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

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
II наукової онлайн-конференції

(Суми, 02 липня 2024)

Суми
Сумський державний університет
2024

004.056.5:336(082)
В43

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

Затверджено Вченою Радою Сумського державного університету (протокол № 1, 29.08.2024)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 02 липня 2024. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2024. – 72 с.

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

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

004.056.5:336(082)

ЗМІСТ

СЕКЦІЯ 1	***ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ***	**5**
Іван Нестеренко	ДОСЛІДЖЕННЯ ЦИФРОВИХ ТРАНСФОРМАЦІЙ В ЕКОНОМІЦІ	5
Катерина Дідоренко	ЦИФРОВІЗАЦІЯ ЯК ФАКТОР ПОСИЛЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ КРАЇНИ	9
Володимир Науменко	МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ВПЛИВУ РІВНЯ ЦИФРОВІЗАЦІЇ НА ЕКОНОМІЧНИЙ РОЗВИТОК	12
Дмитро Харченко	РОЛЬ ЦИФРОВІЗАЦІЇ В ПРОТИДІЇ КОРУПЦІЇ	16
Захарченко Андрій	ЦИФРОВІ НАВИЧКИ: ВИКЛИКИ ТА МОЖЛИВОСТІ	19
Даніїл Савченко, Тетяна Доценк	ТЕОРЕТИЧНІ АСПЕКТИ ВЗАЄМОЗВ'ЯЗКІВ КІБЕРБЕЗПЕКИ ТА БЕЗПЕКИ ОХОРОНИ ЗДОРОВ'Я	24
СЕКЦІЯ 2	***КІБЕРЗАГРОЗИ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ***	***27***
Віталія Койбічук	ІДЕНТИФІКАЦІЯ ТА УПЕРЕДЖЕННЯ КІБЕРШАХРАЙСТВ В ЕЛЕКТРОННОМУ БАНКІНГУ: ДОСВІД ЄС	27
Роєнко Олександр	КОНВЕРГЕНЦІЙНІ ПРОЦЕСИ МІЖ КІБЕРЗЛОЧИННІСТЮ ТА ТІНЬОВОЮ ЕКОНОМІКОЮ	31
Ксенія Могильна	АНАЛІЗ ОСНОВНИХ ТРЕНДІВ НА СВІТОВОМУ РИНКУ КІБЕРСТРАХУВАННЯ	34
Ольга Горбачова	ТЕНДЕНЦІЇ РОЗВИТКУ РИНКУ КІБЕРСТРАХУВАННЯ У СВІТІ	39
Валерія Кочнєва	РОЛЬ КІБЕРСТРАХУВАННЯ У ПІДВИЩЕННІ РІВНЯ КІБЕРСТІЙКОСТІ КОМПАНІЙ	41
Іван Гончарук	КОРУПЦІЯ ЯК ІНСТРУМЕНТ ПРОНИКНЕННЯ ТА ВИКРАДАННЯ ІНСАЙДЕРСЬКИХ ДАНИХ	45
СЕКЦІЯ 3	***ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ***	92

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Avhusta Hrytsenko	*THE ROLE OF ARTIFICIAL INTELLIGENCE IN COUNTERING CYBER THREATS*	*48*
Вікторія Біловодська	*РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ*	*53*
Оголь Дмитро	*МЕТОДИ ПІДВИЩЕННЯ ЦИФРОВОЇ ОБІЗНАНОСТІ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ: УСПІШНІ ВІТЧИЗНЯНІ ТА ЗАКОРДОННІ КЕЙСИ*	*57*
Анна Шаповалова	*ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ*	*61*
Еліна Шрамко	*ШТУЧНИЙ ІНТЕЛЕКТ У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ: ЕФЕКТИВНІ СТРАТЕГІЇ ТА ІНСТРУМЕНТИ*	*64*
Єлизавета Литюга	*ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ*	*69*

ТЕОРЕТИЧНІ АСПЕКТИ ВЗАЄМОЗВ'ЯЗКІВ КІБЕРБЕЗПЕКИ ТА БЕЗПЕКИ ОХОРОНИ ЗДОРОВ'Я

THEORETICAL ASPECTS OF INTERCONNECTIONS OF CYBER SECURITY AND HEALTH CARE SECURITY

Даніїл Савченко, студент
Сумський державний університет, Україна

Тетяна Доценко, доктор філософії
Сумський державний університет, Україна,
Технічний університет Берліну, Німеччина

В сучасному цифровому світі, де віртуальна реальність переплітається з реальним життям, питання кібербезпеки та безпеки міцного здоров'я стають дедалі більш актуальними та важливими. Зростання залежності від інформаційних технологій вносить свої виклики і загрози, які впливають на економічний, соціальний та медичний аспекти суспільства. В цьому контексті виникає потреба в розробці комплексних економіко-математичних моделей, спрямованих на аналіз та прогнозування взаємозв'язків між кібербезпекою та безпекою міцного здоров'я країн світу.

Поняття кібербезпеки і безпеки охорони здоров'я є відносно новими категоріями, що набувають активного використання серед сучасних науковців світу: Алкудхайбі А. (Alqudhaibi et al., 2024), Феррейра Д. (Ferreyra et al., 2024), Фатокун Ф. (Fatokun et al., 2024), Хоссейн М. (Hossain et al., 2024), Ху К. (Hu et al., 2024).

Кібербезпека (cyber security) – це заходи, які вживають для захисту даних або пристроїв, підключених до мережі, від несанкціонованого доступу та використання у злочинних цілях. Кібербезпека це те, що забезпечує конфіденційність, цілісність і доступність даних протягом їх всього життєвого циклу. Виклики сучасної кібербезпеки наступні: у цифрову еру кібербезпека є критичною проблемою для людей, корпорацій та урядів; зі збільшенням використання технологій і цифрових пристроїв як ніколи необхідно захищати електронні пристрої, мережі та дані від небажаного доступу, крадіжки та пошкодження; з розвитком технологій дія кібербезпеки щодо захисту організації, співробітників і критично важливих активів від кіберзагроз стикається з кількома проблемами. Для кращого захисту від кіберзагроз необхідно знати типи кібербезпеки: безпека мережі, безпека програми, інформаційна безпека, хмарна безпека, безпека інтернету речей, управління ідентифікацією та доступом.

Безпеки охорони здоров’я включає зобов’язання щодо безпеки працівників, надання та адекватний доступ до засобів безпеки та засобів індивідуального захисту, а також широкі зусилля з навчання, які використовують протоколи, що вимагають певних заходів безпеки. Виділяють категорії небезпек, пов’язаних з роботою системи охорони здоров’я: біологічні небезпеки, хімічні небезпеки, механічні небезпеки навколишнього середовища, фізичні небезпеки, психосоціальні небезпеки.

Зв'язок між кібербезпекою та безпекою охорони здоров'я можна представити наступною схемою (рисунок 1).

Рисунок 1. Взаємозв’язок між кібербезпекою та безпекою охорони здоров'я

Джерело: сформовано автором

Ця схема демонструє взаємозв'язок між кібербезпекою та безпекою охорони здоров'я, акцентуючи на загрозах, які виникають внаслідок вразливостей у медичних системах, таких як кібератаки на медичні системи. Це призводять до вразливостей у медичних інформаційних системах, що в свою чергу може призвести до зловмисних дій, таких як витік даних, шифрування даних або блокування доступу. При чому зв'язок між кібербезпекою та безпекою охорони здоров'я також полягає в тому, що кібербезпека дозволяє забезпечувати захист інформаційних систем, даних медичних установ, персональної інформації пацієнтів, що є критичним для безперебійного функціонування закладів охорони здоров’я, надійного захисту пацієнтів. А вразливості в системі кібербезпеки можуть призвести до витоків важливої конфіденційної інформації, порушень у функціонуванні

медичних систем, загроз для здоров'я пацієнтів. В свою чергу, ефективна кібербезпека є невід'ємною складовою загальної безпеки охорони здоров'я.

Особливе місце у дослідженні напрямків кібербезпеки та безпеки охорони здоров’я відводиться саме моделюванню таких систем. Це дможе суттєво допомогти у прийнятті обґрунтованих управлінських рішень, підвищенні рівня безпеки медичного персоналу, пацієнтів, оптимізації роботи медичних закладів в умовах обмеженості ресурсів, а також надзвичайних ситуацій.

Моделювання кіберзагроз – це процес аналізу різноманітних ділових і технічних вимог до системи, визначення потенційних загроз і документування того, наскільки ці загрози роблять систему вразливою. Загроза стосується будь-якого випадку, коли неавторизована сторона отримує доступ до конфіденційної інформації, програм або мережі організації. Процес моделювання кіберзагроз включає наступні ключові кроки: постановка цілі; візуалізація; визначення загрози; пом’якшення; перевірка. Наступним виділено три методологій моделювання кіберзагроз: STRIDE (методологія, розроблена корпорацією Майкрософт для моделювання загроз, пропонує мнемоніку для визначення загроз безпеці в шести категоріях: підробка, втручання, відмова, розголошення інформації, відмова в обслуговуванні, підвищення привілеїв); DREAD (спосіб класифікувати й оцінювати ризики безпеки за п’ятьма категоріями: потенційна шкода, відтворюваність, можливість використання, постраждалі користувачі, виявленість); P.A.S.T.A («Процес симуляції атак і аналізу загроз» – семиетапна методологія, орієнтована на ризик; пропонує динамічну ідентифікацію загроз, процес підрахунку та оцінювання; після того, як експерти проведуть детальний аналіз виявлених загроз, розробники можуть розробити стратегію пом’якшення, орієнтовану на ресурси, проаналізувавши програму через погляд, орієнтований на зловмисників).

Моделювання безпеки охорони здоров'я - це процес побудови та застосування моделей для аналізу, оцінки та прогнозування безпеки в системах охорони здоров'я, що включає наступні напрямки: аналіз ризиків; прогнозування подій; оцінка ефективності заходів; планування ресурсів; симуляції. Можна виділити основні моделі охорони здоров’я: модель Беверіджа (уряд діє як єдиний платник, усуваючи будь-яку конкуренцію на ринку, щоб зберегти низькі витрати та стандартизувати виплати; будучи єдиним платником, національна служба охорони здоров’я контролює, що можуть робити «внутрішні мережеві» провайдери та які вони можуть стягувати; фінансується за рахунок податків); модель Бісмарка (більш децентралізована форма охорони здоров’я; роботодавці та працівники несуть відповідальність за фінансування своєї системи медичного

страхування через «лікарняні фонди», створені шляхом відрахувань із заробітної плати; постачальники та лікарні, як правило, є приватними, хоча страхові компанії є державними); національна модель медичного страхування (держава діє як єдиний платник за медичні процедури; провайдери є приватними; моделлю керують приватні постачальники, але виплати надходять від державної програми страхування, у яку платить кожен громадянин; є універсальним страхуванням, яке не приносить прибутку та не відмовляє у виплаті претензій); кишенькова модель (пацієнти повинні платити за свої процедури зі своєї кишені; заможні отримують професійну медичну допомогу, а бідні – ні, якщо тільки вони якимось чином не знайдуть достатньо грошей).

Отже, взаємозв'язки між кібербезпекою та безпекою охорони здоров'я є критично важливими і необхідними для забезпечення безпечного, надійного, ефективного функціонування медичних систем, захисту здоров'я пацієнтів у цифрову епоху. Результати досліджень, проведених у цій роботі, мають потенціал відіграти важливу роль у формуванні політики в галузі кібербезпеки, а також слугувати основою для подальших наукових досліджень у цій області.

Список використаних джерел

1. Alqudhaibi, A., Krishna, A., Jagtap, S. et al. (2024). Cybersecurity 4.0: safeguarding trust and production in the digital food industry era. *Discov Food*, 4, 2. https://doi.org/10.1007/s44187-023-00071-7.

2. Diaz Ferreyra, N.E., Vidoni, M., Heisel, M. (2024). Cybersecurity discussions in Stack Overflow: a developer-centred analysis of engagement and self-disclosure behaviour. *Soc. Netw. Anal. Min*., 14, 16. https://doi.org/10.1007/s13278-023-01171-z.

3. Faith Fatokun, Zalizah Awang, Suraya Hamid, Johnson O. Fatokun and Azah Norman. (2024). Cybersecurity Knowledge Deterioration and the role of Gamification Intervention. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 43, 1, pp.66–94. https://doi.org/10.37934/araset.43.1.6694.

4. Hossain, M.A., Islam, M.S. (2024). Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity. *Cybersecurity*, 7, 16. https://doi.org/10.1186/s42400-024-00205-z.

5. Hu, C., Wu, T., Liu, C. et al. (2024). Joint contrastive learning and belief rule base for named entity recognition in cybersecurity. *Cybersecurity*, 7, 19. https://doi.org/10.1186/s42400-024-00206-y.