© Marushchak A., Skitsko O. The influence of Shadow Information Technology on the cyber security of business entity // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 1, p. 69-74.

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ БЕЗПЕКИ ІНФОРМАЦІЇ / ORGANIZATIONAL & LAW INFORMATION SECURITY

DOI: 10.18372/2225-5036.24.12310

ВПЛИВ ТІНЬОВИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ СУБ'ЄКТА ГОСПОДАРЮВАННЯ

Анатолій Марущак, Олексій Скіцько

Національна академія Служби безпеки України

МАРУЩАК Анатолій Іванович, д.ю.н.

Рік та місце народження: 1977 р., с.м.т. Ставище, Київська область, Україна.
Освіта: Національна академія СБ України, 1999 р.
Посада: директор Інституту НА СБ України.
Наукові інтереси: інформаційне право та інформаційна безпека.
Публікації: більше 160 наукових публікацій, серед яких монографії, підручники, навчальні посібники, наукові статті, матеріали і тезиси доповідей на наукових конференціях і інше.
E-mail: martol_law@ukr.net

СКІЦЬКО Олексій Іванович, к.т.н.

Рік та місце народження: 1980 рік, м. Київ, Україна.
Освіта: КВІУЗ НТУ «КПІ», 2002 рік.
Посада: завідувач кафедри Інституту НА СБ України.
Наукові інтереси: інформаційна безпека, захист інформації, фізика.
Публікації: більше 50 наукових публікацій, серед яких підручники, наукові статті, матеріали і тезиси доповідей на наукових конференціях.
E-mail: vidocq2002@ukr.net

Анотація. *Інформаційна безпека стала невід'ємною складовою національної безпеки й водночас важливою самостійною сферою забезпечення безпеки суб'єктів господарювання. На сьогодні інформаційні простір, інфраструктура та технології значною мірою впливають на рівень і темпи соціального, економічного та технічного розвитку. Тому успіх суб'єкта господарювання, гарантія отримання прибутку все більше стає залежною від збереження в таємниці секретів виробництва, що спирається на інтелектуальний потенціал і конкретну технологію. Співробітники зберігають дані на носимих пристроях - важлива корпоративна інформація стає доступною з будь-якого ноутбука, смартфона або планшета, який співробітник використовує в офісі або кафе. В статті здійснено аналіз загрози, що набирає все більших масштабів в інформаційній сфері і пов'язана з використанням мобільних або носимих пристроїв (wearable device) на робочому місці. Розроблено визначення «тіньові інформаційні технології» та приведена структура можливих місць прояву відповідної загрози.*

Ключові слова: *Shadow IT, Stealth IT, носимі пристрої, інформаційна безпека, суб'єкт господарювання.*

Постановка проблеми та аналіз останніх досліджень

Загрози, що впливають на інформаційну безпеку суб'єкта господарювання можуть бути зовнішніми і внутрішніми. Однією з таких внутрішніх загроз стало використання мобільних або носимих пристроїв на робочому місці. Мобільні пристрої стали не лише переворотом у розвитку інформаційних технологій, але і кардинально змінили життя сучасних людей. Сьогодні немає необхідності знаходитись в офісі, використання сучасних мобільних пристроїв – головним чином смартфонів та планшетів – дозволило людям отримувати віддалений доступ до своїх даних та пошти, спілкуватись на відстані у реальному часі та зберігати інформацію на віртуальних носіях. Проте розширення можливостей і

широкий спектр використання мобільних пристроїв призводить до появи нових загроз. А враховуючи, що ринок саме таких пристроїв є відносно молодим, то і програмних засобів для якісного адміністрування та захисту від вірусів та витоку даних є не достатньо. В основному проблемами захисту своїх мобільних пристроїв займаються виробники, що користуються базовими засобами захисту, які передбачені в сучасних операційних системах (iOS, Android, Windows Phone) [1].

Крім того за результатами аналізу наслідків вірусу-вимагача Petya, що атакував комп'ютерні системи по всьому світу, 27 червня 2017, Україна найбільше постраждала від нього, на її долю припало 75,24% випадків ураження. На Німеччину, що посіла друге місце за числом уражень, припадає лише 9,06% від їх загальної кількості. На третьому місці - Польща (5,81% випадків) [2].

Постраждалі від вірусу проігнорували можливість здійснити превентивні заходи. Причинами цього може бути як неуважність, так і використання в суб'єктах господарювання піратського програмного забезпечення, зокрема операційних систем. Крім цього, адміністратори мали б уважно відноситись до рекомендацій компаній і лабораторій, що працюють у сфері кібербезпеки. Першочергове зараження трояном WannaCry відбулося скоріше за все через неуважність або недостатню обізнаність персоналу суб'єктів господарювання з політикою інформаційної безпеки. Співробітники могли, наприклад, користуватись особистою поштою на робочому ПК чи відкрити вкладення в листах від невідомого адресата в корпоративній пошті, тим самим заразити комп'ютер. Порушення першочергових базових правил може говорити чи про те, що спрацював «людський чинник», або навіть про те, що про ці правила не було відомо персоналу суб'єкта господарювання.

Метою статті є аналіз теоретичних положень і практики діяльності суб'єктів господарювання та розробка визначення «тіньові інформаційні технології», приведення структури можливих місць прояву відповідної загрози. Наведено пропозиції щодо удосконалення діяльності підрозділів інформаційної безпеки суб'єктів господарювання у протидії несанкціонованому доступу до інформаційних ресурсів. Об'єкт дослідження – суспільні відносини та закономірності, які виникають у процесі діяльності працівників суб'єктів господарювання під час використання в роботі не зареєстрованих носимих пристроїв. Предмет дослідження – вплив тіньових інформаційних технологій на інформаційну безпеку суб'єкта господарювання.

Обсяг світового ринку носимих цифрових пристроїв (тільки типу розумних годинників, окулярів і носимих сканерів), які використовуються в компаніях, в 2017 році склала 10,6 млрд. дол., а в період 2017-2022 роках зростатиме із середньорічними темпами понад 41% і до 2022 року досягне 60 млрд. дол. [3].

Науковці розглядали проблематику впливу носимих цифрових пристроїв на забезпечення інформаційної безпеки на суб'єктах господарювання лише частково (А. Марущак [4], О. Корченко [5]).

Викладення основного матеріалу

Суб'єкти господарювання завжди шукають нові шляхи для збільшення продуктивності, і саме це забезпечують носимі при собі пристрої (. Однак зростання популярності і збільшення числа таких пристроїв в мережі підвищують ризики безпеки. Тому особливу роль в таких мережах починають відігравати рішення управління парком мобільних пристроїв підприємств (enterprise mobility management, EMM), впровадження яких дозволяє уникнути ризиків втрати будь-яких даних і забезпечує їх захист. Рішення EMM, що працюють на декількох рівнях забезпечення безпеки (на рівнях: пристрої, додатки і дані) є життєво-важливими для захисту даних, особливо при втраті або крадіжці пристрою або хакерському проникненні в нього.

Рішення EMM в контексті застосування їх для носимих пристроїв мають свої особливості, оскільки в останніх часто відсутня процедура аутентифікації і не підтримується аутентифікаційний протокол. Тому необхідна процедура забезпечення безпеки на цьому рівні. Доцільно інструктувати персонал суб'єкта господарювання, який використовує ці пристрої, що надсилання електронної пошти або підключення до сервера хоча і схожі на процедури для ПК, але відрізняються за рівнем захищеності, і без використання EMM несуть у собі певні ризики.

На ринку існують платформи безпеки EMM, що забезпечують захищеність носимих пристроїв, наприклад, пропоновані компаніями 42Gears, Augmate, Hipaax, SOTI і VMware [6]. Ці рішення підтримують всі протоколи захисту доступу, використовуючи аутентифікаційні протоколи, шифрування і віддалене керування пристроями (в тому числі для віддаленого видалення даних з пристрою і його блокування при втраті або крадіжці).

Однак таких заходів не достатньо без врахування дій користувачів (співробітників) суб'єкта господарювання [7]. Від використання методів соціальної інженерії не захистять жодні технічні засоби. Озброївшись знаннями з людської психології зловмисники надсилають небезпечні посилання на нову композицію улюбленої музичної групи чи направляють бухгалтеру лист з вкладенням «акт звірки», в якому насправді прихований вірус. Співробітникам необхідно передавати відповідальність за інформаційну безпеку (ІБ), навчати їх, контролювати і обов'язково давати зворотний зв'язок (і, якщо необхідно, то і передбачати відповідальність). Тобто всіляко розвивати культуру ІБ, заохочувати дбайливе і усвідомлене використання інформаційних активів.

Якщо цього не робити, то працівники будуть орієнтуватися на свій колишній досвід і поведінку колег, що не завжди добре і може привести до появи нових або зростання старих ризиків ІБ. Одним з таких ризиків, а скоріше навіть «викликом» для ІБ, стає Shadow IT (тіньові інформаційні технології) [6]. Іноді ще зустрічається термін «Stealth IT»[3].

На сьогоднішній день це явище і підходи до його контролю практично залишилося поза увагою дослідників з питань ІБ. Gartner дає таке визначення: «Shadow IT refers to IT devices, software and services outside the ownership or control of IT organizations»

[3], (перекл. авт. «Тіньові інформаційні технології – не контрольовані (не зареєстровані) пристрої, програмне забезпечення та послуги, що не належать до власності або контролю організації, але використовуються в ній»).

Подібне визначення міститься на сайті «Securitylab»: «Shadow IT (Теневое ИТ): Неконтролируемое оборудование, ПО и сервисы ИТ, используемые в организации и, обычно, не принадлежащие ей» [6].

Це, наприклад, персональні хмарні сховища, що надають доступ до збереженої в них інформації з будь-якого місця, і скачане неліцензійне програмне забезпечення (співробітники суб'єкта господарювання ігнорують встановлене на робочому місці ліцензоване програмне забезпечення, а використовують ті програми, до яких звикли і в яких працюють вдома), і особистий ноутбук (деякі суб'єкти господарювання дозволяють використовувати для роботи власну техніку), і персональна пошта, в якій не встановлені обмеження щодо отримання та відправлення файлових повідомлень, і особиста WiFi-точка доступу, на якій теж не встановлені обмеження і не налаштований визначеним чином firewall (мережевий екран), і багато іншого, що використовується працівниками на робочому місці. Причому мотив такої поведінки, зазвичай, є конструктивним і раціональним: це мотивується обмеженими строками виконання поставленого завдання, ігнорування співробітниками технічної підтримки звернень щодо налаштування робочого місця, необхідністю підвищити ефективність, для виконання завдань і таке інше.

Великі компанії в інформаційній сфері наводять таку аналітику:

Використання Shadow IT:

– Skyhigh: 72% організацій не розуміють сферу охоплення Shadow IT, але усвідомлюють проблему [8].

– Cisco: тільки 8% організацій розуміють сферу охоплення Shadow IT у себе [9].

– Forbes: 71% співробітників використовують несанкціоноване програмне забезпечення [10].

– Cisco: 80% співробітників використовують несанкціоноване програмне забезпечення [9].

– Використання хмарних сервісів:

– Skyhigh: в середньому співробітники використовують 30 хмарних сервісів [8].

– Cisco: в середньому організації використовують 91 хмарний сервіс [9].

– ITP.net: у 83% організацій використовуються несанкціоновані хмарні сервіси, при цьому більше третини респондентів заявили, що це заборонено в їх організації [11].

Відношення бюджету використання Shadow IT:

– Cisco (посилаються на Gartner): бюджет Shadow IT часом досягає 40% від загального IT-бюджету організації [12].

– 2016 BYOD «Bring Your Own Device» («принеси свій пристрій») and Mobile Security: у 40% організацій BYOD дозволений для всіх співробітників, в 32% дозволений для обраних співробітників [13].

Щоб краще зрозуміти підходи до зниження ризиків, також моніторингу і контролю, необхідно краще проаналізувати складові Shadow IT. Найкраще це зробити схематично (рис. 1).

І, найважливіше: Gartner: до 2020 року третина успішних атак на суб'єкти господарювання буде реалізовано за допомогою Shadow IT [13].

Як бачимо, Shadow IT різноманітне, тому підходити до захисту потрібно системно і комплексно. Необхідними заходами протидії використання Shadow IT мають бути: 1. Здійснення оцінки обсягу використання Shadow IT в суб'єкті господарювання. 2. Мінімізація прав доступу, а також переліку доступного обладнання, програмного забезпечення і сервісів. У співробітників (користувачів) суб'єкта господарювання не повинно бути адміністративних прав і великого вибору можливих програмних продуктів. Характерним прикладом забезпечення безпеки від Shadow IT можна привести роботу підрозділу кібербезпеки Міноборони Данії. У березні 2017 року датські депутати приїхали до Росії без мобільних пристроїв та ноутбуків через небезпеку зламування (англ. software cracking) та впровадження шкідливих програм-шпіонів (Spyware) в ці носимі електронні пристрої. На своїй сторінці в соціальній мережі Facebook колишній міністр зарубіжних справ Данії Мартін Лідегар (Martin Lidegaard), написав наступне: «Комітет із зовнішньої політики рекомендував нам не брати з собою в Росію гаджети з міркувань безпеки» [14]. Але депутатів не залишили без стільникового зв'язку, всім видали кнопочну модель телефону Nokia, який дозволили взяти з собою в Росію (рис. 2) [14]. Датські міністерства неодноразово піддавались хакерським атакам у 2015-2016 роках, що і стало причиною вжиття вищезазначених дій за рекомендацією підрозділу кібербезпеки Міноборони Данії [15]. 3. У суб'єкта господарювання мають бути документи, що визначають правила роботи з програмним забезпеченням, апаратним обладнанням і сервісами IT (Acceptable use policy, (AUP) «Політика допустимого використання» - один з документів, що регламентує інформаційну безпеку суб'єкта господарювання). 4. Планування адміністраторами безпеки проведення інвентаризації програмного забезпечення і апаратного обладнання. Термінова доповідь керівництву та усунення виявленого тіньового IT. Моніторинг і контроль повинні проводитись постійно. У цьому адміністраторам безпеки допоможе наступне програмне забезпечення та технології: SIEM (Security Information & Event Management - забезпечує аналіз в реальному часі подій (тривог) безпеки, що отримані від мережевих пристроїв і додатків), CASB (cloud access security broker - безпека доступу до хмарного сервісу), MDM (master data management - управління майстер-даними, серія технологій та програмних інструментів для керування основними даними суб'єкта господарювання), DLP (Data Leak Prevention - запобігання витоків, технології запобігання витоку конфіденційної інформації з інформаційної системи на зовні, а також технічні пристрої (програмні або програмно-апаратні) для такого запобігання витоків) тощо.

5. Найголовніше, необхідно розвивати культуру ІБ, навчати співробітників і давати їм зворотний зв'язок.

Кіберінциденти в промислових мережах трапляються через помилки і ненавмисні дії співробітників - саме цей фактор загрожував майже третині (29%) компаній у світі [16].

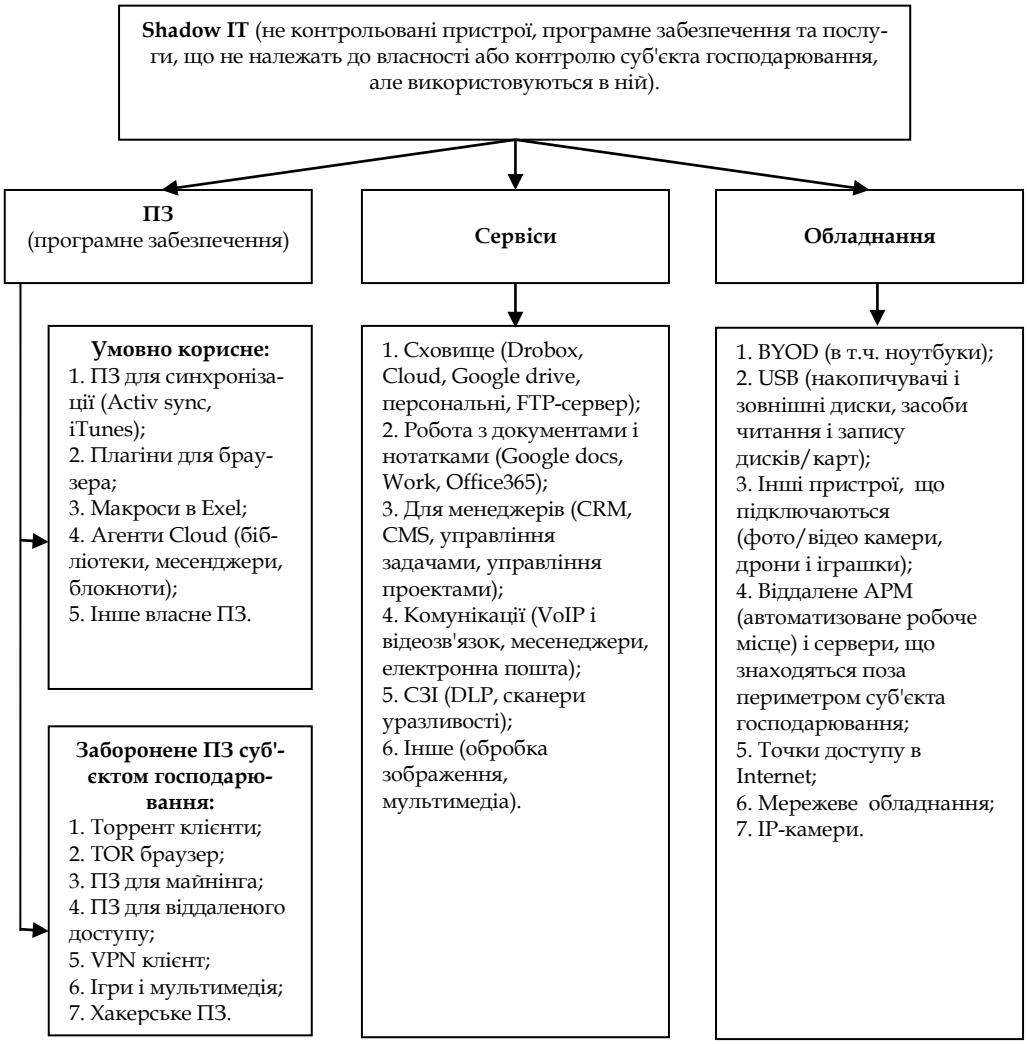

Рис. 1. Складові Shadow IT

Для суб'єктів господарювання важливо: 1) Встановити міжмережевий екран. Кожний суб'єкт господарювання повинен мати міжмережевий екран, що обмежує доступ в її мережу. Це перша лінія оборони. 2) Забезпечити контроль доступу. Використання Інтернету співробітниками повинно ретельно контролюватись. Крім того, суб'єкт господарювання повинен мати шлюз антивірусного захисту і фільтрації контента, який стане другою лінією оборони. 3) Проводити постійні перевірки. Адміністратори мережі або менеджери повинні перевіряти всі аккаунти користувачів і права доступу до них. 4) Фізичний захист. Захист не обмежується лише даними всередині електронного пристрою. Суб'єкт господарювання повинен також забезпечити фізичний захист. Постійно контролювати парк пристроїв, що мають доступ до мережі суб'єкта господарювання, а також всіх відвідувачів повинен супроводжувати хтось із персоналу, екрани моніторів не повинні проглядатись з коридору. 5) Паролі повинні бути надійними. Суб'єкт господарювання повинен забезпечити вибір надійних паролів, це означає певний рівень їх складності і періодичну зміну. 6) Не економити на захисті. Якщо суб'єкт господарювання може собі дозволити, бажано найняти в штат спеціаліста із захисту даних. Крім цього, в бюджеті слід передбачити витрати на обладнання і програмне забезпечення для захисту. 7) Проводити навчання з працівниками. З працівниками необхідно постійно проводити навчання з інформаційної безпеки та соціальної інженерії [5]. Кожен повинен розуміти наслідки, якщо зайти на невідомий веб-сайт, адреса якого надіслана по електронній пошті.

Рис. 2. Фото зі сторінки Мартіна Лідегара в Facebook

Висновки

Shadow IT створює нові вразливості і точки входу в IT-інфраструктуру суб'єкта господарювання, збільшуються ризики витоку інформації, нецільове встановлення та використання неліцензованого програмного забезпечення, що може бути шкідливим для діяльності суб'єкта господарювання. Використання носимих і мобільних пристроїв для вирішення робочих завдань стає нормою для працівників суб'єктів господарювання. Але більшість цих суб'єктів не використовують жодних рішень з управління мобільними пристроями, що в результаті може призвести до витоку корпоративних даних. Загроза для суб'єктів господарювання полягає в тому, що зростає не тільки кількість і масштаб атак - все частіше зловмисники використовують невідоме шкідливе програмне забезпечення. Це шкідливі програми, які не може відслідковувати традиційний антивірус тому, що даних про них ще немає в базах антивірусів.

Література

[1] М.О. Жованик, «Загальні принципи захисту мобільних пристроїв в корпоративній мережі», *Молодий вчений*, № 5 (20), с. 39-42, 2015.

[2] ЛІГА.net, «Украина стала главной жертвой вируса Petya инфографика». URL: http://biz.liga.net/ekonomika/it/novosti/3698413-ukraina-stalaglavnoy-zhertvoy-virusa-petya-infografika.htm.

[3] Gartner «Make Mobile Part of Your Digital Workplace Strategy». URL: https://www.gartner.com/doc/3015425?ref=SiteSearch&sthkw=Shadow%20IT%20refers%20to%20IT&fnl=search&srcId=1-3478922254.

[4] А.І. Марущак, «Структура інформаційної безпеки юридичної особи», *Інформаційна безпека людини, суспільства, держави*, №3-4, с. 7-9, 2012.

[5] О.Г. Корченко, Д.А. Горніцька, А.Ю. Гололобов, «Розширена класифікація методів соціального інжинірингу», *Безпека інформації*, Т. 20, № 2, с. 197-205, 2014.

[6] А.С. Прозоров, «Когда мало контроля ИБ», Электронный ресурс, Режим доступа: https://www.securitylab.ru/blog/personal/80na20/342486.php.

[7] А.С. Марков, В.Л. Цирлов, «Руководящие указания по кибербезопасности в контексте ISO 27032», *Вопросы кибербезопасности*, № 1(2), с. 28-35, 2014.

[8] Skyhigh «Shadow IT Security Checklist». URL: http://info.skyhighnetworks.com/CH-Shadow-IT-Security-Checklist_Banner-Cloud.html.

[9] Joann Starke, «The Shadow IT Dilemma». URL: https://blogs.cisco.com/cloud/the-shadow-itdilemma.

[10] Christopfer Frank, «Shadow IT». URL: https://www.forbes.com/sites/forbesproductgroup/2017/02/22/shadow-it/#66e90c3c79fd.

[11] Mark Sutton, «Unauthorised cloud adoption growing issue for CIOs». URL: http://www.itp.net/603235-unauthorised-cloud-adoption-growingissuefor-cios.

[12] Cisco «Shadow IT and Cisco Cloud Consumption Professional Services». URL: https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Intercloud_Fabric_A.html.

[13] Kasey Panetta, «Gartner's Top 10 Security Predictions 2016» Сайт компанії «Gartner». URL: http://www.gartner.com/smarterwithgartner/top-10security-predictions2016/?cm_mmc=soc ial-_-rm-_-gart-_-swg.

[14] Facebook. URL: https://m.facebook.com/martin.lidegaard/photos/a.451142271606144.111938.447217575331947/1215056811881349/?type=3&source=54.

[15] Tadviser «Киберприступность в мире». URL: http://www.tadviser.ru/index.php/.

[16] 16 Статья: Киберпреступность_в_мире. Лабораторія Каперського. URL: https://www.kaspersky.ru/about/press-releases/2017_kaspersky-lab-has-launched-an-active-search-service-for-cyber-attacks.

УДК 004.056.53 (045)

Марущак А.И., Скицко А.И. Влияние теневых информационных технологий на информационную безопасность субъекта хозяйствования

Аннотация. *Информационная безопасность является неотъемлемой частью национальной безопасности и в то же время важной самостоятельной сферой обеспечения безопасности субъектов хозяйственной деятельности. Сегодня информационное пространство, инфраструктура и технологии в большей степени влияют на уровень и темпы социального, экономического и технического развития. Поэтому успех субъекта хозяйствования, гарантия получения прибыли все больше зависят от сохранения в тайне секретов производства, опираются на интеллектуальный потенциал и конкретную технологию. Сотрудники хранят данные на носимых устройствах - важная корпоративная информация становится доступной с любого ноутбука, смартфона или планшета, который сотрудник использует в офисе или кафе. В статье проведен анализ угрозы, которая приобретает все большие масштабы в информационной сфере и связана с использованием мобильных и носимых устройств (wearable device) на рабочем месте. Разработано определение-перевод Shadow IT или Stealth IT и приведена структура возможных мест проявления этой угрозы.*

Ключевые слова: *Shadow IT, Stealth IT, носимые устройства, информационная безопасность, субъект хозяйствования.*

Marushchak A., Skitsko O. The influence of Shadow Information Technology on the cyber security of business entity

Abstract. *The development of information technology over the past decades has led to radical changes in all the spheres of human, social and state activity: new cultural and economic trends appear, the production of information as an independent product develop, new types of social communications emerge. In this connection the information sphere of any state becomes critical and therefore needs to be protected. Particularly urgent is the issue of information security. That is why scientists actively research the issues related to a set of measures aimed at ensuring the security of information from unauthorized access, as well as studying methods and tools that ensure the integrity, confidentiality and availability of information under the influence of any threats, the realization of which can cause damage to the owners and users of information. Information security has become an integral part of national security and at the same time an important independent sphere of ensuring the safety of business entities. Nowadays the information space, infrastructure and technologies considerably influence the level and rate of social, economic and technological development. There-*

fore, the success of the business entity, the guarantee of profit, becomes more and more dependent on keeping production secrets, based on the intellectual potential and specific technology. Employees store data on mobile or wearable devices – and important corporate information becomes available from any laptop, smartphone or tablet that an employee uses at the office or cafe. In the paper the analysis of threat that becomes extremely urgent in the information sphere and is connected with the use of mobile or wearable devices at the workplace is performed. The definition of Shadow IT or Stealth IT is developed and the structure of possible places of the emergence of the corresponding threat is given. The suggestions on improving the operation of corporate information security units in counteracting unauthorized access to information resources are offered.
Key words: Information security, Shadow IT, Stealth IT, shadow information technologies, wearable devices, access control, network display, business entity.
***Key words**: information security, Shadow IT, Stealth IT, shadow information technologies, wearable devices, access control, firewall, business entity.*

Отримано *31 січня 2018 року*, затверджено редколегією *14 березня 2018 року*