КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (1), 2018

УДК 004.056

Борсуковський Юрій Володимирович
кандидат технічних наук , професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
OrcID: 0000-0003-1973-2386
gmbyurii@gmail.com

Борсуковська Вікторія Юріївна
ПАТ «Укрсоцбанк», департамент безпеки, керівник проектів
Київ, Україна
OrcID: 0000-0002-4929-6987
v.barsik@gmail.com

ПРИКЛАДНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ ОБМЕЖЕНОГО ФІНАНСУВАННЯ

Анотація. В даній статті проведено розгорнутий аналіз тенденцій розвитку кіберзагроз та напрямків забезпечення інформаційної безпеки зі сторони світової спільноти. Сучасний розвиток перспективних інформаційних систем та технологій сприяє появі нових форм кібератак, що піддають державні, банківські та приватні інформаційні ресурси загрозам, з якими вони не готові мати справу. Визначена тенденція щодо формування у кіберпросторі принципів гібридної війни. Передумовами виникнення таких гібридних війн стає зростання зацікавленості урядових структур в отриманні інформації, яка може бути використана протиборчими сторонами в світовій конкурентній і політичній боротьбі Визначено необхідність адаптивного формування напрямків проведення превентивних заходів із інформаційної і кібернетичної безпеки. Акцентовано увагу на відсутність, у більшості випадків, стратегії забезпечення безпеки щодо захисту ключових інформаційних систем у відповідності до існуючих ризиків. Звернено увагу на те, що модель загроз повинна враховувати можливість повної компрометації систем інформаційної та кібернетичної безпеки при ціле-направленій атаці на інформаційні активи державних, банківських та приватних організацій. Розглянуто можливі напрямки забезпечення інформаційної та кібернетичної безпеки в умовах обмеженого фінансування. Наведені категорії CIS Control, щодо напрямків пріоритетного забезпечення інформаційної безпеки бізнесу. Наведено перелік ключових напрямків для формування пріоритетів інформаційної безпеки державних, банківських та приватних організацій. Проаналізовані і сформовані рекомендації та вимоги щодо прикладних аспектів побудови стратегії захисту в умовах обмежених фінансових ресурсів. Одним із шляхів оптимізації фінансових ресурсів що витрачаються на системи інформаційної безпеки, у відповідності до визначених ризиків, може стати використання кращих світових практик, а також чітке узгодження вимог забезпечення інформатизації та цифрової трансформації з боку бізнесу і створення узгоджених регулятивних вимог до певних напрямків бізнесу із точки зору інформаційної та кібернетичної безпеки. Сформульовані мінімальні вимоги щодо забезпечення інформаційної та кібернетичної безпеки державних, банківських та приватних організацій.

Ключові слова: загрози, ризики, категорії, кібербезпека, стратегія, фінансування**.**

1. ВСТУП

Постановка проблеми. Розгорнутий аналізу тенденцій розвитку кіберзагроз показує, що кількість атак проти державних, банківських і приватних організацій країн світу постійно буде зростати, а самі атаки будуть ставати все дедалі досконалішими.

Визначати ініціаторів атак, незалежно від того чи це урядові структури або приватні групи зловмисників, які заробляють таким чином гроші, — стає дедалі важче.

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

Аналіз останніх досліджень і публікацій. 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 [0].

Створення та поширення перспективних інформаційних систем та технологій сприяє появі нових форм кібератак, що піддають державні, банківські 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.

Як приклад важливості формування шляхів протидіє таким тенденціям можна привести оцінку експертів із кібербезпеки щодо щорічних втрат світової економіки в результаті дій кіберзлочинців що складає біля 500 мільярдів дол. США, в той час, як, наприклад, річний ВВП Швейцарії в 2017 році оцінюється в 659 мільярдів доларів США.

Про важливість формування активних шляхів протидії міжнародній кіберзлочинності говорить і те, що у січні 2018 року на Всесвітньому економічному форумі було прийнято рішення про створення Глобального центру кібербезпеки, покликаного допомагати будувати безпечний і захищений глобальний кіберпростір [0].

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Враховуючи викладене, особливо важливо прийняти зважене рішення, щодо напрямків і пріоритетів захисту ключових інформаційних систем в державних, банківських 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:

– 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 для визначення критичних профілів захисту інформаційних систем державних та приватних організацій. Ці профілі повинні включати в себе підходи та методики щодо всебічних перевірок елементів ІТ-інфраструктури, конфігурацій, прав доступу, привілеїв, системних журналів, заходів і засобів реагування на інциденти та принципи ініціювання перевірок.

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

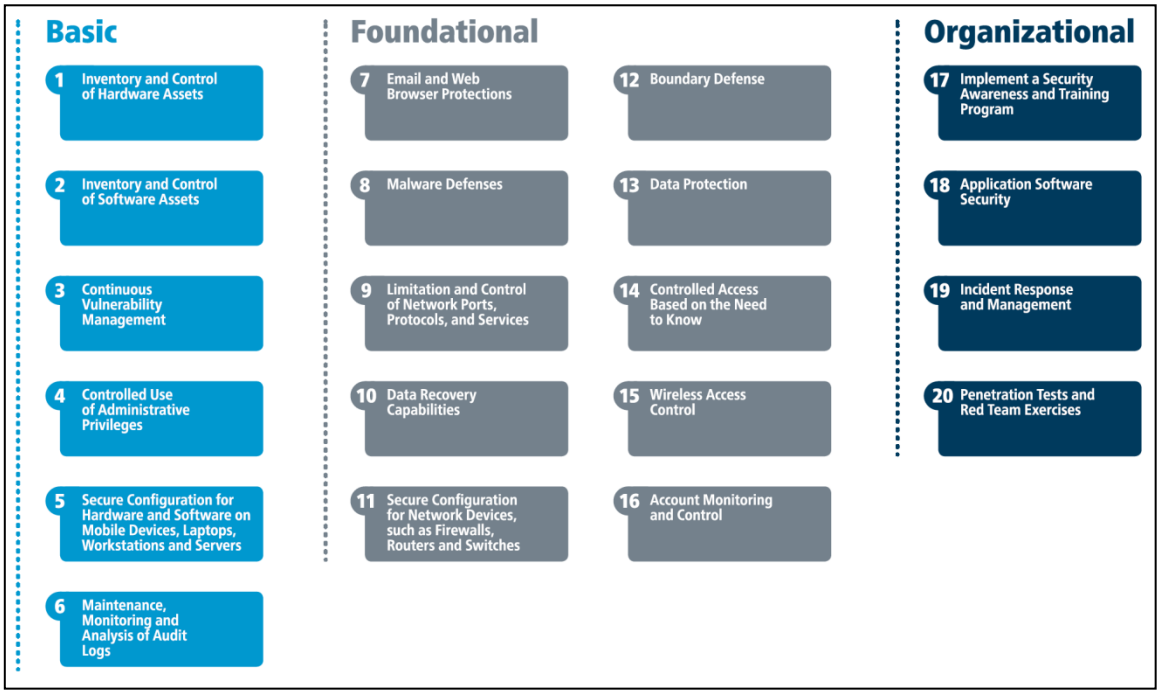

Рис. 1. Категорії забезпечення інформаційної та кібернетичної безпеки

Базові категорії містять ключові напрямки для забезпечення інформаційної безпеки державних, банківських 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:

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, банківські 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:

– 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 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.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

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.” [Онлайн]. Режим доступу: https://www.cisecurity.org/controls/ [18 черв. 2018].

[2] “CIS Controls Version 7 — What’s Old, What’s New.” [Онлайн]. Режим доступу: https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/ [18 черв. 2018].

[3] «Давос 2018: совместный ответ глобальным угрозам», *Euronews*. [Онлайн]. Режим доступу: http://ru.euronews.com/2018/01/24/davos-2018-what-are-humanitarian-organisations-bringing-to-the-world-economic [18 черв. 2018].

[4] “Information Resistance.” [Онлайн]. Режим доступу: http://sprotyv.info/ru/news/kiev/es-utverdil-mery-po-usileniyu-svoey-kiberbezopasnosti [18 черв. 2018].

[5] “Russia step supcyber-attackson UK,» *The Sunday Times*, Feb. 2017. [Онлайн]. Режим доступу: http://www.thetimes.co.uk/edition/news/russia-steps-up-cyber-attacks-on-uk-rl262pnlb [18 черв. 2018].

[6] «В Давосе объявили о создании Глобального центра кибербезопасности», *UKRINFORM*. [Онлайн]. Режим доступу: https://www.ukrinform.ru/rubric-technology/2389711-v-davose-obavili-o-sozdanii-globalnogo-centra-kiberbezopasnosti.html [18 черв. 2018].

[7] "Reports 2018," *World Economic Forum*. [Онлайн]. Режим доступу: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf [18 черв. 2018].

[8] «Из-за атаки хакеров Минфин и Госказначейство потеряли 3 терабайта данных». [Онлайн]. Режим доступу: http://biz.censor.net.ua/n3017228 [18 черв. 2018].

[9] Ю. В. Борсуковський, В. Ю. Борсуковська і В. Л. Бурячок, «Напрямки формування політик кібербезпеки для державного, банківського та приватного секторів», *Modern Methodologies, Innovations, and Operational Experience on the Field of Technical Science*, Radom, Republic of Poland, сс. 8–11, Dec. 2017.

[10] В. Ю. Борсуковська і Ю. В. Борсуковський, «Безперервність бізнесу: новий тренд або необхідність», *Економіка. Менеджмент. Бізнес*, №2 (20), сс. 48–52, 2017.

[11] Ю. В. Борсуковський, В. Л. Бурячок і В. Ю. Борсуковська, «Базові напрямки забезпечення кібербезпеки державного та приватного секторів», *Сучасний захист інформації*, №2 (30), сс. 85–89, 2017.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (1), 2018

UDC 004.056

Yurii V.Borsukovskyi
PhD in technical sciences, professor of the Department of Information and cyber security
Borys Grinchenko Kyiv University, Ukraine
OrcID: 0000-0003-1973-2386
gmbyurii@gmail.com

Victoria Y.Borsukovska
PJSC "Ukrsotsbank", Security Department, Kyiv, Ukraine
OrcID: 0000-0002-4929-6987
v.barsik@gmail.com

PRACTICAL POINTS FOR INFORMATION SECURITY CONSIDERING LIMITED FINANCING

Abstract. This article provide the detailed analysis of tendencies of cyber threats development and trends to ensure the informational security by the world`s community. Modern development of perspective informational system and technologies promote the uprising of new forms of cyberattacks that lead the state, banking and private informational resources to threats with which these agencies are not ready to deal. The article defines the tendency on creation at cyberspace the principles of hybrid war. Preconditions for such hybrid wars are the interest of government structures to receive information which could be used by opposing parties in world`s competitive and political battles. The article defines the adaptive creation of directions for preventive actions on informational and cyber security. Document underlines the absence, in most cases, of any security strategy to protect key informational systems considering the existent risks. Article focuses that threat model should consider the complete compromising of information and cyber security systems during targeted attack to informational assets of state, banking and private organizations. Document considers the possible directions to ensure informational and cyber security in case of limited financing. Article provides CIS Control elements assisting to prioritize and ensure the informational security of business. Document includes the list of key directions to create the priorities of informational security in state, banking and private organizations. Article analyses and generate recommendations and requirements on practical aspects for development of security policy considering limited financing. One of the ways for optimization of financial resources allocated for informational security systems, considering the defined risks, could be the application of word`s best practices, as well the clear coordination of requirements to ensure informational and digital transformation by business and creation of coordinated regulatory requirements for certain businesses considering informational and cyber security. The article provides minimum requirements to ensure informational and cyber security in state, banking and private organizations.

Keywords: threats, risks, categories, cybersecurity, strategy, financing.

REFERENCES

[1] "Center for Internet Security." [Online]. Available: https://www.cisecurity.org/controls/ [Jun. 18, 2018].
[2] "CIS Controls Version 7 — What's Old, What's New." [Online]. Available: https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/ [Jun. 18, 2018].
[3] "Davos 2018: sovmestnyi otvet global'nym ugrozam [Davos 2018: joint response to global threats]," *Euronews*. [Online]. Available: http://ru.euronews.com/2018/01/24/davos-2018-what-are-humanitarian-organisations-bringing-to-the-world-economic [Jun. 18, 2018]. (In Russian).
[4] "Information Resistance." [Online]. Available: http://sprotyv.info/ru/news/kiev/es-utverdil-mery-po-usileniyu-svoey-kiberbezopasnosti [Jun. 18, 2018].
[5] "Russia step supcyber-attackson UK,» *The Sunday Times*, Feb. 2017. [Online]. Available: http://www.thetimes.co.uk/edition/news/russia-steps-up-cyber-attacks-on-uk-rl262pnlb [Jun. 18, 2018].
[6] "V Davose ob"yavili o sozdanii Global'nogo tsentra kiberbezopasnosti [In Davos, the creation of the global cybersecurity center]," *UKRINFORM*. [Online]. Available: https://www.ukrinform.ru/rubric-

technology/2389711-v-davose-obavili-o-sozdanii-globalnogo-centra-kiberbezopasnosti.html [Jun. 18, 2018]. (In Russian).

[7] "Reports 2018," *World Economic Forum*. [Online]. Available: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf [Jun. 18, 2018].

[8] "Iz-za ataki khakerov Minfin i Goskaznacheistvo poteryali 3 terabaita dannykh [Due to the attack of hackers, the Ministry of Finance and the State Treasury lost 3 terabytes of data]." [Online]. Available: http://biz.censor.net.ua/n3017228 [Jun. 18, 2018]. (In Russian).

[9] Yu. V. Borsukovs'kyy, V. Yu. Borsukovs'ka and V. L. Buryachok, "Napryamky formuvannya polityk kiberbezpeky dlya derzhavnoho, bankivs'koho ta pryvatnoho sektoriv [Directions of forming cybersecurity policies for the state, banking and private sectors]," *Modern Methodologies, Innovations, and Operational Experience on the Field of Technical Science*, Radom, Republic of Poland, pp. 8–11, Dec. 2017. (In Ukrainian).

[10] V. Yu. Borsukovs'ka and Yu. V. Borsukovs'kyy, "Bezperervnist' biznesu: novyy trend abo neobkhidnist' [Business continuity: a new trend or need]," *Ekonomika. Menedzhment. Biznes*, no. 2 (20), pp. 48–52, 2017. (In Ukrainian).

[11] Yu. V. Borsukovs'kyy, V. L. Buryachok and V. Yu. Borsukovs'ka, "Bazovi napryamky zabezpechennya kiberbezpeky derzhavnoho ta pryvatnoho sektoriv [The basic directions of providing cybersecurity of public and private sectors]," *Suchasnyy zakhyst informatsiyi*, no. 2 (30), pp. 85–89, 2017. (In Ukrainian).