8. Пігош В. А. Аналіз та прогнозування діяльності вищих навчальних закладів за допомогою методів інтерполяції та екстраполяції. *Актуальні проблеми економіки.* 2014. № 2. С. 529–538. URL: http://nbuv.gov.ua/UJRN/ape_2014_2_63

9. Бабій Ю. О., Нездоровін В. П., Махрова Є. Г., Луцкова Л. П. Хмарні обчислення проти розподілених обчислень: сучасні перспективи. *Вісник Хмельницького національного університету.* 2011. № 6. С. 80–85. URL: http://dspace.bsmu.edu.ua:8080/xmlui/bitstream/handle/123456789/3067/Makhrova_KhMARNI %20OBChYSLENN.pdf?sequence=1&isAllowed=y

10. Skafi M., Yunis M., Zekri A. Factors Influencing SMEs' Adoption of Cloud Computing Services in Lebanon: An Empirical Analysis Using TOE and Contextual Theory. *IEEE Access.* 2017. Vol. XX. URL: https://www.researchgate.net/ publication/340625422_Factors_Influencing_SMEs'_Adoption_of_Cloud_Computing_Services_in_Lebanon_An_Empirical_Analysis_Using_TOE_and_Contextual_Theory/fulltext/5e95c206299bf1307997ba38/Factors-Influencing-SMEs-Adoption-of-Cloud-Computing-Services-in-Lebanon-An-Empirical-Analysis-Using-TOE-and-Contextual-Theory.pdf

УДК 004.72.056.52:316.42

ХАКЕРСТВО ЯК ФЕНОМЕН ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

А. В. Даценко, Т. М. Яворська

Анотація. У дослідженні подана інформація про роль хакерства як складного соціального явища інформаційного суспільства, його історія. Методологічною основою роботи є системний підхід, принцип наукової об'єктивності, критичного та структурно-системного підходу до літературної та джерельної бази роботи. Специфіка досліджуваної теми передбачає застосування прикладів впровадження порівняльного та дискусійного методу, який дає можливість розглянути це поняття з різних сторін.

Ключові слова: інформаційне суспільство, хакерство, хакерська етика, кібертероризм.

Досліджувана тема є доволі актуальною у сучасному світі, оскільки розвиток інформаційно-комунікаційних, цифрових технологій, формування цифрового суспільства спричинили появу феномену хакерства. Хакерство як явище інформаційного суспільства стало однією з провідних тем у суспільстві, у світових засобах масової інформації ще з кінця XX століття. У сучасному світі ця тема приваблює багатьох підлітків, які починають свій шлях у вивченні інформаційних технологій, адже сам термін «хакер», на думку багатьох, ототожнюється з інтелектуальною, висококваліфікованою людиною, що має неоднотипне світосприйняття. Також хакерами все частіше почали називати програмістів, які блискуче орієнтуються в інформаційних технологіях, тобто у відповідній їм сфері діяльності, професії.

Піку популяризації хакерство набуло на початку XXI століття. З цим пов'язано створення у 2003 році міжнародної мережі кіберактивістів та хактивістів – Anonymous. Саме до цього угруповання хотіли долучитися тисячі підлітків, і саме воно дало поштовх для більшої зацікавленості молоді у цій сфері.

Anonymous – колективна назва, під якою діють різні групи та індивіди, що виконують різноманітні дії в інтернеті або в публічних просторах, зазвичай залишаючи свою особистість прихованою або невідомою. Ця група вирізнялася своєю активною участю в різних анонімних операціях та протестах, часто брала участь у різноманітних гібридних акціях, кібератаках та викриттях корупції у владних структурах.

Тож угрупування Anonymous має на меті високі цілі щодо боротьби з негативними суспільними явищами, що проявляються на міжнародному рівні. Зазначимо, що останнім часом поширене так зване патріотичне хакерство, що здійснює багато атак протягом останнього десятиліття в усьому світі в періоди підвищеної напруги чи конфліктів. Доказом є кібератаки цього угруповання, спрямовані на РФ. Так, на початку повномасштабної російсько-української війни угруповання Anonymous стало на бік українців. Із 26 лютого 2022 року було викладено в інформаційний простір сотні гігабайтів конфіденційних даних російського уряду, були зламані російські державні сервіси, що показують телеканали, було передано багато важливої стратегічної, військової інформації у загальний доступ українським відповідним службам [1].

Загалом поняття «хакерство» та його розвиток умовно можна поділити на «добре» та «зле» хакерство [2]. З одного боку, хакер – висококваліфікований фахівець, метаю якого – зосеред-

женість на активізації, розвитку знань, неоднотипного, різностороннього мислення, а з іншого хакер – злочинець в інформаційному інтернет-просторі, мета такого хакера – зламування чужих комп'ютерів, здійснення крадіжок у мережі Інтернет. Питання хакерства залишається доволі дискусійним неоднозначним, але все ж таки, заглиблюючись в історію, можна зробити висновок, що таке спірне та багатогранне поняття містить у собі більше добрих, світлих і справедливих вчинків щодо негативних суспільних явищ.

Розглядаючи хакерство як складне соціальне явище, можна виділити кілька ключових аспектів:

1. Культура та хакерська спільнота. Хакерська спільнота почала свій шлях як невеликий сектор в інформаційній та комп'ютерній культурі. Вона має унікальну ідеологію і відрізняється від стереотипних понять у цих сферах. Відповідно хакерську спільноту можна розглядати як з негативного боку (незаконного), так і з позитивного (інтелектуальний капітал певної країни) [3].

2. Мотивація. Хакери можуть бути мотивовані різними чинниками, як-от соціальна справедливість, прибуткове зловмисництво або політичні переконання. Ця мотивація впливає на їхні подальші цілі та дії.

3. Етика та закон. Хакерство викликає відповідні дискусії у суспільстві про етичність та законність. Деякі хакери вважають свої дії морально обґрунтованими, тоді як інші порушують закон.

4. Безпека та загрози. Хакерство може становити серйозну кіберзагрозу для інформаційної безпеки, економіки та громадського порядку.

5. Реакція суспільства та влади. Уряди та компанії реагують на хакерство шляхом удосконалення кіберзахисту та прийняття законодавства, яке регулює цю діяльність.

Класифікація хакерства:

1. Ламер.
2. Просунутий ламер.
3. Хакер-новачок.
4. Хакер-любитель.
5. Хакер [4].

Головне завдання будь-якого хакерства («злого» чи «доброго») – прозорість інформації, невичерпна свобода інформації для її аналізу та реалізації в ній індивідуальної особи, неординарний підхід у розв'язанні будь-якої проблеми, задачі, підтримка і захист своїх колег, надання їм будь-яких інформаційних ресурсів, спрямованість на працездатність світових мереж.

Хакерська етика – поняття, згідно з яким хакер зобов'язаний ділитися своїми знаннями, досвідом з іншими колегами [5]. Цей термін найбільше з усіх демонструє філософію та ідеологію головного завдання хакерства та зображає їхній відповідний стандарт відносин.

Можна охарактеризувати ідеологію хакерської етики:

1. Доступ до технологічних ресурсів повинен бути необмеженим.
2. Уся шукана інформація зобов'язана бути безкоштовною.
3. Боротьба за децентралізацію. Влада – це зло.
4. Хакерство – це своєрідне мистецтво.
5. Інформаційні технології можуть змінити життя на краще.

Хакерство також можна розглядати і погляду психологічного впливу. Психологи, які вивчають цю тему, стверджують, що більшість хакерів мають надзвичайно високий рівень інтелекту, і високоінтелектуальні здібності, необхідні хакерам, щоб успішно виконувати свою роботу. Як уже було сказано, мотивація дуже важлива. У цьому випадку це бажання бути найкращим хакером, завойовувати, домінувати, демонструвати свої можливості та потенціал. Для хакерів найважливішим у роботі є безперервне отримання відповідних знань, постійне професійне зростання, набуття нових знань у цій сфері та процес самовдосконалення. Одним з найважливіших психологічних аспектів хакерів є нездатність зрозуміти наслідки деяких своїх дій. Проблема в тому, що незважаючи на високий рівень інтелекту, інколи хакери навіть не можуть уявити наслідки своєї незаконної роботи.

Соціальний хакер – це той, хто володіє інформацією про те, як «зламувати інших» і вміло використовує ці знання у своїй діяльності.

Активний розвиток інформаційних технологій наприкінці XX – початку XXI століття привів до появи понять кібертероризму та хактивізму. Кібертероризм є потужним засобом політичної боротьби всередині окремої країни, або на міжнародному рівні. Кібертероризм – форма маніпулятивного впливу на суспільну свідомість [6].

Хактивізм – це поєднання соціальної активності та хакерства, тобто використання комп'ютерів і комп'ютерних мереж для просування політичної думки, свободи слова, захисту прав людини та забезпечення свободи інформації [7].

Злом – це використання спеціального програмного забезпечення для використання комп'ютерів у складний і часто незаконний спосіб.

За десятиліття хакерство перетворилося на форму соціального протесту та відходу від реального світу у світ кіберпростору. Важливо зазначити, що останніми роками кібертероризм поширився. У сучасному світі в деяких країнах хакерство вважається одним із головних джерел технологічних інновацій. Прикладом може слугувати Фінляндія та США. Під час будівництва глобальних хакерських мереж фінські хакери домоглися визнання та встановлення зв'язку з університетами і бізнесами, які зосереджуються переважно на вивченні інформаційних технологій, особливо якщо це програмування [8]. Отже, хакерство – це складне соціальне явище, яке має позитивні та негативні аспекти.

Позитивні сторони:

1. Кібербезпека: етичні хакери (тобто ті, хто займається безпекою) можуть допомогти виявити та виправити вразливості у програмному забезпеченні та мережах, забезпечуючи кращу кібербезпеку.

2. Свобода інформації. Деякі хакери працюють над проєктами, спрямованими на розкриття конфіденційної інформації, яка може виявити корупцію чи недоліки уряду.

3. Творчість та інновації: хакери можуть просувати нові технології та інновації, особливо у сферах вільного програмного забезпечення та відкритого коду.

Негативні сторони:

1. Кіберзлочинність: негативна хакерська діяльність може призвести до кіберзлочинів, якот крадіжка особистих даних, шахрайство, кібератаки тощо.

2. Вторгнення в конфіденційність: деякі хакери можуть вторгатися в особисту інформацію та конфіденційність користувачів.

3. Правові наслідки: більшість хакерських дій є незаконними та можуть мати серйозні правові наслідки.

Значимість хаку залежить від контексту та мотивації його використання. Це може бути корисно, якщо метою злому є покращення безпеки мережі, викриття корупції чи стимулювання інновацій. Але незаконний злом, спрямований на шкоду іншим, завжди є негативним. Нині цінності хакерів викликають велике занепокоєння, оскільки вони є важливим фактором у соціальному середовищі. Подальша ізоляція хакерів є реальною перспективою. Існує величезна цінність у тому, щоб передати свою спадщину (знання та досвід) наступному поколінню. Якщо глобально розглядати цю тему, то у сучасному світі країни, що пригнічують і не сприймають хакерів, чим, можливо, відсікають від себе одне з основних джерел інтелектуального капіталу держави.

Abstract. This study provides information on the role of hacking as a complex social phenomenon of the information society, its history. The methodological basis of the work is a systematic approach, the principle of scientific objectivity, a critical and structural-systemic approach to the literary and source base of the work. The specificity of the researched topic involves the use of examples of the implementation of the comparative and discussion method, which makes it possible to consider this concept from different angles.

Keywords: information society, hacking, hacking ethics, cyber terrorism.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Некрасов В. Втрати окупантів на кіберфронті: як Anonymous веде війну проти росіян і що це дає. *Економічна правда.* URL: https://www.epravda.com.ua/publications/2022/04/7/685362/ (дата звернення 01.10.2023).

2. Баранюк К. Хто насправді стоїть за багатьма хакерськими нападами. *BBS NEWS Україна.* URL: https://www.bbc.com/ukrainian/vert-fut-40776711.amp (дата звернення 01.10.2023).

3. Хакери – хто вони? *Портал освітньо-інформаційних послуг «Студентська консультація».* URL: http://studcon.org/hakery-hto-vony (дата звернення 06.10.2023).
4. Єсіна О. Г., Варналій А. О. Хакерство як соціальне явище. *Інформатика та інформаційні технології:* студ. наук. конф., 20 квітня 2015 р.: матер. конф. Одеса: ОНЕУ, 2015. С. 107–110.
5. Що таке хакерська етика? *Визначення з техопедії.* URL: https://uk.theastrologypage.com/hacker-ethic
6. Грінік Р. О., Пилипенко В. М. Кібертероризм як нова форма міжнародного тероризму. *Науковий блог Львівського державного університету безпеки життєдіяльності.* URL: https://sci.ldubgd.edu.ua/bitstream/123456789/3203/1/13.pdf (дата звернення 09.10.2023).
7. Що таке хактивізм? *Фінансова енциклопедія.* URL: https://ua.nesrakonk.ru/hacktivism (дата звернення 10.10.2023).
8. Фінська модель розвитку інформаційного суспільства. *Розвиток інформаційного суспільства.* URL: http://elbib.in.ua/finska-model-informatsiynogo-suspilstva-rozvitok-informatsiynogo-suspilstva.html (дата звернення 10.10.2023).
9. Трансформаційні процеси у суспільній та соціокультурній сферах України / О. М. Анісімова, Л. А. Ковальська, Г. П. Лукаш, О. В. Прігунов, О. С. Щербіна, Т. М. Яворська. Вінниця: ДонНУ імені Василя Стуса, 2021. 176 с.

УДК 004.056.53

БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ У БАЗАХ ДАНИХ

І. С. Діброва, Т. В. Січко

Анотація. Дослідження зосереджено на аспектах забезпечення інформаційної безпеки в організаційному середовищі. Пояснюється, наскільки важливо розуміти загрози та вразливості для ефективного захисту інформаційних активів. Також проаналізовано важливі принципи доступності інформаційних ресурсів, як-от: політика безпеки та надійний захист, безперебійна робота систем і послуг. До того ж вказано важливість дотримання низки правил, стандартів, законів і рекомендацій для ефективного управління ризиками та підвищення рівня кібербезпеки.

Ключові слова: захист баз даних, екосистема баз даних, кібербезпека, кіберзлочинність, ризики, аутентифікація, авторизація.

Безпека бази даних має важливе значення для запобігання доступу, зміні або знищенню секретних даних організації. Бази даних містять важливу інформацію, як-от дані про клієнтів, фінансову інформацію та інтелектуальну власність. Усі ці дані є цінними цілями для хакерів і злочинців. Отже, підтримка надійної системи безпеки бази даних має вирішальне значення для підтримки точності даних, дотримання правил захисту даних та завоювання довіри клієнтів і зацікавлених сторін.

Дані – це цінний корпоративний актив для будь якого підприємства. База даних – це організований набір даних, до якого можна отримати доступ, вивчити та реалізувати за допомогою СКБД (системи керування базами даних). Бази даних необхідно захищати та регулярно оцінювати ефективність цього захисту. За допомогою спеціальних методів і програм можна запобігти несанкціонованому доступу до бази даних у локальних мережах або оприлюдненню інформації, не призначеної для широкого загалу [1, 4].

Жодна організація, корпорація чи держава не може уникнути використання інформаційної системи (клієнти, препарати, правила, продукти, фінансові звіти). Ці масиви майже завжди складаються з особистої, інституційної та конфіденційної інформації. Їх втрата може мати серйозні наслідки – як фінансові, так і народні.

Два основні фактори спонукають компанії та державні установи виділяти все більше ресурсів на захист баз даних.

Перший і найважливіший – це кіберзлочинність. Постійна еволюція інструментів зловмисників, поява нових програм-вимагачів, розвиток безфайлових методів проникнення та постійна можливість вчинення дій, які створюють загрозу секретній інформації. Згідно зі звітом про витоки даних, лише у 2019 році було розкрито понад 9 мільярдів облікових записів з особистою інформацією. З огляду на розвиток кримінальних технологій, суттєву увагу слід приділяти заходам, що гарантують захист конфіденційної інформації. Важливим етапом є впровадження превентивних заходів, як-от налаштування брандмауера, який обмежує доступ до сумнівного