УДК 004.056 **Борсуковський Ю.В., Борсуковська В.Ю.**

ПРИКЛАДНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ

В даній статті проведено детальний аналіз актуального ландшафту кіберзагроз та напрямки забезпечення інформаційної безпеки зі сторони світової спільноти. Розглянуто можливі напрямки забезпечення інформаційної та кібернетичної безпеки в умовах обмеженого фінансування. Наведені категорії CIS Control, щодо напрямків пріоритетного забезпечення інформаційної безпеки бізнесу. Проаналізовані і сформовані рекомендації та вимоги щодо прикладних аспектів побудови стратегії захисту в умовах обмежених фінансових ресурсів. Сформульовані мінімальні вимоги щодо забезпечення інформаційної та кібернетичної безпеки державних та приватних організацій.

Ключові слова: загрози, ризики, категорії, кібербезпека

Вступ і постановка задачі

У жовтні 2017 року Європейська Рада зобов'язала уряди країн ЄС посилити питання кібербезпеки. Останні рішення, прийняті Європейською Радою, вказують на необхідність виділення всіма країнами-членами ЄС потрібних ресурсів і інвестиції для боротьби із кіберзлочинністю. «Кіберзлочини і фінансована державами діяльність шкідливих програм є однією з найбільших глобальних загроз для наших суспільств і економік. Ми вже втрачаємо близько 400 млрд євро у всьому світі через кібератаки. Це чітко підкреслює необхідність використання ЄС наявних інструментів для підвищення стабільності в кіберпросторі та реагування на масштабні кіберінциденти», - йдеться в повідомленні Європейської Ради [4].

Експерти Давоського форуму оприлюднили глобальний ландшафт загроз, які загрожують людству в 2018 році (рис. 1). Список катаклізмів, здатних зіпсувати життя світовому співтовариству, дуже різноманітний: від некерованої інфляції до екстремальних погодних умов, від інфекційних захворювань до кібератак, від тероризму до падіння урядів [3].

Глобальні тренди, які загрожують проблемами, теж численні. Найзначніші з них - це зміни клімату, зростаюча кіберзалежність людства, зростаюче розшарування за рівнем доходів і зростаюча поляризація суспільства. На думку експертів Всесвітнього економічного форуму, світ вступає в критичний період і, сьогодні, фокус світової негативної енергії зосереджений на розпалюванні розбрату. На цьому фоні масові випадки шахрайства з даними та/або їх крадіжки призводять не лише до значної економічної шкоди, але і спричиняють геополітичну напруженість і втрату довіри в Інтернеті, що автоматично може призвести до значної соціальної нестабільності з непрогнозованими наслідками [3].

Створення та поширення перспективних інформаційних систем та технологій сприяє появі нових форм кібератак, що піддають державні та приватні інформаційні ресурси загрозам, з якими вони не готові мати справу. Кібератаки можуть становити критичну загрозу для тих економік, держав і суспільств, у яких недостатньо розвинуто співробітництво і відсутня ефективна система інформаційного та кібернетичного захисту. Результати аналізу векторів кібератак говорять про те, що у кіберпросторі сформувалася стійка тенденція свого роду гібридної війни. Головною передумовою такої тенденції стало перш за все зростання зацікавленості урядових структур в отриманні інформації, яка може бути використана протиборчими сторонами в світовій конкурентній і політичній боротьбі [5, 8].

Враховуючи ці тенденції, у січні 2018 року на Всесвітньому економічному форумі було прийнято рішення про створення Глобального центру кібербезпеки, покликаного допомогти побудувати безпечний і захищений глобальний кіберпростір [6].

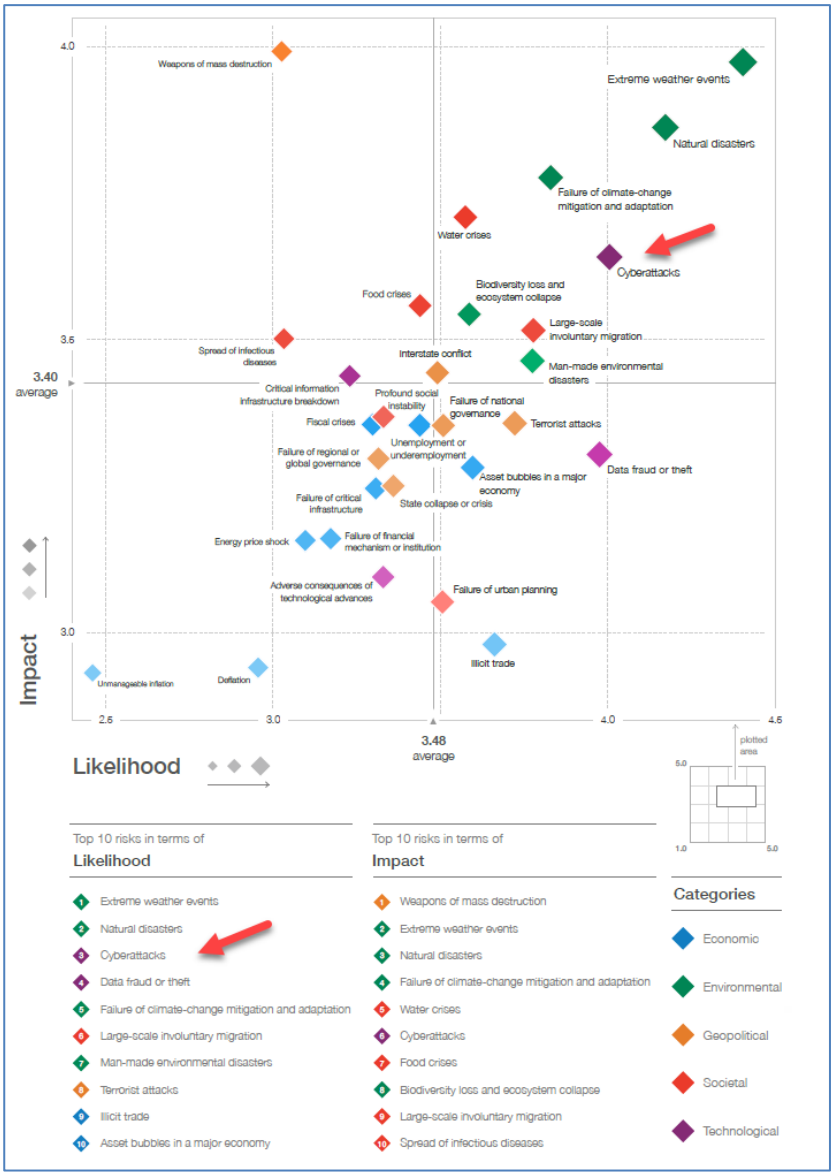
Метою центру є створення першої міжнародної платформи для урядів, компаній, фахівців і правоохоронних органів, призначеної для співпраці у подоланні проблем кібербезпеки. Очевидно, що проблеми кібератак непідвладні силам і організаціям, які намагаються впоратися з ними окремо. Тільки за рахунок співпраці, обміну інформацією та загальних стандартів світова громадськість зможе успішно протистояти електронної злочинності [6].

© Ю.В. Борсуковський, В.Ю. Борсуковська, 2018

«Якщо ми хочемо запобігти настанню темних часів, нам потрібно наполегливіше працювати над тим, щоб досягнення і потенціал Четвертої промислової революції перебували в безпеці і під захистом на благо суспільства. Новий Глобальний центр кібербезпеки буде першою платформою для зменшення кібернетичних ризиків в дійсно світовому масштабі», - сказав директор-розпорядник Всесвітнього економічного форуму і директор Глобального центру кібербезпеки Алоїз Звінггі [6].

За оцінками експертів, щорічні втрати світової економіки в результаті дій кіберзлочинців можуть досягати 500 мільярдів дол. США, в той час, як, наприклад, річний ВВП Швейцарії в 2017 році оцінюється в 659 мільярдів доларів США [6].

Всесвітній економічний форум визнав, що кіберзлочинність є одним з найбільш критичних глобальних ризиків (рис. 1). Відповідно, Глобальний центр кібербезпеки буде орієнтований на надання підтримки урядам і галузевим компаніям, що є учасниками форуму, в частині забезпечення більш безпечного кіберпростору з використанням підходу, що передбачає залучення численних зацікавлених сторін [7].



Основними цілями даного центру визначена консолідація існуючих програм кібербезпеки Всесвітнього економічного форуму, створення незалежної бібліотеки з даними передових практик кібербезпеки, допомога партнерам в поліпшенні їх знань у сфері кібербезпеки, робота над створенням належної гнучкою законодавчої бази в сфері кібербезпеки, робота в якості лабораторії та аналітичного центру раннього попередження про майбутні сценарії кібератак.

Рис. 1. Глобальний ландшафт загроз 2018

Як видно із викладеного вище, кількість атак проти державних і приватних організацій країн світу постійно зростає, а самі атаки стають дедалі досконалішими. Визначити ініціаторів атак, незалежно від того чи це урядові структури або приватні групи зловмисників, які заробляють таким чином гроші, - стає також дедалі важче.

Така ситуація вимагає динамічної адаптації інформаційних систем і систем інформаційної безпеки до поточного ландшафту загроз, а також до вимог, завдань і

© *Ю.В. Борсуковський, В.Ю. Борсуковська,* 2018

масштабів сучасної економіки та бізнесу. Це, у свою чергу, потребує визначення пріоритетних напрямків проведення превентивних заходів із інформаційної та кібернетичної безпеки відповідно до поточного ландшафту загроз в інформаційній сфері.

Виклад основного матеріалу дослідження

Враховуючи викладене, особливо важливо прийняти зважене рішення, щодо напрямків і пріоритетів захисту ключових інформаційних систем в державних та приватних організаціях з урахуванням обмеженого фінансування в сферах ІТ та ІБ. Це особливо актуально у економічних умовах в яких сьогодні знаходиться Україна. Тут ми стикаємося з низкою проблем, які потребують пріоритетного розгляду при прийнятті рішень.

Твердження 1. Як правило, відсутня стратегія забезпечення безпеки захисту ключових інформаційних систем у відповідності до існуючих ризиків. Кіберзлочинці націлені на отримання максимальної вигоди і постійно вдосконалюють методи атак. По такому принципу потрібно підходити до організації комплексної системи інформаційної безпеки. Вона повинна адаптивно змінюватися, відповідно до нових викликів та загроз, що формуються в кіберпросторі.

Твердження 2. Модель загроз повинна враховувати той факт, що при цільовій атаці зловмисники досягнуть 100% успіху. Ґрунтуючись на даній аксіомі повинні бути внесені відповідні зміни в інфраструктуру ІТ та ІБ, а також, з дуже високим ступенем імовірності, і в деякі бізнес процеси, які можуть виявитися критичними в разі успішної кібератаки.

Твердження 3. Потрібно враховувати недостатнє фінансування ІТ та ІБ і відсутність у відповідальних осіб чіткого розуміння, що потрібно впроваджувати першочергово для захисту ключових інформаційних активів. Найчастіше кошти виділяються тільки на антивіруси для робочих станцій, які, як показав досвід останніх епідемій шифрувальників, нездатні гідно протистояти сучасним атакам. Але навіть наявність фінансування, особливо в державних структурах, не гарантує ефективний рівень захисту інформаційних активів. Найчастіше необхідний рівень безпеки підтримується лише для звіту («паперова безпека» на рівні розробки та затвердження КСЗІ), а за фактом, ключові інформаційні ресурси захищаються від кіберзагроз системами інформаційної безпеки позавчорашнього дня.

Відповідно до сформульованих тверджень, очевидно, що інфраструктура ІТ та ІБ повинна вибудовуватися на основі багато-ешелонованих організаційно-технічних шарів безпеки із використанням кращих світових практик, рекомендацій і методологій PCI, NIST, ISO і HIPAA. Особливо це стає актуальним в умовах недостатніх або нульових бюджетів ІБ. Адже будь які помилки, що будуть допущені на етапі прийняття рішень щодо побудови або модернізації систем ІТ та ІБ можуть призвести до катастрофічних наслідків, як у фінансовому плані, так і в плані захисту ключових інформаційних активів. Останні події в Україні та світі це досить добре продемонстрували.

На сьогоднішній день експерти визначають такі основні ключові напрямки, які повинні потрапити в сферу уваги при визначені пріоритетних напрямків розгортання систем інформаційної та кібернетичної безпеки [1, 2, 10]:

- аналіз поточних атак та сучасний розвиток технологій і вимог до ІТ та ІБ технологій;
- аутентифікація, шифрування і створення білих списків додатків;
- аналіз і зіставлення прийнятих рішень із існуючими методологіями і галузевими рекомендаціями;
- підходи до застосування продуктів забезпечення інформаційної безпеки;
- проведення тестування на наявність вразливостей та перевірки на відповідність діючим стандартам безпеки;
- використання рекомендацій світової спільноти при створенні галузевих систем інформаційної безпеки.

Тут в повній мірі можна використовувати ключові рекомендації CIS Controls [1, 2] для визначення критичних профілів захисту інформаційних систем державних та приватних організацій. Ці профілі повинні включати в себе підходи та методики щодо всебічних

© Ю.В. Борсуковський, В.Ю. Борсуковська, 2018

перевірок елементів IT-інфраструктури, конфігурацій, прав доступу, привілеїв, системних журналів, заходів і засобів реагування на інциденти та принципи ініціювання перевірок.

У 7 редакції керівництва CIS Controls [1] дані елементи розподілені на три категорії, що враховують сучасний ландшафт кіберзагроз (рис. 2) – базові, фундаментальні та організаційні.

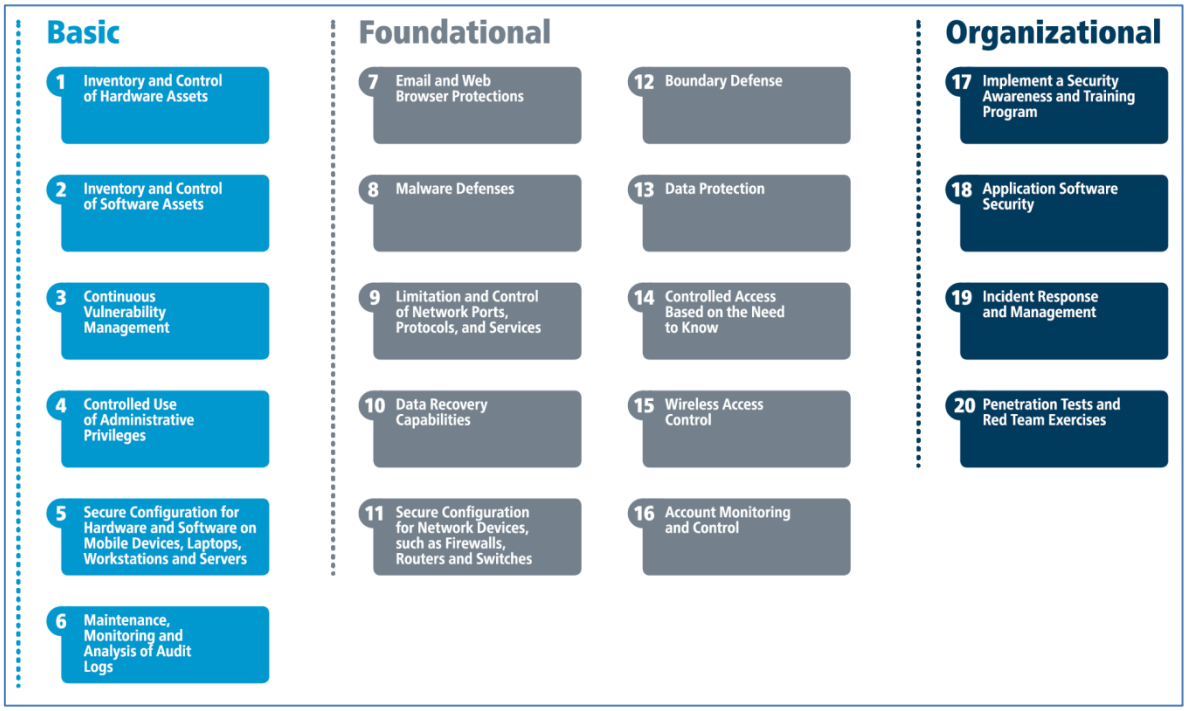


Рис. 2. Категорії CIS V7

Базові категорії містять ключові напрямки для забезпечення інформаційної безпеки державних та приватних організацій:

1) інвентаризація авторизованих і неавторизованих пристроїв;
2) інвентаризація авторизованого і неавторизованого програмного забезпечення;
3) засоби управління вразливостями;
4) використання адміністративних привілеїв;
5) захищені конфігурації для мобільних пристроїв, ноутбуків, робочих станцій і серверів;
6) обслуговування, моніторинг та аналіз журналів аудиту.

Фундаментальні категорії містять рекомендації, необхідні для застосування кращих практик для забезпечення переваг і використання передових технологій кібербезпеки:

7) захист електронної пошти та веб-браузера;
8) захист від шкідливих програм;
9) обмеження і контроль мережевих портів;
10) можливість відновлення даних;
11) захищені конфігурації для мережевих пристроїв (файерволи, роутери, комутатори);
12) захист периметра;
13) захист даних;
14) контроль доступу;
15) контроль доступу бездротових мереж;
16) контроль облікових записів.

Організаційні категорії містять рекомендації, орієнтовані на організаційні процеси і адміністративні заходи, пов'язані із забезпеченням інформаційної безпеки, з метою підвищення обізнаності персоналу та проведення тестування на проникнення. А саме:

© *Ю.В. Борсуковський, В.Ю. Борсуковська,* 2018

17) контроль рівня обізнаності персоналу;
18) контроль прикладного програмного забезпечення;
19) реагування на інциденти;
20) тестування на проникнення.

Пріоритети стратегічного планування тут, мабуть, можна визначити трьома основними твердженнями, які ми повинні враховувати першочергово:

Твердження 4. Безпека, повинна бути заснована на обізнаності. Внутрішні порушники, зовнішні атаки, нові інфраструктурні сервіси та бізнес-додатки вже складають багатовимірну множину активів і ризиків. Розібратися в них аналітичним способом стає практично неможливо. В умовах недостатнього фінансування, ключовим напрямком оптимізації ресурсів ІБ, у відповідності до визначених ризиків, можуть стати кращі світові практики. Вони дозволяють в умовах обмежених фінансових ресурсів мінімізувати ризики та загрози шляхом здійснення контролю внутрішніх процесів (моніторинг мережевої безпеки, профілювання активності користувачів і сервісів, сегментація мережі, шифрування і т.д.) і зовнішніх процесів (використання ЗМІ, баз даних і підписок про погрози). Без врахування кращих світових практик, останньої і повної інформації про якість управлінських рішень і ефективність систем кібербезпеки в цілому говорити вже не доводиться.

Твердження 5. Великі державні та приватні організації приступили до тотальної інформатизації та цифрової трансформації, внаслідок якої навіть традиційно консервативні, в плані ІТ, бізнеси реального сектору вже не зможуть реалізовувати свої бізнес-процеси без точної і надійної роботи інформаційних систем.

Управління вимогами до ІТ з боку бізнесу і неминуче виникаючими конфліктами пріоритетів вимагає створення узгоджених регулятивних вимог до певних напрямків бізнесу із точки зору ІБ. При вироблені узгоджених вимог повинно бути розуміння не тільки завдань бізнесу, а і розуміння проблем ІТ та ІБ для того, щоб амортизувати корпоративні тертя і оптимізувати часові та фінансові витрати при виробленні спільного ефективного рішення.

Твердження 6. Проведення регулярних оцінок стану ІБ. Без здійснення безперервного тестування, оцінювання загроз, ризиків та стану захищеності ключових корпоративних інформаційних активів втрачається сенс цифрової трансформації. Якщо процеси трансформації не захищені, дані можуть бути рано чи пізно викрадені або знищені, то очевидно, що рух до цифрової трансформації буде генерувати тільки збитки для організацій. Тут державним та приватним організаціям потрібно створювати систему внутрішньої безперервної експертизи ІБ, а, для виконання рутинних та трудомістких операцій, використовувати ресурси та спеціалістів MSSP провайдерів.

Об'єднуючи всі ці вимоги, ми можемо сформулювати мінімальні умови при яких ми можемо, на основі аналізу сучасних загроз і оцінок власних ризиків, здійснити оптимізацію фінансових витрат в процесах забезпечення ІБ інформаційних активів державних та приватних організацій [9, 10, 11]:

- мінімізація шляхів атак за рахунок побудови сегментованої та багатошарової системи захисту на базі рішень Open Source (це, наприклад, системи формування та ведення безпечних конфігурацій для апаратного та програмного забезпечення, контрольоване використання адміністративних привілеїв, захист електронної пошти та веб-браузеру, обмеження та контроль мережевих портів, управління безпечними конфігураціями для мережевих пристроїв, контрольований доступ на основі ролі користувача, моніторинг і контроль облікових записів, сегментація мережі і т.д.);
- побудова ефективної системи захисту мережевого периметру – тут ми можемо використовувати (наприклад, pfSense, OPNsense та ін.);
- шифрування критичних даних (наприклад, OpenPGP, GnuPGP та ін.);
- резервне копіювання (наприклад, Veeam Backup, Effector saver та ін.);
- забезпечення внутрішньої та зовнішньої оцінки вразливостей (наприклад, Kali

© *Ю.В. Борсуковський, В.Ю. Борсуковська,* 2018

Linux) або використання ресурсів вищих учбових закладів в якості MSSP провайдерів.

Зрозуміло, що комерційні продукти у багатьох випадках виграють наявністю покращеної технічної підтримки і більш проблемно орієнтованим набором інструментальних рішень для спрощення їх впровадження і використання. Але коли у нас немає або не вистачає фінансових ресурсів, такий гібридний підхід може стати одним із шляхів забезпечення ефективного захисту інформаційних активів.

Все це, з урахуванням кращих світових практик, дозволяє достатньо ефективно формувати стратегію інформаційного та кібернетичного захисту критичних інформаційних активів в умовах обмежених фінансових ресурсів ІТ та ІБ. І тут уже в кожному конкретному випадку бізнесом буде прийматися рішення, яким чином оптимізувати фінансові витрати і мінімізувати ризики.

Висновок

Сучасні проблеми глобалізації та висока ефективність перспективних ІТ технологій підвищує імовірність реалізації сучасних інформаційних і кібернетичних загроз і, як наслідок, це може сприяти виникненню загального світового колапсу. Кібератаки все частіше стають інструментом швидкого досягнення необхідних результатів як в економічній, так і політичній сферах.

На даний час питання цифрової трансформації і організації безпеки ключових інформаційних активів в державних та приватних організаціях стоїть досить гостро у цілому світі. Сформовані рекомендації та вимоги щодо прикладних аспектів побудови стратегії захисту в умовах обмежених фінансових ресурсів можуть бути використані при розробці політик захисту інформаційних активів державних та приватних організацій.

Подальші дослідження варто зосередити на створенні та впровадженні типових політик, процедур та рекомендацій щодо захисту інформаційних активів державних і приватних організацій як опорних точок для побудови оптимізованих по вартості і функціоналу систем інформаційної та кібернетичної безпеки.

Список використаних джерел:

1. Center for Internet Security [Електронний ресурс] // – Режим доступу: https://www.cisecurity.org/controls/
2. CIS Controls Version 7 - What's Old, What's New [Електронний ресурс] // – Режим доступу: https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/
3. Euronews. Давос 2018: совместный ответ глобальным угрозам [Електронний ресурс] // – Режим доступу: http://ru.euronews.com/2018/01/24/davos-2018-what-are-humanitarian-organisations-bringing-to-the-world-economic
4. Information Resistance [Електронний ресурс] // – Режим доступу: http://sprotyv.info/ru/news/kiev/es-utverdil-mery-po-usileniyu-svoey-kiberbezopasnosti
5. Russia step supcyber-attackson UK. – The Sunday Times, February 2017 [Електронний ресурс] // – Режим доступу: http://www.thetimes.co.uk/edition/news/russia-steps-up-cyber-attacks-on-uk-rl262pnlb
6. UKRINFORM. В Давосе объявили о создании Глобального центра кибербезопасности [Електронний ресурс] // – Режим доступу: https://www.ukrinform.ru/rubric-technology/2389711-v-davose-obavili-o-sozdanii-globalnogo-centra-kiberbezopasnosti.html
7. World Economic Forum. Reports 2018 [Електронний ресурс] // – Режим доступу:www3.weforum.org/docs/WEF_GRR18_Report.pdf
8. Из-за атаки хакеров Минфин и Госказначейство потеряли 3 терабайта данных [Електронний ресурс] // – Режим доступу: http://biz.censor.net.ua/n3017228
9. Борсуковський Ю.В. Рекомендації по категоріюванню інформації з обмеженим доступом / Борсуковський Ю.В., Борсуковська В.Ю. / Сучасний захист інформації. 2017. - №4. – С. 9-17
10. Борсуковський Ю.В. Базові напрямки забезпечення кібербезпеки державного та приватного секторів / Борсуковський Ю.В., Бурячок В.Л., Борсуковська В.Ю. / Сучасний захист інформації. – 2017. - №2. – С.85-89
11. Борсуковська В.Ю. Безперервність бізнесу: новий тренд або необхідність / Борсуковська В.Ю., Борсуковський Ю.В. / Економіка. Менеджмент. Бізнес. 2017. - №2. – С. 48-53

Надійшла: 16.03.2018 Рецензент: к.т.н. Курченко О.А.

© *Ю.В. Борсуковський, В.Ю. Борсуковська,* 2018