ISSN 2308-0361

DOI: https://doi.org/10.33731/32019.173819

КІБЕРЗЛОЧИННІСТЬ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я: РЕАЛЬНІСТЬ, ЩО ПОТРЕБУЄ ЗАХИСТУ

Інна Волинець,
молодший науковий співробітник, аспірант НДІ інтелектуальної власності НАПрН України, фахівець Науково-освітнього центру інтелектуальної власності Київського національного університету імені Тараса Шевченка
ID ORCID: 0000-0002-2029-2165

У статті розглянуто проблемні питання протидії кіберзлочинності як потенційній загрозі у сфері охорони здоров'я. Розкрито зміст понять «кіберзлочин» і «кіберзлочинність»; окреслено причини та наслідки впливу кібератак. Відповідно до характеристики видів кіберзлочинів наведено приклади здійснення кібератак у сфері охорони здоров'я. Проведено аналіз нормативно-правових актів з цієї проблематики. Визначено можливі загрози інформаційній безпеці Україні. Наголошено на важливості теоретичного та практичного вдосконалення заходів протидії кібератакам відповідно до сучасних закордонних напрацювань боротьби з кіберзлочинністю та захисту персональних даних, а також імплементації на законодавчому рівні керівних принципів захисту даних.

Ключові слова: кіберзлочинність, хакер, кібератаки, охорона здоров'я, захист персональних даних, кібербезпека, реєстр

Вступ. Загрози людству у XXI столітті сягнули нового рівня. В інформаційну епоху пересічному користувачеві нескладно знайти, передати, відслідкувати дані через мережу Інтернет. Однак, якщо йдеться про досвідчених користувачів, які можуть скористатися отриманими даними проти особи, суспільства, держави, що ставить під загрозу їх безпеку, то це є однин із видів порушення національної безпеки країни та називається кіберзлочинністю.

Постановка проблеми. Світова статистика стверджує, що в період між 2015–2017 роками основними галузями, що потерпали від дій кіберзлочинців, були охорона здоров'я, промисловість, фінанси, уряд, транспорт [1].

Однією з найбільш уразливих сфер є охорона здоров'я. Через слабкі системи захисту відбувається викрадення особистих даних пацієнтів, виводиться з ладу обладнання лікарень, що працює через мережеве живлення. Як наслідок, зазнають шкоди репутація лікарень, під загрозою опиняються приватність пацієнтів, їхнє здоров'я і навіть життя.

Огляд літератури. Проведений аналіз засвідчує, що українськими та зарубіжними науковцями вивчено значний комплекс проблем стосовно механізмів запобігання та протидії кіберзлочинності, однак проблеми останньої, зокрема у сфері охорони здоров'я, є малодослідженими.

Провідними вченими, які вивчають питання законодавчого забезпечення захисту прав людини у сфері охорони здоров'я, є О. Кашинцева, І. Сенюта, О. Орлюк та інші. Різноманітні питання теорії та практики запобігання кіберзлочинності, боротьби з її проявами та про-

тидії злочинам у сфері високих технологій розглянуто в роботах Н. Ахтирської, П. Біленчука, М. Гуцалюк, М. Карчевського, О. Манжая, В. Номоконова, І. Хараберюша та інших.

Зазначена проблематика є предметом дослідження зарубіжних учених. Зокрема, Eric D. Perakslis проводив дослідження щодо кібербезпеки у сфері охорони здоров'я [2]. Науковці Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson і D. Kyle Monticone розглянули питання сприяння кібербезпеці у сфері охорони здоров'я та подали системний огляд сучасних загроз і тенденцій [3]. Зокрема, Clemens Scott Kruse, Luna Raul, Rhine Emily, Myhra Matthew, Sullivan Ross здійснили системний огляд кіберзагроз інформаційним системам охорони здоров я [4]. Lynne Coventry, Dawn Branley з Нортумбрійського університету (Велика Британія) провели дослідження щодо кібербезпеки у сфері охорони здоров'я та описового аналізу тенденцій, загроз і напряму подальших дій [5].

Метою статті є огляд кіберзлочинів, аналіз їх видів, визначення видів кібератак у сфері охорони здоров'я, окреслення наслідків кібератак, дослідження сучасних закордонних методів боротьби з кібератаками та можливих впливів кібератак в Україні на сферу охорони здоров'я.

Виклад основного матеріалу. На сьогодні в Україні є низка нормативно-правових актів, які регулюють відносини щодо захисту від інформаційних загроз. Так, затверджено закони України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про захист персональних даних», «Про інформацію», «Про державну таємницю», а також Указ Президента України «Про Національний координаційний центр кібербезпеки» тощо.

Значимо, що у 2017 році набрав чинності Закон України «Про основні засади забезпечення кібербезпеки України» (із змінами, внесеними згідно із законом № 2469-VIII від 21 червня 2018 року), який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки [6].

Важливе значення має також Стратегія кібербезпеки нашої країни. Так, в Указі Президента України «Про Стратегію кібербезпеки України» від 27 січня 2016 року вказано на необхідність створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства та держави, а також визначено мету, основні принципи забезпечення кібербезпеки України, окреслено загрози кібербезпеці, визначено Національну систему кібербезпеки, а також основні суб'єкти забезпечення кібербезпеки і пріоритети та напрями забезпечення кібербезпеки України [7].

Чинний Кримінальний кодекс України встановлює (відповідно до розділу XVI) відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [8].

Крім того, правове регулювання міжнародної співпраці у сфері запобігання та протидії кіберзлочинності здійснюється «Конвенцією про кіберзлочинність», прийнятою Радою Європи 23 листопада 2001 року в Будапешті [9], яку ратифіковано Законом України «Про ратифікацію Конвенції про кіберзлочинність» [10] від 7 вересня 2005 року тощо. У документі сформульовано найбільш загальні та головні принципи забезпечення заходів боротьби із кіберзлочинами на національному та міжнародному рівнях.

У «Конвенції про кіберзлочинність» (2001 рік) розрізняють такі види кіберзлочинів (правопорушень): незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему; зловживання пристроями; підробка, пов'язана з комп'ютерами; шахрайство, пов'язане

з комп'ютерами; правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських та суміжних прав [9].

На сьогодні національне законодавство не виділяє сферу охорони здоров'я як окрему для захисту від кіберзлочинів.

Так, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» поняття кіберзлочин (комп'ютерний злочин) визначено як «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України». У документі зазначено, що кіберзлочинність — це сукупність кіберзлочинів [6].

Кіберзлочинність спрямована на заподіяння шкоди саме репутації особи або групі осіб чи порушення фізичного та/або психічного здоров'я, використовуючи сучасні методи комунікації між людьми (Інтернет, електронну пошту, соціальні мережі, мобільний зв'язок (СМС, ММС тощо). Налічується велика кількість видів кіберзлочинів, зокрема: інтернет-шахрайство (фішинг, англ. *Phishing*), крадіжка особистості (англ. *Identity theft*), хакінг, підбурення до тероризму, розповсюдження дитячої порнографії тощо [11].

Кіберзлочини здійснюються завдяки кібератакам, що поділяються на дві категорії:

- націлена завдати шкоду через мережу або пристрої (віруси, шкідливе програмне забезпечення, потенційно небажана програма (англ. PUPs), DoS-атаки);
- спрямована на використання пристроїв для участі у злочинній діяльності (фішинг, віртуальне переслідування, соціальна інженерія, крадіжка особистості) [12].

Основними причинами вторгнення кібератак у сферу охорони здоров'я є:

- малозахищеність цієї сфери, порівняно з рівнем розвитку кіберзлочинності;
- зберігання даних пацієнтів в електронному вигляді;
- цінність конфіденційних даних лікарень та інших медичних установ;
- торгівля конфіденційними даними пацієнтів на «чорному ринку» з метою шантажу, збагачення, розголошення інформації тощо;
- посягання на особисті дані лікаря (історії хвороб пацієнтів, виписаних ним рецептів, результатів аналізів) або на адреси електронної пошти, паролі, номери соціального страхування, конфіденційну інформацію співробітників медичних установ тощо;
- викрадення патентів фармацевтичної компанії конкурента [13].

Для розуміння поняття кіберзлочинності вважаємо за доцільне розглянути основні види кібератак.

1. ***Програми-вимагачі*** (англ. *ransomware*, що походить від слів *ransom* — викуп і *software* — програмне забезпечення). Це тип шкідливого програмного забезпечення, що заражує системи і файли, блокує їх та вимагає викуп для відновлення останніх. Коли це відбувається у сфері охорони здоров'я, критичні процеси сповільнюються або стають повністю непрацездатними. Зараження комп'ютера від такої програми може відбутися у такий спосіб: через фішингові листи, що містять шкідливий додаток, через користувача, через перехід на шкідливе посилання та через перегляд реклами, що містить шкідливу програму (англ. *malvertising*) [14].

Наприклад, 12 травня 2017 року у Лондоні (Велика Британія) найбільш резонансна масова кібератака сталася через програму, що спричинила поломку комп'ютерів Національної системи охорони здоров'я (англ. NationalHealthService (NHS)). Майже 40 організацій цієї системи були інфіковані вірусом WanaCrypt0r 2.0, більш відомим як WannaCry. Ця програма є програмою-вимагачем коштів та діє тільки при операційній системі Microsoft Windows.

Після ураження комп'ютера програмний код заблокував та зашифрував майже всі збережені на ньому файли. Було запропоновано заплатити грошовий викуп за їх розшифрування у розмірі 300 дол. (233 фунти стерлінгів) за кожен заражений комп'ютер [15]. У разі несплати протягом 3 днів з моменту блокування даних вірусом ціна подвоювалася, а несплата протягом 7 днів унеможливлювала розшифрування файлів, що втрачалися назавжди. Як наслідок, було відкладено проведення призначених медичних процедур, обстежень і термінових операцій. Єдине, чого не в змозі зробити вірус — це викрасти персональні дані пацієнтів лікарень, госпіталів та інших медичних організації.

Атака вірусу поширилася за 4 дні не тільки на Велику Британію, а по всьому світу. Великих збитків та уражень вірус завдав в Україні, Росії, Індії, Тайвані. Від вірусу WannaCrypo постраждали близько 200–300 тис. користувачів у 150 країнах світу. Відповідальність за атаку була покладена на Корейську Народно-Демократичну Республіку. Загальна сума збитків становила 1 млрд дол. [16].

2. ***Хакерські атаки, що спричинюють відмову в обслуговуванні***, відомі як атака DoS (англ. denialofservice) або атака DDoS (англ. Distributed denial of service), по-розмовному «докінг». Різниця між ними полягає у тому, що атака DDoS поширюється через безліч комп'ютерів та спрямована на масову відмову добре захищених систем лікарень, фармацевтичних компаній тощо. Від такої атаки неможливо захиститися, заблокувавши лише один комп'ютер або кілька. Однак, атака DoS, як правило, зламує одного користувача через один пристрій. Такі хакерські атаки спрямовані на блокування даних користувачів тимчасово або на невизначений термін [17]. Проте, навіть незначна (короткотривала) хакерська атака може спричини зупинку в медичному обслуговуванні, яке потребує доступу до мережі, щоб забезпечити належний догляд за пацієнтами, або доступу до Інтернету для відправлення та отримання електронних листів, рецептів, записів та інформації про пацієнтів [18].

Розглянемо приклад кібератаки, наслідком якої стало відкриття судової справи. У 2014 році в дитячій лікарні Бостона була здійснена хакерська атака хактивістським угрупованням «Анонімус».

Причиною став випадок із 15-річною дівчиною Юстиною Пеллетьє, яка хворіла на соматичний розлад, спричинений психологічними проблемами, що викликали фізичне нездужання. Батьки дівчини наполягали на примусовому утримуванні дитини в лікарні та застосовуванні всіх можливих методів лікування.

Ознайомившись з історією хвороби Юстини Пеллетьє, служба охорони штату Массачусетс визначила, що застосування примусового лікування є спірним і взяла дівчину під опіку. Їй надали палату в Бостонській лікарні для повторного обстеження та лікування, а батькам заборонили втручатися в цей процес.

Хактивістське угруповання «Анонімус» обурило таке ставлення до дівчини, адже це порушувало її права. Угруповання запустило «докінг», спрямований на відмову системи дитячої лікарні. Хакерська атака спричинила збій основної медичної мережі Бостона, який тривав майже тиждень і завдав збитків на близько 300 тис. дол. [19].

3. ***Інсайдерські загрози*** (англ. *Insider Threats*). Шкоду у сфері охорони здоров'я спричинюють також робітники медичних закладів. За даними «2018 IBM X-Force Threat Intelligence Index», на такий вид кібератак припадає понад 60 % випадків [20].

Серед порушників безпеки можна виділити: працівників, які через свою недбалість ненавмисно спричинили збій у роботі лікарні (перехід на шкідливе посилання, відкриття доступу до баз даних тощо); працівників, які діяли навмисно, надаючи ключі доступу до приватної інформації (англ. *Personally Identifiable Information (PII)*) або до за-

хищеної інформації про стан здоров'я пацієнтів (англ. *Protected Health Information (PHI)*) задля отримання прибутку тощо [21].

Прикладом інсайдерської загрози може слугувати подія, що сталася у 2009 році в місті Даллас (штат Техас, США). Зокрема, колишній нічний охоронець Північного центрального медичного центру Джессі Вільям МакГроу (за сумісництвом хакер під псевдонімом «Ghost Exodus») зламав комп'ютерну систему лікарні, у тому числі комп'ютери медсестер, що містили дані про стан здоров'я пацієнтів, особисті дані, історії хвороб, а також платіжні документи. Метою таких дій була дискредитація системи лікарні та передача ключів доступу членам хакерського угруповання «Electronik Tribulation Army» (ETA).

Вказані дії могли призвести до збою в системі управління опаленням, вентиляцією та кондиціонуванням, до погіршення самопочуття пацієнтів лікарні через спеку, спричинити псування ліків і медичного обладнання [22].

У березні 2011 року прокуратура Північного округу штату Техас, підпорядкована Міністерству юстиції Сполучених Штатів, засудила МакГроу до 110 місяців ув'язнення у Федеральній в'язниці [23].

Отже, сфера охорони здоров'я потребує сучасних методів захисту.

Зазначимо, що на зменшення, припинення, подолання кібернетичних атак у США передбачається виділити у 2017–2021 роках 65 млрд дол. [24]. Це зумовлено тим, що від кібератак найбільше потерпають розвинені країни через використання сучасних медичних технологій, однак застарілих систем захисту у сфері охорони здоров'я.

На підставі аналізу зазначеного наголосимо, що охорона здоров'я є однією з найбільш уразливих сфер перед загрозою кіберзлочинів.

На веб-порталі іспанської компанії Panda Security, що спеціалізується на розробці технологій у галузі інформаційної безпеки, зокрема щодо запобігання кіберзлочинності [25], вказано профілактичні методи попередження кібератак:

1. Не натискати на незнайомі посилання або рекламу.
2. Використовувати VPN (скорочення від англ. Virtual Private Network — віртуальна приватна мережа).
3. Перш ніж вводити облікові дані, переконатися у безпеці веб-сайта.
4. Своєчасно активувати та підтримувати в дії антивірусні програми.
5. Використовувати надійні паролі з 14+ символами.

Запропоновані методи будуть дієвими як для особистого користування мережею Інтернет, так і для підприємств [12].

У нашій країні питання захисту від кібератак у сфері охорони здоров'я також є важливими з огляду на перспективи реалізації Міністерством охорони здоров'я України стратегії та механізмів, що гарантуватимуть доступність, ефективність ліків. Нововведення вже розпочалися згідно з Урядовою програмою «Доступні ліки» та повинні бути реалізовані до кінця 2019 року. Ідеться про системи Е-рецепту (з 1 квітня 2019 року) та Е-документообігу, що включатиме: е-редукціон, автоматизоване формування реєстру, звітності [26].

Утілення зазначеного плану дій МОЗ України забезпечене набранням чинності Законом України «Про державні фінансові гарантії медичного обслуговування населення» від 30 січня 2018 року. Медична реформа передбачає, зокрема, й електронну систему охорони здоров'я «eHealth» — інформаційно-телекомунікаційна система, що забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією в електронному вигляді, до складу якої входять центральна база даних і медичні інформаційні системи, між якими забезпечено автоматичний обмін даними через відкритий програмний інтерфейс (API) [27].

Національною службою здоров я України (далі — НСЗУ) забезпечується

функціонування електронної системи охорони здоров'я. Так, відповідно до постанови Кабінету Міністрів України «Деякі питання електронної системи охорони здоров'я» від 25 квітня 2018 року затверджено Порядок функціонування електронної системи охорони здоров'я, у якому подано перелік таких реєстрів:

1) реєстр пацієнтів, що містить інформацію про фізичних осіб;
2) реєстр декларацій про вибір лікаря, який надає первинну медичну допомогу, що містить інформацію про декларації;
3) реєстр суб'єктів господарювання у сфері охорони здоров'я, що містить інформацію про заклади охорони здоров'я, фізичних осіб-підприємців;
4) реєстр медичних спеціалістів, що містить інформацію про осіб, які здобули освіту у сфері охорони здоров'я;
5) реєстр медичних працівників, що містить інформацію про осіб, які перебувають у трудових відносинах із суб'єктами господарювання у сфері охорони здоров'я або є фізичною особою-підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та надають медичну допомогу;
6) реєстр договорів про медичне обслуговування населення, що містить інформацію про договори про медичне обслуговування населення за програмою медичних гарантій, укладені з НСЗУ;
7) реєстр договорів про реімбурсацію, що містить інформацію про договори про реімбурсацію за програмою медичних гарантій, укладені з НСЗУ;
8) інші реєстри [28].

Таким чином, в Україні започаткований перехід від паперової документації до електронної, тому закордонні напрацювання щодо безпеки та захисту від кібератак варто реалізувати до введення в дію медичної реформи, не чекаючи на інформаційне наповнення особистими «уразливими даними» в реєстрах про пацієнтів, медичних працівників, медичних закладів тощо.

Висновки. Проблематика поширення кіберзлочинності у сфері охорони здоров'я є актуальною в усьому світі та стосується не лише розвинених країн, а й тих, що розвиваються. На жаль, зазначені національні та міжнародні нормативно-правові акти не відповідають новим тенденціям протидії кіберзлочинності. Кількість вірусних програм щороку зростає, натомість бракує сучасних методів боротьби, особливо на державному рівні. В Україні перехід від паперової форми зберігання даних до електронної варто посилити на технологічному і законодавчому рівнях, прописавши дієвий алгоритм дій для всіх можливих випадків втручання в електронну систему збереження медичної інформації. Зокрема, доцільним буде застосувати практичні закордонні напрацювання боротьби з кіберзлочинністю та захистом персональних даних, а також імплементувати на законодавчому рівні керівні принципи захисту даних. Особливу увагу варто звернути на нещодавно прийняті у Страсбурзі Рекомендації Комітету міністрів Ради Європи державам-членам про захист даних, пов язаних зі здоров ям (англ. Recommendation CM/Rec (2019) 2 of the Committee of Ministers to member States on the protection of health-related data) від 27 березня 2019 року. Однією з головних цілей зазначеного документа є надання державам-членам керівних принципів щодо регулювання обробки пов язаних зі здоров'ям даних, їх захисту. Комітет міністрів підкреслює, що вказані дані повинні бути захищені відповідними заходами безпеки з урахуванням останніх технологічних досягнень і оцінки потенційних ризиків. Таким чином, захист від кіберзлочинності повинен ураховувати зазначену міжнародну практику та сучасні технологічні досягнення у сфері протидії правопорушенням в електронних мережах, які здійснюють зберігання, обробку, накопичення та використання медичної інформації. ◆

Список використаних джерел / List of references

1. *Morgan S.Top 5 IndustriesAtRiskOfCyber-Attacks.*
URL: https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#22d4c536715e.
2. *Perakslis Eric D.Cybersecurity in Health Care.*
URL: https://www.nejm.org/doi/full/10.1056/NEJMp1404358?url_ver=Z39.88-2003&rfr_id=ori%3Arid%3Acrossref.org&rfr_dat=cr_pub%3Dpubmed.
3. *Kruse C. S., Frederick B., Jacobson T.,MonticoneK. Cybersecurity in healthcare: A systematic review of modern threats and trends. TechnologyandHealthCare. 2017. vol. 25. P. 1–10. URL: https://content.iospress.com/download/technology-and-health-care/thc1263?id=technology-and-health-care%2Fthc1263.*
4. *Raul L. Rhine E., Myhra M., Sullivan R., Kruse C.S. Cyberthreatstohealthinformationsystems: A systematicreview. Technology and Health Care. 2016. vol. 24. 1. P. 1–9. URL: https://content.iospress.com/articles/technology-and-health-care/thc1102.*
5. *CoventryL., BranleyD.Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018. vol. 113. P. 48–52. URL: https://www.sciencedirect.com/science/article/pii/S0378512218301658?via%3Dihub#.*
6. *Про основні засади забезпечення кібербезпеки України : Закон України від 08.07.2018 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.*
7. *Про рішення Ради національної безпеки і оборони України : Указ Президента України від 27.01.2016 р. «Про Стратегію кібербезпеки України». Офіційний вісник Президента України. 2016. № 10. Ст. 39. стаття 198.*
8. *Кримінальний кодекс України від 26.02.2019 р. №2341-III. Відомості Верховної Ради України. 2001. № 25–26. Ст.131.*
9. *Конвенція про кіберзлочинність. Ратифікація від 07.09.2005 р. № 994_575. Офіційний вісник України. 2007. № 65. Ст. 107.*
10. *Про ратифікацію Конвенції про кіберзлочинність: Закон України від 14.10.2010 р. № 2824-IV. Відомості Верховної Ради України. 2006. № 5. Ст. 128.*
11. *Forms of cybercrime. Cyber crime takes many forms, and it is there fore difficult to fight. URL: https://www.government.nl/topics/cybercrime/forms-of-cybercrime*
12. *Types of Cybercrime.*
URL: https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime.
13. *Кибер-пандемия: компьютерные атаки в сфере здравоохранения.*
URL: https://habr.com/company/panda/blog/304382.
14. *Ransomware: In the Health care Sector.*
URL: https://www.cisecurity.org/ransomware-in-the-healthcare-sector.
15. *Jones S.NHS seeks to recover from global cyber-attack as security concerns resurface. URL: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack.*
16. *Эксперты оценили ущерб от вируса WANNACRY в $ 1 млрд. Специалисты подсчитали ущерб, нанесенный вирусом WannaCrypt0r за первые четыре дня масштабной кибератаки.*
URL: http://runews24.ru/internet/25/05/2017/3deb290a821bd12cc946653ea418e439.
17. *Security Tip (ST04-015). Understanding Denial-of-Service Attacks.*
URL: https://www.us-cert.gov/ncas/tips/ST04-015.
18. *DDoS Attacks: In the Healthcare Sector.. URL: https://www.cisecurity.org/ddos-attacks-in-the-healthcare-sector.*
19. *Anyoneis a Target: DoSAttackCaseAnalysisonBostonChildren'sHospital.*
URL: https://security.radware.com/.../DownloadAsset.aspx?id=873.
20. *Henry J.These 5 Types of Insider Threats Could Lead to Costly Data Breaches.*

URL: https://securityintelligence.com/these-5-types-of-insider-threats-could-lead-to-costly-data-breaches.

21.Insider Threats: In the Healthcare Sector.

URL: https://www.cisecurity.org/blog/insider-threats-in-the-healthcare-sector.

22.PoulsenK.Leader of hacker gang sentenced to 9 years for hospital malware.

URL: https://www.wired.com/2011/03/ghostexodus-2.

23.Former security guard, who hacked into hospital's computer system, is sentenced to 110 months in federal prison. Defendant Posted Video of Himself Compromising a Hospital's Computer System on YouTube.

URL: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/mcgrawSent.pdf.

24.Morgan S.Why healthcare cybersecurity spending will exceed $65B over the next 5 years. Hospitals and healthcare providers remain under cyber attack, causing organizations to spend more to protect their systems and patient dataURL:https://www.csoonline.com/article/3252343/cyber-attacks-espionage/why-healthcare-cybersecurity-spending-will-exceed-65b-over-the-next-5-years.html.

25.About Panda Security. URL: https://www.pandasecurity.com/ukraine/company-profile.

26.Ілик Р. Фармполітика 2019. Цілі та нові виклики. Стратегія лікарських засобів до 2025. Аптечний саміт України – 2018 : матеріали презентації. Київ. 06.12.2018. URL : C:\Users\user\AppData\Local\Temp\Rar$DI07.255.2-¦Ш¦¬ТЛ¦¦.pdf.

27.Про державні фінансові гарантії медичного обслуговування населення : Закон України від 19.10.2017 р. № 2168-VIII. Відомості Верховної Ради України. 2018. № 5. Ст. 5.

28.Деякі питання електронної системи охорони здоров'я : постанова Кабінету Міністрів України від 25.04.2018 р. № 411. Офіційний вісник України. 2018. № 46. Ст. 14.

29.Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data.

URL : https://search.coe.int/cm/pages/result_details.aspx?objectid =090000168093b26e.

30.Protection of health-related data: Council of Europe issues new guidelines. URL: https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=090000168093b57d.

1. Morgan S.Top 5 IndustriesAtRiskOfCyber-Attacks.

URL: https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#22d4c536715e.

2. Perakslis Eric D.Cybersecurity in Health Care.

URL: https://www.nejm.org/doi/full/10.1056/NEJMp1404358?url_ver=Z39.88-2003&rfr_id=ori%3Arid%3Acrossref.org&rfr_dat=cr_pub%3Dpubmed.

3. Kruse C. S., Frederick B., Jacobson T.,MonticoneK. Cybersecurity in healthcare: A systematic review of modern threats and trends. TechnologyandHealthCare. 2017. vol. 25. P. 1–10. URL: https://content.iospress.com/download/technology-and-health-care/thc1263?id=technology-and-health-care%2Fthc1263.

4. Raul L. Rhine E., Myhra M., Sullivan R., Kruse C.S. Cyberthreatstohealthinformationsystems: A systematicreview. Technology and Health Care. 2016. vol. 24. 1. P. 1–9. URL: https://content.iospress.com/articles/technology-and-health-care/thc1102.

5. CoventryL., BranleyD.Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018. vol. 113. P. 48–52. URL: https://www.sciencedirect.com/science/article/pii/S0378512218301658?via%3Dihub#.

6. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid

08.07.2018 r. № 2163-VIII. Vidomosti Verkhovnoi Rady Ukrainy. 2017. № 45. St. 403.

7. *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy : Ukaz Prezydenta Ukrainy vid 27.01.2016 r. «Pro Stratehiiu kiberbezpeky Ukrainy». Ofitsiinyi visnyk Prezydenta Ukrainy. 2016. № 10. St. 39. stattia 198.*
8. *Kryminalnyi kodeks Ukrainy vid 26.02.2019 r. №2341-III. Vidomosti Verkhovnoi Rady Ukrainy. 2001. № 25–26. St.131.*
9. *Konventsiia pro kiberzlochynnist. Ratyfikatsiia vid 07.09.2005 r. № 994_575. Ofitsiinyi visnyk Ukrainy. 2007. № 65. St. 107.*
10. *Pro ratyfikatsiiu Konventsii pro kiberzlochynnist: Zakon Ukrainy vid 14.10.2010 r. № 2824-IV. Vidomosti Verkhovnoi Rady Ukrainy. 2006. № 5. St. 128.*
11. *Forms of cybercrime. Cyber crime takes many forms, and it is there fore difficult to fight. URL: https://www.government.nl/topics/cybercrime/forms-of-cybercrime*
12. *Types of Cybercrime.*

URL: https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime.

13. *Kyber-pandemyia: kompiuternыe ataky v sfere zdravookhranenyia.*

URL: https://habr.com/company/panda/blog/304382.

14. *Ransomware: In the Health care Sector.*

URL: https://www.cisecurity.org/ransomware-in-the-healthcare-sector.

15. *Jones S.NHS seeks to recover from global cyber-attack as security concerns resurface. URL: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack.*
16. *Эkspertы otsenyly ushcherb ot vyrusa WANNACRY v $ 1 mlrd. Spetsyalystы podschytaly ushcherb, nanesennыi vyrusom WannaCrypt0r za pervыe chetыre dnia masshtabnoi kyberataky.*

URL: http://runews24.ru/internet/25/05/2017/3deb290a821bd12cc94 6653ea418e439.

17. *Security Tip (ST04-015). Understanding Denial-of-Service Attacks.*

URL: https://www.us-cert.gov/ncas/tips/ST04-015.

18. *DDoS Attacks: In the Healthcare Sector. URL: https://www.cisecurity.org/ddos-attacks-in-the-healthcare-sector.*
19. *Anyoneis a Target: DoSAttackCaseAnalysisonBostonChildrensHospital.*

URL: https://security.radware.com/.../DownloadAsset.aspx?id=873.

20. *Henry J.These 5 Types of Insider Threats Could Lead to Costly Data Breaches. URL: https://securityintelligence.com/these-5-types-of-insider-threats-could-lead-to-costly-data-breaches.*
21. *Insider Threats: In the Healthcare Sector.*

URL: https://www.cisecurity.org/blog/insider-threats-in-the-healthcare-sector.

22. *PoulsenK.Leader of hacker gang sentenced to 9 years for hospital malware.*

URL: https://www.wired.com/2011/03/ghostexodus-2.

23. *Former security guard, who hacked into hospitals computer system, is sentenced to 110 months in federal prison. Defendant Posted Video of Himself Compromising a Hospitals Computer System on YouTube.*

URL: https://www.justice.gov/sites/default/files/ criminal-ccips/legacy/2012/03/15/mcgrawSent.pdf.

24. *Morgan S.Why healthcare cybersecurity spending will exceed $65B over the next 5 years. Hospitals and healthcare providers remain under cyber attack, causing organizations to spend more to protect their systems and patient data. URL: https: // www.csoonline.com/article/3252343/cyber-attacks-espionage/why-healthcare-cybersecurity-spending-will-exceed-65b-over-the-next-5-years.html.*
25. *About Panda Security.*

URL: https://www.pandasecurity.com/ukraine/company-profile.

26. *Ilyk R. Farmpolityka 2019. Tsili ta novi vyklyky. Stratehiia likarskykh zasobiv do 2025. Aptechnyi samit Ukrainy — 2018 : materialy prezentatsii. Kyiv. 06.12.2018.*

URL : C:\Users\user\AppData\Local\Temp\Rar$DI07.255.2-¦Sh¦¬TL.pdf.

27. *Pro derzhavni finansovi harantii medychnoho obsluhovuvannia naselennia : Zakon Ukrainy vid 19.10.2017 r. № 2168-VIII. Vidomosti Verkhovnoi Rady Ukrainy. 2018. № 5. St. 5.*
28. *Deiaki pytannia elektronnoi systemy okhorony zdorovia : postanova Kabinetu Ministriv Ukrainy vid 25.04.2018 r. № 411. Ofitsiinyi visnyk Ukrainy. 2018. № 46. St. 14.*
29. *Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data.*
URL : https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168093b26e.
30. *Protection of health-related data: Council of Europe issues new guidelines. URL: https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=090000168093b57d.*

Надійшла до редакції 23.03.2019 року

Волынец И. Киберпреступность в сфере здравоохранения: реальность, которая требует защиты. В статье рассмотрены проблемные вопросы противодействия киберпреступности как потенциальной угрозе в сфере здравоохранения. Раскрыто содержание понятий «киберпреступление» и «киберпреступность»; обозначены причины и последствия влияния кибератак. В соответствии с характеристикой видов киберпреступлений приведены примеры осуществления кибератак в сфере здравоохранения. Проведен анализ нормативно-правовых актов по данной проблематике. Определены возможные угрозы информационной безопасности Украины. Подчеркнута важность теоретического и практического совершенствования мер противодействия кибератакам в соответствии с современными иностранными наработками борьбы с киберпреступностью и защитой персональных данных, а также имплементации на законодательном уровне руководящих принципов защиты данных.

Ключевые слова: киберпреступность, хакер, кибератаки, здравоохранение, защита персональных данных, кибербезопасность, реестр

Volynets I. Cybercrime in health care: demand for protection. The study aimed to analyze problems of countering cybercrime as a potential threat for healthcare. The scope of the term «cybercrime» is provided. The causes and consequences of the influence of cyberattack are identified. Legislation of Ukraine on information threat protection was analyzed. Examples of cyberattack in health care are provided in accordance with types characteristics of cybercrime (ransomware, denial-of-service attack (DoS attack), Insider Threats etc.).

Since the beginning of the realization of electronic healthcare system in Ukraine, there is a certain possibility of a threat for information security. The importance of theoretical and practical improvement of counteraction against cyberattacks is argued in compliance with modern foreign practices in combating cybercrime and personal data protection.

The relevance of implementation of data protection guidelines at the legislative level is noted. Recommendation CM/Rec (2019) 2 of the Committee of Ministers to member States on the protection of health-related data was studied in relation to its implementation to national legislation.

Keywords: cybercrime, computer hacker, cyberattacks, healthcare, personal data protection, cybersecurity, register