family members; by prevention of family violence. To reach this aim we conduct coordination work between law enforcement agencies, social services, medical and educational institutions, non-governmental organizations within a single strategy for liquidation and prevention of domestic violence. The problem of child abuse in the family has a multidimensional nature. This stipulates the need of a multidimensional, integrated approach to the problem solving. The effectiveness of such an integrated assistance is its coordination, which should be entrusted to social services.

Keywords: violence, children, family, prevention, counteraction.

УДК [004:343.3/.7](477)
В. В. Марков

ХАКЕРСЬКІ АТАКИ НА ІМПЛАНТАТИ ЯК ОДИН ІЗ СПОСОБІВ ПРОТИПРАВНОГО ВИКОРИСТАННЯ КІБЕРПРОСТОРУ: СУТНІСТЬ ТА ВИДИ

З правових позицій проаналізовано сутність кіберпростору як середовища здійснення хакерських атак, визначено об'єкти атак, сутність і види хакерських атак на імплантати. Актуальність зумовлена відсутністю будь-яких правових досліджень в Україні щодо розгляду вразливостей імплантованих медичних пристроїв та їх захисту від хакерських атак. Проблеми попередження хакерських атак потребують розробок як з боку фахівців у юриспруденції, так і з боку спеціалістів у сфері комп'ютерних технологій та захисту інформації.

Ключові слова: імплантація, імплантований медичний пристрій, хакерська атака, кіберпростір, захист інформації.

Технології застосування сучасних засобів комп'ютерної техніки у різних сферах суспільної діяльності на сьогоднішній день здатні не лише автоматизувати працю людини, збільшивши при цьому її продуктивність, але й врятувати їй життя. Так, у світі вже набуло поширення використання діагностично-консультативних систем, комп'ютерної томографії, апаратів для радіохірургії тощо. Відомо, що різноманітні медичні пристрої (далі – МП) розробляються та використовуються з метою моніторингу змін у здоров'ї пацієнта та можуть бути як «зовнішніми», так і імплантованими. Актуальним і затребуваним на даний час, але малозастосовним в Україні через велику вартість як матеріалу, так і операції, є власне імплантація МП в тіло людини.

Слід звернути увагу на те, що впровадження безпроводових технологій у мережі медичних закладів та безпроводове використання МП відкриває як нові можливості, так водночас і продукує нові виклики для медичних закладів і для пацієнтів. Не вдаючись до дискусії щодо технічних деталей процесів зберігання та передачі

інформації в галузі охорони здоров'я, зазначимо, що раціональне вирішення питання доступу до інформації полягає у використанні саме безпроводових технологій, зокрема доступ до баз даних, які містять інформацію про пацієнта, про стан його здоров'я, про ліки, які йому призначаються тощо, можна вже отримати через МП. Якщо розглядати негативні явища, які породжує такого роду нововведення, то виділимо наступні загрози: з одного боку, крадіжка медичної інформації, з іншого – можливість віддаленого підключення до МП та управління ним з метою заподіяння шкоди життю та/або здоров'ю людини.

Враховуючи наведене, мета цієї роботи полягає в тому, щоб на основі дослідження теоретичних і практичних здобутків вітчизняних і зарубіжних вчених у галузі інформаційної безпеки та захисту інформації проаналізувати сутність кіберпростору як середовища здійснення віртуальних атак, визначити об'єкти злочинного посягання, сутність та види одного з нових способів здійснення правопорушень з використанням кіберпростору – хакерських атак на імплантати.

Зазначимо, що будь-які теоретичні дослідження питань попередження, розкриття та відповідальності щодо протиправного використання кіберпростору з метою здійснення хакерських атак на імплантати в Україні відсутні. Тому вважаємо за необхідне використовувати здобутки зарубіжних вчених у цій сфері. Серед науковців, які у своїх роботах торкалися окремих аспектів нашої проблематики, слід згадати Марка Гордона, Джерома Редкліфа, Катерину Базаку, Мохана Якоба, Вілліама Масела, Тадайоши Коно, Джансі Слоба та ін.

На нашу думку, дослідження цього проблемного питання доцільно умовно розділити на дві частини – перша частина буде присвячена аналізу так званої «медичної» складової проблеми задля кращого розуміння об'єкта посягання, а друга – характеристиці «середовища» для хакерських дій і самих атак. Отже, визначимо логічну послідовність аналізу кожної з названих частин: спочатку схарактеризуємо поняття та мету імплантації МП, які можуть зазнати протиправних хакерських зломів, та загрози, пов'язані з використанням імплантатів; після цього розглянемо поняття та ознаки кіберпростору як підґрунтя для появи нового виду протиправної дії у вигляді хакерських атак на імплантати, і на завершення визначимо сутність хакерських атак на імплантати з метою усунення неоднозначності в розумінні цього явища та узагальнимо їх різновиди у кіберпросторі стосовно імплантованих МП.

Аналіз чинних нормативно-правових актів за обраним напрямком дослідження дозволяє стверджувати, що вітчизняне законодавство не дає визначення поняття «імплантат», однак згадка про нього є, наприклад, в Інструкції про порядок медичного забезпечення у Службі безпеки України [1], Законі України «Основи законодавства

України про охорону здоров'я» [2], Постанові Кабінету Міністрів України від 09.11.2004 № 1497 «Про затвердження Порядку державної реєстрації медичної техніки та виробів медичного призначення» [3] тощо. Слід зазначити, що у березні 2013 р. уряд Киргизької Республіки вже затвердив Технічний регламент «Про безпеку медичних імплантатів» [4], в якому надано змістовне та поділене за видами імплантації визначення поняття «імплантат».

Відповідно до названого регламенту [4]:

– імплантація – це введення в організм людини імплантату для заміщення або корекції функції органів чи систем організму на тривалий період часу або довічно (ч. 10 п. 6);

– медичні імплантати – вироби медичного призначення, що контактують з наступними тканинами внутрішнього середовища організму: з кісткою; з м'якими тканинами і міжклітинною рідиною; з кров'ю (ч. 11 п. 10);

– вироби медичного призначення – прилади, апарати, інструменти, пристрої, комплекси, системи з програмними засобами, обладнання, запасні частини та приладдя до них, пристосування, перев'язувальні й шовні засоби, стоматологічні матеріали, набори реагентів, контрольні матеріали і стандартні зразки, калібратори, витратні матеріали, вироби з полімерних, гумових та інших матеріалів, програмне забезпечення, які застосовують у медичних цілях окремо або в поєднанні між собою і які призначені для:

– профілактики, діагностики, у тому числі in vitro, лікування захворювань, реабілітації, проведення медичних процедур, досліджень медичного характеру, заміни та модифікації частин тканин, органів людини, відновлення або компенсації порушених або втрачених фізіологічних функцій, контролю над зачаттям;

– впливу на організм людини таким чином, що їх функціональне призначення не реалізується шляхом хімічної, фармакологічної, імунологічної або метаболічної взаємодії з організмом людини, спосіб дії яких може підтримуватися такими засобами (ч. 9 п. 10).

Слід зауважити, що найбільш докладну класифікацію видів МП, які імплантуються у тіло людини, подано в роботі німецьких дослідників, присвяченій інфекціям, пов'язаним з МП [5].

Отже, аналізуючи відповідну літературу [6–12], можна дійти висновків, що мета імплантації МП у тіло людини полягає у наступному:

– визначення місця розташування особи;

– контроль за загальним станом здоров'я особи;

– стимулювання серцевої функції в критичній ситуації;

– самозахист;

– ідентифікація особи;

– автоматизована доставка необхідної дози інсуліну до організму тощо.

Доречно зауважити, що до об'єктів, які можуть зазнати злому з боку хакерів, можна віднести наступні:

– інсулінові помпи;

– дефібрилятори;

– кохлеарні імплантати;

– серцево-судинні монітори;

– штучні бета-клітини тощо [5].

Визначивши поняття та мету вживлення імплантату, а також короткий перелік імплантованих у тіло людини об'єктів, вразливих до хакерських атак, вважаємо за доцільне коротко зупинитися на загрозах різного походження, пов'язаних із використанням імплантатів, у тому числі пов'язаних з кіберпростором:

– перебій у роботі чипа імплантату;

– комп'ютерний вірус;

– атака кібертерористів (наприклад, перехват радіосигналу імплантату з наступним його протиправним використанням);

– втрата частина тіла, в яку було вшито імплантат;

– перебій у роботі програмного забезпечення, під управлінням якого працює чип імплантату;

– атака хакерів на базу даних про стан здоров'я людини через імплантований МП, оскільки імплантат не підтримує шифрування даних через необхідність економії заряду акумулятора тощо [6–12].

Таким чином, підбиваючи підсумки першої, «медичної» частини нашого дослідження, зазначимо, що на сьогоднішній день, по-перше, в Україні відсутнє правове регулювання порядку імплантації МП в тіло людини та їх захисту від кібернетичних та будь-яких інших загроз (для порівняння, у США регулювання питань, пов'язаних з імплантованими МП, покладено на Управління санітарного нагляду за якістю харчової продукції та медикаментів і Центр радіологічної безпеки); по-друге, враховуючи розповсюдження бездротових технологій передачі даних, множинність МП, які можуть бути імплантовані в тіло людини, та зростаючий інтерес з боку хакерів до протиправного використання кіберпростору, все більшої актуальності набувають питання дослідження вразливостей імплантованих МП з метою попередження атак на них.

Переводячи наші дослідження у площину визначення поняття кіберпростору як основного фактора, який став джерелом розвитку не тільки окремих хакерських атак на імплантовані МП, але й для кібертероризму, вважаємо за доцільне назвати тих українських і російських вчених, роботи яких присвячені саме цій тематиці. Серед них С. В. Бондаренко, В. Д. Гавловський, В. О. Голубєв, Й. М. Дзялошинський, О. В. Манжай, М. А. Погорецький, В. П. Шеломенцев, М. Ю. Яцишин та ін.

Як слушно зауважує М. Ю. Яцишин, «поява кіберпростору як особливого середовища існування людини уже призвела до зміни у соціумі архетипів, ритмів функціонування, естетичних образів,

моделей економічної діяльності та форм соціальних взаємодій… Таким чином, з виникненням кіберпростору виникли й нові виміри у проблематиці прав людини» [13].

Здійснивши аналіз поняття «кіберпростір», М. Ю. Яцишин підкреслює, що «…цей термін можна зустріти в деяких міжнародно-правових актах, національних джерелах права (переважно англоамериканської правової сім'ї), а також в доктринальних працях зарубіжних та вітчизняних науковців. Водночас, його застосування є достатньо умовним і суперечливим, немає чітких загальноприйнятих рамок, а також часто пов'язується чи ототожнюється з поняттями: «інформаційний простір», «віртуальний простір», «комп'ютерна сфера», «Інтернет», «інформаційно-комунікаційні системи і мережі». Усі зазначені поняття є достатньо складними та багатоаспектними і складають предмет самостійного наукового дослідження…» [13]. На таке ж розмаїття підходів до визначення поняття «кіберпростір» звертає увагу і вітчизняний вчений О. В. Манжай, досліджуючи можливості використання кіберпростору для здійснення оперативно-розшукових заходів [14].

Підкреслюючи основні ознаки кіберпростору, О. В. Манжай виділяє серед них наступні: це, по-перше, інформаційний простір, по-друге, комунікативне середовище, по-третє, утворюється за допомогою технічних систем [14]. Таким чином, він визначає кіберпростір з урахуванням інформаційної складової як «…інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами» [14]. У свою чергу, М. Ю. Яцишин пропонує зовсім інший підхід, акцентуючи увагу на правовій складовій, зазначаючи, що «…це поле чи середовище, пов'язане із комп'ютерною технікою, системами та мережами, в рамках якого виникають, змінюються або припиняються правовідносини» [13].

Узагальнюючи існуючі підходи до визначення поняття «кіберпростір», відстоюємо позицію, що обидва наведені визначення є справедливими і доповнюють одне одного.

Отже, визначивши, що собою представляє кіберпростір як середовище для здійснення протиправних дій щодо імплантованих МП, перейдемо безпосередньо до розгляду суті хакерської атаки на імплантати, тобто проаналізуємо, в чому проявляється така дія і через які умови можливе її існування.

За останні роки розповсюдженість імплантованих МП пояснюється їх широким використанням для лікування аритмії, діабету та хвороби Паркінсона [6]. При цьому слід зазначити, що кількість різновидів атак на імплантовані МП не може бути розрахована через велику кількість як самих різновидів МП, які імплантуються, так і через різноманітність підходів, які можуть застосувати хакери,

атакуючи один і той же МП. Тому вважаємо за доцільне розглянути декілька прикладів для розкриття сутності хакерських атак на імплантовані МП та усвідомлення їх небезпеки для життя та/або здоров'я людини.

Так, наприклад, електричний дефібрилятор серця містить у собі магнітний перемикач (або сенсор), який активується достатньо потужним магнітним полем. Такого типу доступ не вимагає будь-якої ідентифікації, тому є небезпечним. Вразливості в комунікаційному інтерфейсі безпроводового імплантованого МП, яке може бути перепрограмоване, дозволяють хакерам управляти функціями МП, не перебуваючи поблизу від нього [6]. Як інший приклад можна назвати те, що сьогодні ряд мобільних телефонів мають функцію зчитування даних з імплантованого МП (так звані Implantable Medical Devices Readers – IMD-readers). За таких умов хакери можуть дуже легко здійснити несанкціоноване пасивне перехоплення інформації без її зміни [6]. Слід звернути увагу на те, що в ролі хакерів можуть виступати і страхові компанії. Встановлюючи IMD-readers на вході у будівлю, вони отримують усю приватну інформацію з імплантованих МП людини, коли вона проходить біля зчитувача даних [6]. Також слід назвати ще один з видів хакерських атак на імплантовані МП – «виснаження ресурсів» [6]. Суть цієї атаки полягає в тому, що вичерпуються ресурси батареї імплантованого МП, і якщо працездатність МП розрахована на кілька років, то після такої атаки заряду батареї вистачає на кілька місяців. Слід зауважити, що метою хакерських атак може бути також впровадження комп'ютерного віруса у програмне забезпечення імплантованого МП.

Наведені приклади свідчать про те, що потенційна загроза хакерських атак на імплантовані МП може бути більшою за вигоду, яку отримали люди з їх винаходом. Через наведені приклади простежується мета хакерських атак – заподіяння шкоди здоров'ю або навіть життю особи та несанкціонований доступ до особистих даних з подальшим їх використанням у своїх злочинних намірах (наприклад, вимагання, шантаж тощо). Слід підкреслити, що в Масачусетському технологічному інституті дослідники вже почали розробляти технічні пристрої для захисту імплантованих МП від атак, і першим рішенням цієї проблеми стало впровадження генератора перешкод, який людина має носити із собою задля блокування сигналів хакерів [15]. На жаль, в Україні до теперішнього часу не проведено жодного правового дослідження вразливостей імплантованих МП з метою попередження атак на них, як і питання технічного захисту імплантованих МП від хакерських атак залишилося поза увагою фахівців у галузі інформаційної безпеки та захисту інформації.

Таким чином, проблема попередження здійснення хакерських атак на імплантовані МП як один із способів протиправного використання кіберпростору потребує подальших досліджень як з боку фахівців у галузі юриспруденції, так і з боку спеціалістів у сфері комп'ютерних технологій та захисту інформації.

Список використаних джерел: **1.** Про затвердження Інструкції про порядок медичного забезпечення в Службі безпеки України : наказ Служби безпеки України від 8 жовт. 2007 р. № 718 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z1238-07. **2.** Основи законодавства України про охорону здоров'я : закон України від 19 листоп. 1992 р. // Відомості Верховної Ради України. – 1993. – № 4. – Ст. 19. **3.** Про затвердження Порядку державної реєстрації медичної техніки та виробів медичного призначення [Електронний ресурс] : постанова Кабінету Міністрів України від 9 листоп. 2004 р. № 1497. – Режим доступу: http://zakon.rada.gov.ua/laws/show/1497-2004-п/paran9#n9. **4.** Об утверждении Технического регламента «О безопасности медицинских имплантатов» [Електронний ресурс] : постановление Правительства Кыргызской Республики от 05 мар. 2013 г. – Режим доступу: http://base.spinform.ru/show_doc.fwx?rgn=58531. **5.** Infections Associated with Medical Devices Pathogenesis, Management and Prophylaxis [Електронний ресурс] / Christof von Eiff, Bernd Jansen, Wolfgang Kohnen, Karsten Becker. – Режим доступу: http://www.iqg.com.br/pbsp/img_up/01318871858.pdf. **6.** Defending Resource Depletion Attacks on Implantable Medical Devices [Електронний ресурс] / Xiali Hei, Xiaojiang Du, Jie Wu, Fei Hu. – Режим доступу: http://www.cis.temple.edu/~wu/research/publications/Publication_files/Defending%20Resource%20Depletion%20Attacks%20on.pdf. **7.** Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System [Електронний ресурс]. – Режим доступу: http://cs.uno.edu/~dbilar/BH-US-2011/materials/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf. **8.** IMDGuard: Securing Implantable Medical Devices with the External Wearable Guardian [Електронний ресурс]. – Режим доступу: http://www.cs.wm.edu/~fxu/data/imd-infocom.pdf. **9.** Maisel W. H. Improving the Security and Privacy of Implantable Medical Devices [Електронний ресурс] / William H. Maisel, Tadayoshi Kohno – Режим доступу: http://homes.cs.washington.edu/~yoshi/papers/IMD/NEJM-Maisel-Kohno.pdf. **10.** Slobbe J. On Security of Implantable Medical Devices : master thesis for obtaining the master of science degree at the TU/e [Електронний ресурс] / J. Slobbe. – Режим доступу: http://alexandria.tue.nl/extra1/afstversl/wsk-i/slobbe2013.pdf. **11.** Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses [Електронний ресурс] / Daniel Halperin, Thomas S. Heydt-Benjamin and oth. – Режим доступу: http://www.secure-medicine.org/public/publications/icd-study.pdf. **12.** Goodman M. Who Does the Autopsy? Criminal Implications of Implantable Medical Devices [Електронний ресурс] / Marc Goodman. – Режим доступу: https://www.usenix.org/legacy/event/healthsec11/tech/final_files/goodman-healthsec11.pdf. **13.** Яцишин М. Ю. Актуальні проблеми захисту прав людини у кіберпросторі [Елетронний ресурс] / Яцишин М. Ю. – Режим доступу: http://er.nau.edu.ua/bitstream/NAU/2030/1/Тези_Яцишин%20М._Ужгород.pdf. **14.** Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності [Електронний ресурс] / О. В. Манжай // Право і безпека. –2009. – № 4. – Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/pib/2009_4/ РВ-4/РВ-4_48.pdf. **15.** Взлом человека: имплантаты как цель атаки [Електронний ресурс]. – Режим доступу: http://www.chip.ua/novosti/2012/07/ vzlom-cheloveka-implantaty-kak-cel-ataki/.

Надійшла до редколегії 12.07.2013

Марков В. В. Хакерские атаки на имплантаты как один из способов противоправного использования киберпространства: сущность и виды

С правовых позиций проанализирована сущность киберпространства как среды осуществления хакерских атак, определены объекты атак, сущность и виды хакерских атак на имплантаты. Актуальность определяется отсутствием каких-либо правовых исследований в Украине по изучению уязвимостей имплантированных медицинских устройств и их защиты от хакерских атак. Проблемы предупреждения хакерских атак требуют разработки как со стороны специалистов в юриспруденции, так и со стороны специалистов в области компьютерных технологий и защиты информации.

Ключевые слова: имплантация, имплантированное медицинское устройство, хакерская атака, киберпространство, защита информации.

Markov V. V. Hacker Attacks on Implants as One of the Ways of Illegal Use of Cyberspace: the Essence and Types

This paper is devoted to the analysis of cyberspace's essence as surroundings of hacker attacks, to identification of hacker attacks' objects, to the essence and types of hacker attacks on implants. The urgency is determined by the absence of any research in Ukraine studying the vulnerability of implanted medical devices, and their protection from hacker attacks. Legislative definition of the notion of implantation and implant is examined. The purposes of medical devices' implantation, hacker attacks' objects in the form of implanted medical devices, threats of various origins associated with implantation, including cyber threats are also examined.

It is stressed that Ukraine hasn't got legal regulation of the implantation order of medical devices in the human body and their protection from cyber and any other threats.

The characteristic of cyberspace stating its properties as surroundings for the development of either hacker attacks on the implants or formation of cyber-terrorism is presented. The author's position on the definition of cyberspace as an information and communication surroundings created by the assistance of computer tools is expressed. Legal relations may appear, vary or be terminated there.

Some types of hacker attacks on implanted medical devices, which provide an idea about the essence, methods, and purposes of these actions – doing harm to person's life and/or health, unauthorized access and receipt of personal data, which are used later in a criminal purposes, are presented in the article basing on the analysis of foreign literature sources.

The author has made a proposition that prevention of hacker attacks requires the development of both experts in the field of law, and experts in the field of computer technology and information security.

Keywords: implantation, implanted medical device, hacker attack, cyberspace, information protection.