sport.ua/uk/news/633161-klub-bez-sovisti-ta-chesti-dynamo-zasudilo-poizdku-fenerbahche-do-rosii> (data zvernennia: 18.08.2023).