УДК 378.016-057.87 DOI: https://doi.org/10.32782/1995-0519.2022.1.10

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УНІВЕРСИТЕТАХ ПІД ЧАС ВІЙСЬКОВОГО СТАНУ

Сергій Близнюк
викладач кафедри математичного моделювання
ПВНЗ «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука», вул. академіка Степана Дем'янчука, 4, Рівне, Україна, 33024;
ORCID: 0000-0002-4363-3524

Олег Онофрійчук
кандидат економічних наук,
старший викладач кафедри економіки та фінансів
ПВНЗ «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука», вул. академіка Степана Дем'янчука, 4, Рівне, Україна, 33024;
ORCID: 0000-0001-6495-2973

Акцентовано увагу на трактуванні поняття «інформаційна безпека». Визначено потенційні загрози можливості швидкого обміну інформацією, здобуття нових знань за допомогою нових інформаційних технологій, розвитку соціальних та індивідуальних форм творчості. Наголошено, що в умовах прямої військової агресії з боку Російської Федерації, активне поширення державою-агресором дезінформації, викривлення відомостей, а також виправдовування або заперечення збройної агресії Російської Федерації проти України, впроваджено реалізацію єдиної інформаційної політики. Виокремлено проблеми інформаційної безпеки в сучасних українських університетах: пріоритезація безпеки для відповідності нормативним вимогам, інерція заважає університетам успішно вирішувати проблеми комп'ютерної безпеки, приховування проблем інформаційної безпеки від громадськості, демонстрація комплексної бюрократії рентабельності інвестицій, відсутність узгоджених стратегій. Відзначено, що для вирішення проблеми безпеки, університетам потрібні безпечні комунікаційні рішення. Вказано на важливість інформаційної безпеки в соціальних мережах – Instagram, Viber, Telegram. Виокремлено основні правила інформаційної безпеки в соціальних мережах. Зазначено як одну з ключових загроз інформаційної безпеки – студенти продовжують ділитися обліковими даними. Акцентовано увагу на необхідності запобігання одночасному входу, що робить користувачів відповідальними за будь-які незаконні дії, які вони вживають. Вказано, що викладачі, співробітники та студенти мають бути підключені до мережі по-різному. Відзначено, що комп'ютерне забезпечення повинно постійно відстежує всі події входу та сеанси, автоматично застосовуючи спеціальні політики. Зазначено проблему надання дозволу студентам і співробітникам використовувати свої власні пристрої, що збільшує шанси небезпечних інформаційних дій.

Ключові слова: військовий стан, вища освіта, пропаганда, електронна пошта, кодування, освітній простір.

АКТУАЛЬНІСТЬ ПРОБЛЕМИ ДОСЛІДЖЕННЯ. Деструктивні та дестабілізуючі інформаційні впливи загрожують насамперед вразливим елементам освітньої системи. У той же час цілеспрямовані та регулярні інформаційні атаки часто створюють середовище, сприятливе для поглинання, коли суб'єкти стають дезорієнтованими та безпорадними споживачами. Суспільство та кожен громадянин якої всі роки незалежності перебували під агресивним впливом різноманітних суб'єктів інформаційного простору, як внутрішнього, так і зовнішнього. Для України питання інформаційної безпеки стало особливо актуальним у зв'язку з г війною, яку веде Росія в останні роки. Іншою важливою причиною актуалізації питання інформаційної безпеки є те, що лише університети з розвиненою інформаційною інфраструктурою здатні стати конкурентоспроможним суб'єктом у сучасному міжнародному глобальному освітньому середовищі. У зв'язку з цим важливим аспектом дослідження різноманітних вимірів інформаційної безпеки є визначення рівня інформатизації освітнього простору українських університетів.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ. Незважаючи на значну кількість наукових досліджень, присвячених проблематиці забезпечення інформаційної безпеки в Україні, обрана проблематика є новою та потребує детального вивчення. При написанні статті були враховані напрацювання ряду науковців: Аносова А. О., Бржевської З. М., Гайдур Г. І., Довженко Н. М., Захаренко К. В., Золотар О. О..

Кальниш В. В., Киричока Р. В., Ліщинської О. А., Петрик В. М., Хворост Х. Ю.

МЕТА ДОСЛІДЖЕННЯ – проаналізувати особливості забезпечення інформаційної безпеки в університетах під час військового стану.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ. Категорія інформаційної безпеки розглядається як така, що має глобальний характер, а тому потребує аналізу в системі глобального інформаційного простору. Визначивши основні переваги та ризики інтенсифікації передачі та руху інформації в комунікаційному просторі та в умовах інформаційної революції, варто відзначити неможливість повноцінного використання нових переваг в інформаційному суспільстві без забезпечення належного рівня інформаційної безпеки [6].

Можливості швидкого обміну інформацією, здобуття нових знань за допомогою нових інформаційних технологій, розвитку соціальних та індивідуальних форм творчості на основі оперування великими обсягами інформації можуть нівелюватися через неналежне або злочинне використання нових технологій для навіювання, маніпулювання та інформаційного саботажу. Одним із ключових завдань сучасної науки є пошук адекватних шляхів глобального стійкого балансу між розвитком інформаційних технологій та вдосконаленням механізмів інформаційної безпеки. Саме глобальність інформаційної цивілізації, через яку люди та суспільство стикаються з додатковими викликами та загрозами інформаційній безпеці, змінює сучасні науково-практичні підходи до неї [2].

Враховуючи основні деструктивні зовнішні та внутрішні інформаційні впливи як основні джерела загострення інформаційної небезпеки, варто відзначити їх особливу гостроту. Сьогодні держава чи заклад вищої освіти не в змозі адекватно відповісти на виклики, які ставить перед собою глобальний інформаційний простір. Але якщо провідні держави зможуть зайняти активну позицію в цьому просторі, то такі трансформаційні суспільства в умовах військового стану, як Україна, автоматично стануть об'єктами інформаційної агресії.

В умовах військового часу та з врахуванням того, що формуються основи демократичної державності та громадянського суспільства, протистояти зовнішнім і внутрішнім деструктивним інформаційним впливам можна лише на основі досвіду та ресурсно-технологічної допомоги більш значущих суб'єктів сучасного інформаційного простору [4].

Ураховуючи пряму військову агресію з боку Російської Федерації, активне поширення державою-агресором дезінформації, викривлення відомостей, а також виправдовування або заперечення збройної агресії Російської Федерації проти України, з метою донесення правди про війну, забезпечення єдиної інформаційної політики в період дії в Україні правового режиму воєнного стану, установлено, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки [5].

Можна виокремити ряд проблем інформаційної безпеки в сучасних українських університетах [7]:

1. Приоритезація безпеки для відповідності нормативним вимогам. Університети – це складні організації, поділені на кілька корпорацій, кожна зі своїми власними вимогами законодавства та проблемами безпеки. Університет зобов'язаний захищати такі дані, як оцінки, результати тестів та інформацію про стан здоров'я.

2. Інерція заважає університетам успішно вирішувати проблеми комп'ютерної безпеки. Один із парадоксів усвідомлення кібербезпеки полягає в тому, що знання не обов'язково перетворюються на дії. Багато університетів усвідомлюють проблеми безпеки, з якими вони стикаються, і наслідки порушень, але відкладають це, оскільки проблеми здаються нездоланними. Кардинальна перебудова кібербезпеки не є швидким або недорогим процесом, і з усіма проблемами управління університетом може легко піддатися інерції.

Трагедія цього полягає в тому, що більшість університетів можуть легко покращити кібербезпеку за допомогою поступового підходу. Зміни з низькими інвестиціями, як-от запровадження безпечного рішення електронної пошти, дозволяють університетам майже миттєво знизити ризики з дуже незначними змінами та невеликою кількістю навчання. Ці основні зміни також дуже легко масштабувати. Просте запровадивши шифрування електронної пошти дозволить університету розпочати вирішувати проблеми безпеки організації в цілому.

3. Приховування проблем інформаційної безпеки від громадськості. Серйозне порушення може призвести до дорогих штрафів, планів виправлення та судових позовів. У разі серйозного порушення університет може витримати місяці або навіть роки негативних відгуків у ЗМІ [7].

Університети часто мають спокусу закрити свої проблеми безпеки від громадськості. Однак

це фактично робить порушення ще більшою шкодою для репутації закладу. Якщо є можливість продемонструвати, що університет вживає всі можливі заходи для захисту студентів, викладачів і співробітників, громадськість звинуватиме працівників, які спричинили порушення.

4. Демонстрація комплексної бюрократії рентабельності інвестицій. У міру того, як університети стають все більше схожими на бізнес, вони стикаються з все більшими проблемами безпеки, які властиві бізнес-структурам. Організації, як правило, ігнорують або недофінансують ініціативи з IT-безпеки, оскільки історично було важко повести конкретну, вимірну рентабельність інвестицій. При цьому неможливо точно дізнатися, коли зловмисний хакер або інсайдерська загроза зашкодять інформаційним базам, чи скільки шкоди вони завдадуть.

Варто відзначити позитивну тенденцію зростання кількості досліджень, які демонструють рентабельність інвестицій від вирішення проблем безпеки університету [7].

5. Відсутність узгоджених стратегій. В університеті кожен має власну думку. Як і в будь-якій організації, керівництво має свої власні погляди на речі, які можуть не відповідати IT-безпеці. Можуть обирати безпечні рішення для електронної пошти, які не відповідають потребам кінцевих користувачів, або, з іншого боку, обирати зручні додатки з недоліками безпеки, які вони не розуміють. Різні факультети також можуть мати різні пріоритети та наполегливо намагатися вибрати безпечні комунікаційні рішення.

Проблема в тому, що набагато важче протистояти проблемам безпеки без узгодженої стратегії в масштабі всієї організації – особливо для комунікаційних рішень, таких як безпечна електронна пошта та база даних. Відділи повинні мати можливість безпечно спілкуватися один з одним, а також з іншими зацікавленими сторонами – такими як студенти, батьки та підрядники – що вони не можуть зробити, якщо кожен має інший безпечний інструмент електронної пошти.

Крім того, багато рішень безпеки недостатньо зручні для повсякденного спілкування. Якщо співробітник фінансового відділу повинен зв'язатися зі студентом з питань оформлення необхідних документів чи проведення оплати за навчання, то в більшості випадків буде надіслано незашифрований електронний лист, ризикуючи безпекою.

Щоб вирішувати проблеми безпеки, університетам потрібні безпечні комунікаційні рішення, які є легкими, зручними та здатними встановлювати комунікаційні зв'язки з усіма зацікавленими сторонами – навіть з тими, хто не хоче встановлювати програму [1].

Інформаційна безпека в соціальних мережах – Instagram, Viber, Telegram активно обговорюється на тренінгах, які організують викладачі університетів для своїх колег та студентів. При цьому головний акцент здійснюється на забезпеченні конфіденційності та безпеки їхніх сторінок у соціальних мережах. Акцентовано увагу на месенджерах Viber, Telegram, які стали популярними для розгортання російської інформаційної пропаганди.

У цьому контексті необхідно звернути увагу учасників онлайн-тренінгу на основні правила інформаційної безпеки в соціальних мережах [3]:

– налаштувати конфіденційність;

– ділитися конфіденційною інформацією лише з тими, кому довіряєте;

– використовувати «зникаючі повідомлення»;

– нікому не надавати SMS-коди підтвердження;

– переглядати історію чатів і членство в групах;

– скаржитися на контакти, які здаються шахрайськими.

Досягнення балансу між відкритою, але безпечною мережею залишається проблемою для всіх IT-відділів університетів. Ці ускладнення призвели до деяких вражаючих порушень даних. Найкращий спосіб для університетів впоратися з такими мережевими порушеннями – це запровадити добре продуману систему контролю доступу до мережі та управління ідентифікацією.

Незважаючи на освіту та підвищену обізнаність, студенти продовжують ділитися обліковими даними, оскільки це не впливає на їхній власний доступ до мережі. Серйозні недоліки безпеки можна зупинити, запобігаючи одночасним заняттям і обмежуючи студентів лише одним можливим підключенням до Windows у кожному окремому випадку. Це зупиняє несанкціонованих користувачів безперешкодно використовувати дійсні облікові дані одночасно з законним власником [2].

Запобігання одночасному входу також робить законних користувачів відповідальними за будь-які незаконні дії, які вони вживають – чи то студентські витівки, чи більш серйозні інсайдерські атаки. Це забезпечує доступ до критичних активів установ, які приписуються одній особі, уникаючи ситуацій, що стосуються підзвітності

та невідмовності. Політики та процедури можна буде послідовно застосовувати для усунення порушень, які дійсно мають місце.

Викладачі, співробітники та студенти мають бути підключені до мережі по-різному, щоб рівень доступу відповідав ролі кожної людини в академічній установі. Крім того, приїжджі викладачі, викладачі та студенти мають бути забезпечені окремо, щоб гарантувати, що їх доступ буде припинено після їхнього від'їзду. Контроль входу користувачів відповідно до користувачів, груп користувачів або організаційних підрозділів є першою лінією захисту для мережі Windows, і права входу повинні (і можуть) надаватися залежно від ролі користувача в організації. Такі обмеження також мають враховувати інші критерії, такі як робоча станція або пристрій (включаючи персональні пристрої), час, години роботи та тип сеансу (включаючи Wi-Fi та VPN).

Наприклад, студент, який зумів отримати облікові дані викладача, зможе отримати доступ до конфіденційної інформації (екзаменаційні запитання, результати тощо) з будь-якої робочої станції в мережі. Однак є спеціалізовані IT сервіси (наприклад, UserLock), які зупинить зловживання обліковим записом, дозволивши адміністратору визначати для кожного користувача та групу користувачів робочі станції, які вони можуть або не можуть використовувати. Таким чином, студент не зможе увійти за допомогою облікових даних викладача з кімнати, обладнаної робочими станціями з вільним доступом [7].

Таким же чином можна обмежити доступ до адміністративних робочих місць (бухгалтерії, фінансів тощо) із визначених робочих місць або заздалегідь визначеного набору робочих місць (наприклад, у відділі бухгалтерії, конкретної будівлі тощо).

UserLock дозволяє впроваджувати та суворо застосовувати політику контролю доступу користувачів за допомогою входу користувачів. Є можливість контролювати, коли, де і як довго користувачі мають доступ до ресурсів.

Комп'ютерне забезпечення повинно постійно відстежує всі події входу та сеанси, автоматично застосовуючи спеціальні політики для запобігання або заборони входу, доступу до робочої станції та часу використання / підключення.

У разі виявлення ненормальної або підозрілої поведінки на робочій станції дозволить адміністратору віддалено відключити користувача або заблокувати сеанс із центральної консолі або будь-якого комп'ютера в мережі.

Дозволяючи студентам і співробітникам використовувати свої власні пристрої – і, отже, ненадійні пристрої – доступ до ресурсів організації перебуває в зоні небезпеки. Оскільки UserLock захищає доступ до мережі до всіх типів сеансів, включаючи Wi-Fi, це дозволяє організації контролювати свої бездротові мережі та забезпечує безпеку для використання власних пристроїв [9].

Веб-інтерфейс дозволяє делегувати адміністративні права не-IT-менеджменту (наприклад, викладачам, керівникам тощо) для підгрупи робочих станцій (наприклад, систем у кімнаті, поверсі, будівлі), що дозволяє здійснювати нагляд та керування (наприклад, закрити або розблокувати сеанс на робочих станціях).

Пропонуючи цей рівень адміністрування, програма надає обмежені права наглядача для не-IT-персоналу, який керує користувачами, не надаючи їм доступу до більш важливих налаштувань програмного забезпечення, зарезервованих для IT-адміністраторів.

Система сповіщень може допомогти надати чітке та послідовне повідомлення про політику безпеки IT. Чітке повідомлення про юридичні наслідки допомагає зменшити ймовірність того, що студенти ненавмисно вчинять злочин або накинуться на уявну несправедливість.

За допомогою такого програмного забезпечення деякі з потенційних сценаріїв, які тепер можна запобігти, включають:

– справжні, але скомпрометовані логіни від експлуатованих користувачів тепер марні для зловмисних інсайдерів або потенційних зловмисників;

– є можливість запобігти необережній поведінці користувачів, як-от обмін паролями, спільні робочі станції, залишені розблокованими або вхід на кілька комп'ютерів одночасно;

– доступ до будь-яких даних / ресурсів тепер завжди можна ідентифікувати та приписувати окремому користувачеві. Ця підзвітність відлякує інсайдерів від зловмисних дій і робить усіх користувачів більш обережними у своїх діях;

– підозріла активність позначається прапорцем і дає IT-відділам можливість миттєво відреагувати [8].

Користувачі можуть отримувати сповіщення за допомогою спеціально розроблених повідомлень і сповіщень, включаючи сповіщення про їхній власний довірений доступ. Інформовані співробітники – це ще одна лінія захисту у безпеці мереж університету.

ВИСНОВКИ. Освітнє середовище часто важче забезпечити інформаційну безпеку, ніж у звичайних компаніях чи організаціях. Традиційна культура освіти сприяє вільному обміну ідеями та миттєвому доступу до інформації, що сприяє академічній місії та цілям будь-якого університету. ІТ-команди повинні знайти відповідний спосіб збалансувати ці значення доступу, які визначають освіту, одночасно захищаючи дані та інформаційні системи.

ЛІТЕРАТУРА

1. Бржевська З. М., Довженко Н. М., Киричок Р. В., Гайдур Г. І., Аносов А. О. Інформаційні війни: проблеми, загрози та протидія. *Кібербезпека: освіта, наука, техніка.* 2019. № 3 (3). С. 88–96.

2. Захаренко К. В. Інституційний Вимір Інформаційної Безпеки України: Трансформаційні Виклики, Глобальні Контексти, Стратегічні орієнтири. Дис. Київ : Національний педагогічний університет імені М. П. Драгоманова, Львівський національний університет імені Івана Франка, 2021. 423 с.

3. Золотар О. О. Особливості інформаційної безпеки людини в умовах гібридної війни. *Інформація і право.* 2017. № 3 (22). С. 124–131.

4. Петрик В. М., Ліщинська О. А., Кальниш В. В. Соціально-правові основи інформаційної безпеки. Київ, 2006. 263 с.

5. Рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#Text

6. Хворост Х. Ю. Інформаційно-психологічний вплив у розрізі безпеки здоров'я. *Наука і освіта.* 2016. № 2–3. С. 184–191.

7. McDonald R. 5 Information Security Challenges All Universities Face. URL: https://www.virtru.com/blog/security-challenges/

8. Network security in Universities, Colleges and Schools. URL: https://www.isdecisions.com/blog/it-management/network-security-in-universities-colleges-and-schools/

9. Why is Information Security important? URL: https://www.plymouth.ac.uk/students-and-family/governance/information-governance/information-security

ENSURING OF THE INFORMATION SECURITY IN UNIVERSITIES DURING THE MARTIAL LAW

Serhii Blizniuk
Lecturer at the Department of Mathematical Modeling
Academician Stepan Demyanchuk International University of Economics and Humanities, 4 Academician Stepan Demianchuk str., Rivne, Ukraine, 33024;
ORCID: 0000-0002-4363-3524

Oleh Onofriychuk
PhD in Economics, Senior Lecturer at the Department of Economics and Finance
Academician Stepan Demyanchuk International University of Economics and Humanities, 4 Academician Stepan Demianchuk str., Rivne, Ukraine, 33024;
ORCID: 0000-0001-6495-2973

Emphasis is placed on the interpretation of the concept of "information security". Potential threats to the possibility of rapid exchange of information, acquisition of new knowledge through new information technologies, development of social and individual forms of creativity have been identified. It was emphasized that in the conditions of direct military aggression by the Russian Federation, active dissemination of disinformation by the aggressor state, distortion of information, as well as justification or denial of armed aggression of the Russian Federation against Ukraine, the unified information policy was implemented. The problems of information security in modern Ukrainian universities are highlighted. Among them are priority of security for compliance with regulatory requirements; inertia prevents universities from successfully solving computer security problems; hiding information security problems from the public; demonstration of complex bureaucracy of return on investment; and lack of agreed strategies. It is noted that to solve the problem of security, universities need secure communication solutions. The importance of information security in social networks – Instagram, Viber, Telegram, is emphasized. The basic rules of information security in social networks are highlighted. It is mentioned as one of the key threats to information security, that students continue to share credentials. Emphasis is placed on the need to prevent simultaneous sign-in, which makes users responsible for any illegal actions they take. It is stated that teachers, staff and students should be connected to the network in different ways. It is noted that computer software must constantly monitor all logon events and sessions, automatically applying special policies. The problem of allowing students and staff to use their own devices is mentioned as the one, which increases the chances of dangerous information actions.

Key words: martial law, higher education, propaganda, Email, coding, educational space.

REFERENCES

1. Brzhevska, Z. M., Dovzhenko, N. M., Kyrychok, R. V., Haidur, H. I., Anosov, A. O. (2019) Informatsiini viiny: problemy, zahrozy ta protydiia [Information wars: problems, threats and counteraction] *Kiberbezpeka: osvita, nauka, tekhnika.* Vol. 3 (3). P. 88–96. [in Ukrainian]

2. Zakharenko, K. V. (2021) Instytutsiinyi Vymir Informatsiinoi Bezpeky Ukrainy: Transformatsiini Vyklyky, Hlobalni Konteksty, Stratehichni oriientyry [nstitutional Dimension of Information Security of Ukraine: Transformational Challenges, Global Contexts, Strategic Guidelines] : Dys. Kyiv : Natsionalnyi pedahohichnyi universytet imeni M. P. Drahomanova, Lvivskyi natsionalnyi universytet imeni Ivana Franka. 423 p. [in Ukrainian]

3. Zolotar, O. O. (2017) Osoblyvosti informatsiinoi bezpeky liudyny v umovakh hibrydnoi viiny [Features of human information security in a hybrid war]. *Informatsiia i pravo*, № 3 (22). P. 124–131. [in Ukrainian]

4. Petryk, V. M., Lishchynska, O. A., Kalnysh, V. V. (2006) Sotsialno-pravovi osnovy informatsiinoi bezpeky [Socio-legal bases of information security]. Kyiv. 263 p. [in Ukrainian]

5. Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 18 bereznia 2022 roku "Shchodo realizatsii yedynoi informatsiinoi polityky v umovakh voiennoho stanu" [Decision of the National Security and Defense Council of Ukraine of March 18, 2022 "On the implementation of a unified information policy in martial law"]. URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#Text [in Ukrainian]

6. Khvorost, Kh. Iu. (2016) Informatsiino-psykholohichnyi vplyv u rozrizi bezpeky zdorovia [Information and psychological impact in terms of health security]. *Nauka i osvita.* № 2–3. P. 184–191. [in Ukrainian]

7. McDonald, R. 5 information Security Challenges All Universities Face. URL: https://www.virtru.com/blog/security-challenges/ (in English).

8. Network security in Universities, Colleges and Schools. URL: https://www.isdecisions.com/blog/it-management/network-security-in-universities-colleges-and-schools/

9. Why is Information Security important? URL: https://www.plymouth.ac.uk/students-and-family/governance/information-governance/information-security

Стаття надійшла 17.02.2022