УДК 666.13

В.В. Ковальчук
Є.О. Кобилянський

ТЕНДЕНЦІЇ ЗАХИСТУ ВІД КІБЕРЗЛОЧИНІВ

Вінницький національний технічний університет

В статті розглянуто стан нинішньої ситуації кібербезпеки у світі, яка вимагає постійного вдосконалення методів боротьби з кіберзлочинністю.
Ключові слова: кіберзлочинність; кібербезпека; захист.

TRENDS IN PROTECTION AGAINST CYBERCRIME

The article examines the state of the current situation of cyber security in the world, which requires continuous improvement of methods of combating cybercrime.
Keywords: cybercrime; cyber security; protection.

Кіберзлочинність є явищем міжнародного значення. Вона включає в себе різні види злочинів, що здійснюються за допомогою комп'ютера і в мережі Інтернет. В останні роки набувають значного поширення такі кіберзлочини : організація азартних ігор (казино, лотерей, інтернет-аукціонів), використання віртуальних крамниць і фірм, що надають платні послуги з вилученням з рахунків і кредитних карток їх власників «електронних» грошей; фінансових пірамід, шлюбних агентств і т. п. шахрайств з викраденням грошових коштів обманутих громадян; комп'ютерне «піратство» (порушення авторських прав на програмне забезпечення) [1]. Кібертероризм є серйозною соціально-небезпечною загрозою для людства, у порівнянні, навіть, з ядерною, бактеріологічною і хімічною зброєю. Досвід, що є у світової спільноти у цій сфері, зі всією очевидністю свідчить про безперечну уразливість будь-якої держави.

Із появою модемного зв'язку, глобальних мереж й Інтернету загрозу почала становити недозволена взаємодія із системою третіх осіб, хоча при цьому система може виконувати свої функції у відповідності до намірів та очікувань її авторів та власників. Найчастіше під ударами кібератак опиняються об'єкти критичної інфраструктури: енергетичні об'єкти, транспорт та банківський сектор. Явним прикладом слугують кібератаки на енергетичні компанії України(2015-2016) , в ході яких , на декілька годин, залишились без електроенергії декілька областей [2]. Як бачимо ,протистояти фізичному руйнуванню технічних засобів, порушенню функціонування об'єктів нападу, а також протиправній діяльності соціальних інженерів в умовах збільшення кібервтручань з дня на день стає все важче.

В Україні, з метою захисту інформаційних та комунікаційних мереж, а також боротьбою із кіберзлочинністю функціонує новостворений Департамент кібербезпеки України. [3]. Кожен з підрозділів вживає заходи щодо безпеки і веде статистику відповідних показників, проте їхня діяльність охоплює тільки окремі власні сфери відповідальності. Як свідчать результати досліджень, питання кібертероризму непокоїть не тільки державу в цілому, а й кожного окремо взятого її мешканця [4].

Належний захист від кіберзлочинців першочергово залежить від самих громадян, які дуже часто легковажно та необережно відносяться до електронних платежів і своїх персональних даних. Саме персональні дані, які ви надаєте банку, є найбільш затребуваними шахраями, а саме: прізвище та ім'я, номер мобільного телефону, адреса електронної пошти. Зазвичай таку інформацію продають на «чорному» ринку, а згодом використовують для розсилок смс, спаму, телефонних дзвінків рекламного характеру. Дуже часто зазначені дані перехоплюються в публічних місцях із відкритим Wi-Fi доступом під час користування електронною поштою або соціальними мережами. У цьому разі спеціалісти радять користуватися засобами захисту інформації, які пропонуються поштовими серверами або соціальними мережами [5].

Що стосується банківського сектору, то необхідно дотримуватися декількох простих правил щодо безпеки з користування платіжними картками. По-перше, не слід давати стороннім у руки свою

платіжну картку, навіть офіціантові в ресторані, адже вони можуть переписати номер вашої картки або сфотографувати її та згодом використати у протиправних діях. По-друге, ніколи не носити разом із карткою PIN-код, краще таку інформацію тримати в пам'яті, також радять час від часу змінювати PIN-код. Останнім часом поширилося викрадення особистих даних з банкоматів. Таких шахраїв називають «кардери». Вони встановлюють на банкомати спеціальні пристрої: скіммери і накладки. Перший приклеюють на карткоприймач банкомату, другий – на клавіатуру. В їх приладах вмонтовані спеціальні передавачі, які пересилають всю отриману інформацію на мобільний телефон чи електронну пошту. В їхньому арсеналі є інші пристрої, які записують зчитану інформацію на іншу картку з магнітною стрічкою [6]. Шахраю достатньо потримати у руках чужу картку, і він перепише її номер та цифри CV-коду, нанесені на зворотному боці. Цих даних вистачить, щоб здійснити будь-який онлайн платіж. Наприклад, здійснити покупку в інтернет-магазині .

Фахівці з IT-безпеки радять прикривати долонею цифри коду, які ви вводите у банкомат, оскільки поряд може бути вмонтовано злочинцями відеокамеру. Серед організаційних заходів пропонується користуватися послугами смс-інформування та установити ліміт на використання грошових коштів, а також надати банку телефон, за яким із вами можна швидко зв'язатися. Якщо в банку помітять незвичайну для вас транзакцію або надмірне використання коштів, вам зателефонують і запитають чи справді ви виконуєте зазначені дії, якщо ні, то картка блокується, а ваші кошти залишаються на рахунку та в безпеці. У разі використання дистанційного обслуговування придбайте надійну антивірусну програму та не забувайте її оновлювати [7].

На сьогоднішній день у багатьох зарубіжних країнах налагоджена система співробітництва та обумов- лена необхідність обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністю на ключові позиції. Для України така тенденція є, в цілому, позитив- ною: поки власна стратегія щодо захисту кіберпростору тільки розробляється, надзвичайно цінною є можливість ознайомлення з досвідом країн, які працюють в зазначеному напрямку не перший рік.

У2016 році відбувся значний прогрес у сфері кібербезпеки , зокрема на інституційно-організаційному рівні: у березні 2016 року уряд прийняв Стратегію кібербезпеки України, яка має на меті створення національної системи кібербезпеки; у червні 2016 року Президент України підписав Указ про створення Національного координаційного центру кібербезпеки [8].

Висновки

Протидія кіберзлочинності та рівень кібербезпеки на сьогодні є одним із пріоритетних напрямків в політиці країни. На жаль, кіберзлочинність постійно удосконалюється і йде в ногу з технологіями, що, у свою чергу, ускладнює виявлення та супротив зазначеним протиправним діям. Завдання кожного громадянина для власної безпеки ¬– бути пильним і ставитись до своїх персональних даних і платіжних карток із особливою обережністю та уважністю. Але для комплексної боротьби з цією проблемою потрібні спільні зусилля держави, громадян та міжнародної спільноти.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Скопа, О. О.Роль телекомунікацій в сучасному бізнесі [Текст] / О. О. Скопа, Н. Ф. Казакова // Нау- кові праці УДАЗ. – Одеса : УДАЗ. − 1999. – № 2. – С. 11-12.

2. Кібератака на енергетичні компанії України [Електронний ресурс]. // Режим доступу : https://uk.wikipedia.org/wiki/Кібератака_на_енергетичні_компанії_України .

3. Йона, О. О. Світові тенденції боротьби з кіберзлочинністю [Текст] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ : СНУ ім. В. Даля. – 2013. − № 15(204). – Ч. 1. − С. 59-62.

4. Інформаційні злочини [Електронний ресурс]. // Режим доступу:https://uk.wikipedia.org/wiki/Інфор-маційні_злочини.

5. Щербина, Ю. В. Принципи вибору формальних параметрів при побудові профілей захисту інфо-ресурсів [Текст] / Ю. В. Щербина, С. Л. Волков, О. О. Скопа // Восточно-Европейский журнал пе-редовых технологий. – Х. : Технологический центр. – 2012. − № 5/2(59). – С. 31-33.

6. Курсы по кибербезопасности. Методы современных киберпреступников и защита от них [Електронний ресурс]. // Режим доступу : https://www.youtube.com/watch?v=uiTvorc6d5c.

7. Три способа украсть деньги с карты и защита от них [Електронний ресурс]. // Режим доступу : https://www.youtube.com/watch?v=Z2hYYnR50nY.

8. Соціальна інженерія: виклики та перспективи боротьби в українському контексті [Електронний ресурс]. // Режим доступу :http://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain/?month=12&year=2017.

Ковальчук Вілена Валентинівна, студентка групи 1БС-16б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vilenca.kanfetca@gmail.com
Кобилянський Євгеній Олександрович, асистент кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: jen4yen @gmail.com

Kovalchuk Vilena V. , student of the group 1SS-16b, department of Information Technologies and Computer Engineering Vinnytsia National Technical University, Vinnitsa, e-mail: vilenca.kanfetca@gmail.com
Kobylyanskiy Eugene O., Assistant of Department of Health and Safety Studies, Vinnitsa National Technical University, Vinnytsia, e-mail: jen4yen@gmail.com.

УДК 681.3

В. В. Монастирська

ФІТНЕС-БРАСЛЕТИ – ЗРУЧНИЙ КОНТРОЛЬ ОСОБИСТОГО СТАНУ ЗДОРОВ'Я

Вінницький національний технічний університет

В статті подано огляд характеристик та функцій фітнес-браслетів. Розглянуто використання даних новітніх технологій у повсякденному житті людини, зокрема – при спостереженні за самопочуттям людини. Зроблено загальний висновок.
Ключові слова: новітні технології, фітнес-браслет, здоров'я, самопочуття.

FITNESS BRACELETS - COMFORTABLE CONTROL OF YOUR PERSONAL HEALTH

Abstract: The article gives an overview of the features and functions of fitness bracelets and smart watches. The usage of the data of the newest technologies in the everyday life of a person is considered, in particular - when observing the state of health of a person. Make a general conclusion.
Keywords: new technologies, fitness bracelet, health, well-being.

Комп'ютери та електронні гаджети міцно увійшли в наше життя і змінили його. Щорічно з'являються і розробляються технологічні новинки, що поліпшують якість повсякденного життя людини. З появою таких технологій наше життя стало набагато комфортнішим. Розвивається тенденція збільшення багатофункціональності речей, що оточують людину. Мобільні телефони, наприклад, перестали нести свою функцію тільки лише як засоби зв'язку – їх функціонал зріс практично до рівня персональних комп'ютерів. Розробляються гаджети, які здійснють контроль у режимі реального часу фізіологічних показників людини; системи безпеки, які працюють з персональною інформацією за допомогою дактилоскопічного доступу, датчики, які використовують для відстежування [1].

Зупинимось на фітнес-браслетах, які останнім часом стали дуже популярними як серед дорослих, так і серед дітей.

Фітнес-браслет – наручний пристрій з мінімальним екраном або зовсім без нього.

Здоров'я є головною цінністю в житті кожної людини. Це начебто і зрозуміло, але цінувати його починаєш тільки тоді, коли виникають проблеми. І добре, що сьогодні люди починають розуміти, наскільки важливо дбати про своє здоров'я і профілактикою хвороб. Все більше людей стають на шлях здорового способу життя, не з чуток знають, що таке детокс, правильне харчування і спорт.

Фітнес-браслети стають у нагоді при контролі за своїм самопочуттям, фізичною активністю та