УДК 004.056

Ю.В. Борсуковський, В.Л. Бурячок

РОЛЬ І МІСЦЕ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ У СТВОРЕННІ СИСТЕМИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

В даній статті проведено детальний аналіз сучасних кіберзагроз. Сформульовано базові вимоги і рекомендації щодо напрямків підготовки фахівців з інформаційної та кібернетичної безпеки відповідно до діючих глобальних загроз в інформаційному просторі.

Ключові слова: загрози, ризики, політика, кібербезпека

Вступ і постановка задачі

Створення та поширення перспективних технологій сприяє появі нових форм кібератак, що піддають державні та корпоративні ресурси загрозам, з якими вони не готові мати справу. Про це було офіційно заявлено на Всесвітньому економічному форумі, що проходив у Давосі у січні 2017 року[1]. Учасники форуму були практично одностайні в думці, що саме досягнення в області комп'ютерних технологій таких як квантові обчислення, паралельні системи, нейронні дослідження, розподілення критичної інформації в мережах та хмарні технології підвищують останнім часом загрози загального колапсу при їх відключенні (наприклад, Інтернет, супутники, мережі і т.д.). Масштабні кібератаки, масові випадки шахрайства даних та/або їх крадіжки призводять, як було констатовано на форумі, до значної економічної шкоди, визивають геополітичну напруженість і втрату довіри в Інтернеті.

Глобальний ландшафт загроз 2017 року, визначений провідними фахівцями із США, Німеччини, Японії, Швейцарії, Австралії, Сінгапуру, ОАЕ та інших країн, наведено на рис. 1.

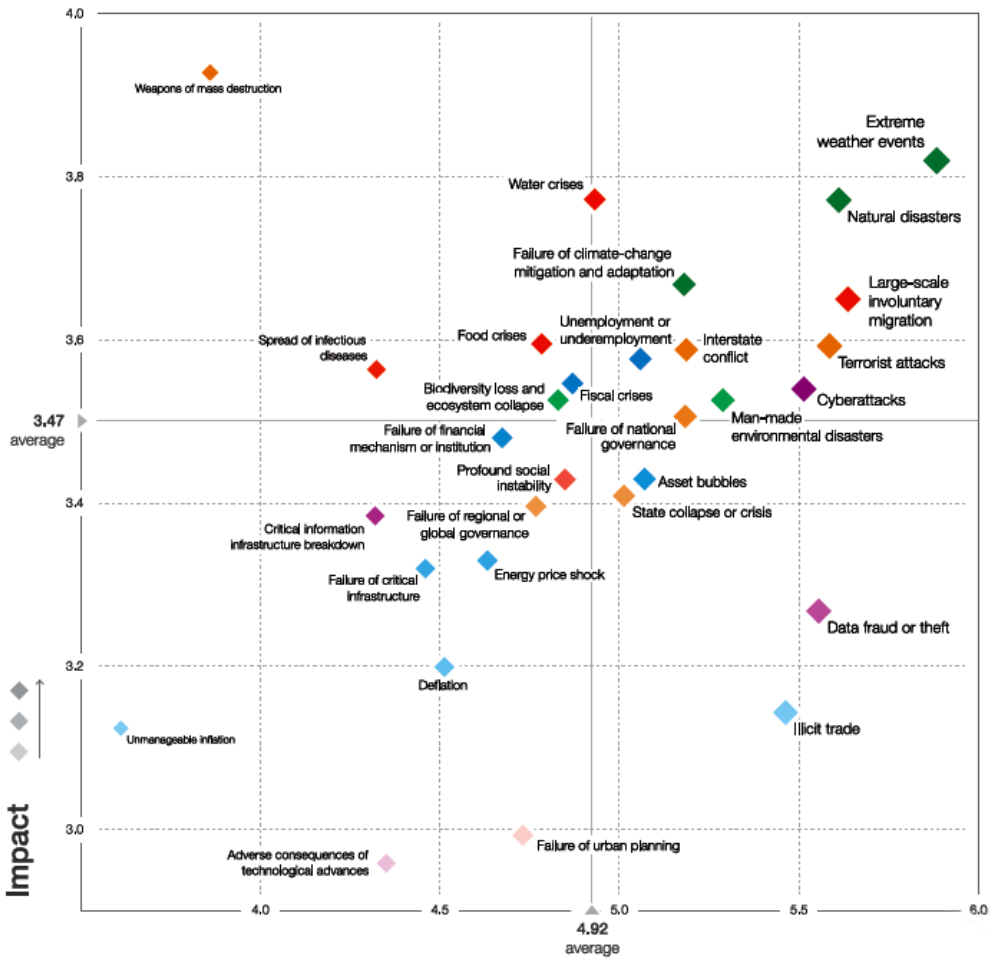

Рис.1. Глобальний ландшафт загроз 2017

Результати їх аналізу говорять про те, що нині у кіберпросторі сформувалася стійка тенденція свого роду гібридної війни. Головною передумовою такому стало перш за все зростання

зацікавленості урядових структур в отриманні інформації, яка може бути використана протиборчими сторонами в світовій конкурентній і політичній боротьбі. Прикладом цьому можна вважати хакерську атаку на сервери Національного Комітету Демократичної партії США. Викрадене електронне листування 7 ключових керівників партії було відкрито використане для досягнення політичних цілей на виборах в США. Ще одним із прикладів такому можуть слугувати хакерські атаки на урядові установи Великої Британії. Голова Національного центру кібербезпеки (NCSC) Кіаран Мартін [6] в одному із своїх інтерв'ю відмітив значне зростання їх кількості – до 60 атак щомісяця. За його даними таким атакам останнім часом піддавались передусім об'єкти у галузі оборони та зовнішньої політики. Нині фахівці Центру констатують появу нової тенденції – атаки на так звані «м'які цілі»: місцеві ради та благодійні фонди з метою крадіжок персональних даних, а також на університети з метою викрадення наукових секретів. Головними спонсорами хакерських груп Кіаран Мартін називає уряди Росії та Китаю.

В Україні до таких подій відносять атаки на IT інфраструктуру в сфері енергетики, державних і банківських фінансів, транспорту і зв'язку. Тільки з грудня 2015 по грудень 2016 років в нашій державі було зареєстровано понад 270 успішних атак на подібні об'єкти. Прикладом цьому є атака на компанію «Прикарпаттяобленерго» (грудень 2015 року). Американська IT-фірма iSight Partners пов'язала атаку з російською хакерською групою, відомою як «Піщаний хробак». Згодом Департамент з національної безпеки США назвав типу вірусу, який хакери використані для злому мережі. Ним виявилась шкідлива програма Black Energy Malware. До подібних випадків слід віднести також атаки на сайти Головного управління розвідки Міноборони України (квітень 2016 року), Міністерства оборони та Національної гвардії України (серпень 2016 року), а також атаку на сайт інформаційно-аналітичного центру Ради національної безпеки й оборони України (вересень 2016 року). Так у День незалежності України, 24 серпня, хакери зламали сторінки Міністерства оборони та Національної гвардії України в соціальних мережах й розмістили на них провокаційні записи. Розвідувальні служби України офіційно заявили, що IP-адреси, з яких були здійснені ці атаки, зареєстровані у Росії і на окупованих територіях України, а координацію такої діяльності здійснює Центр інформаційної протидії Південного військового округу ЗС Російської Федерації. Надзвичайно важкими за наслідками для України виявились атаки на сайт Державної казначейської служби та Міністерства фінансів нашої держави (грудень 2016). Під час спроби зайти на сайт Держказначейства користувача переадресовувало на інший сайт з адресою «whoismrrobot». У Мінфіні назвали таку атаку «очевидною спробою зірвати бюджетний процес, який вперше за більш ніж 17 років йде в Україні за графіком». За заявою першого заступника директора Національного інституту стратегічних досліджень Олександра Власюка [2] ці атаки привели до втрати близько 3 терабайтів даних.

Виклад основного матеріалу дослідження

Як видно з викладеного вище кількість атак проти державних і корпоративних структур країн світу постійно зростає, а самі атаки стають дедалі досконалішими. Визначити ініціаторів атак, будь-то державні структури або приватні групи зловмисників, які заробляють таким чином гроші, – стає також дедалі важче. Як стверджує Чарльз Колоджі, віце-президент Security Products, це пов'язане з тим, що останнім часом «середовище кіберзлочинності більш за все зацікавлене у здійсненні фінансового шахрайства та крадіжці даних, корпоративному шпигунстві та підриві й навіть повному знищенні інфраструктури і процесів» (рис.2).

Рис.2. Мотивація здійснення кібернападів на IT інфраструктуру

Свою долю в здійснення успішних атак на IT інфраструктури державних і корпоративних структур останнім часом вносять й масштабні витоки персональних даних (з соціальних мереж, баз даних медичних установ і т. п.). Про це говориться у звіті аналітичного центру InfoWatch, фахівцями якого лише за I півріччя 2015 року було, наприклад, зареєстровано 723 випадки витоку конфіденційної інформації. Це на 10% більше, ніж за аналогічний період 2014 року (654 витоки). Найбільшу загрозу несе при цьому передусім людський фактор (рис. 3).

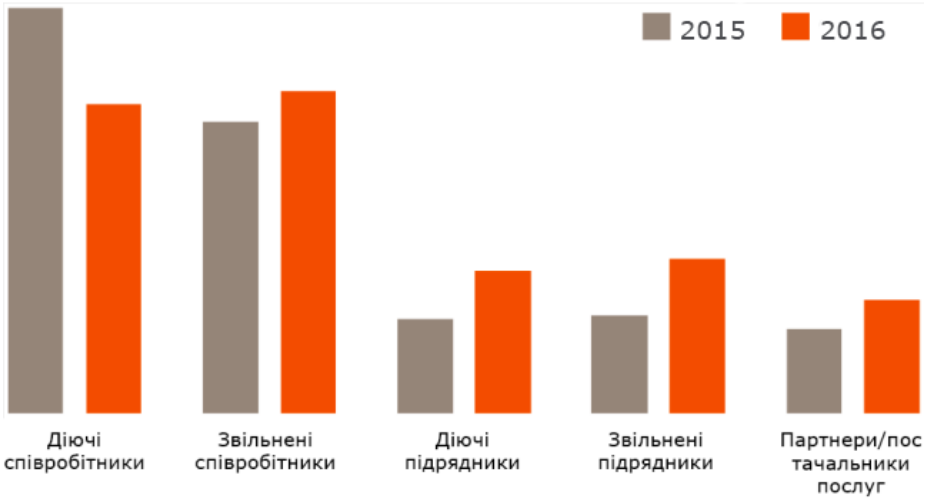

Рис.3. Соціотехнічний фактор у здійсненні кібернападів

Так, за статистикою, приблизно кожен п'ятий співробітник компанії-жертви готовий свідомо продати свої облікові дані. У 40% випадків користувачі готові продати свої облікові дані в тому числі і від віддаленого доступу. Такі дії вони оцінюють у 1000 долл. США [4]. В деяких випадках ця сума може становити 100 долл. США і навіть менше. Все це, як результат, колосально спрощує процедуру і вартість подолання мережевого периметра будь-якої IT інфраструктури. Відомості про це наведено у звіті компанії Dell за квітень 2016 року. За даними фахівців компанії вартість такої процедури має нині фіксовану ціну і в середньому не перевищує 500 долл. США [3]. Зовнішній периметр IT інфраструктури (за даними компанії Positive Technologies) долається в 83% випадків. У 54% випадків це не вимагає висококваліфікованої підготовки. Як приклад, вартість злому поштових акаунтів Mail.ru, Yandex.ru, Rambler.ru в середньому становить нині від 65 до 103 долл. США, Ukr.net, Gmail.com, Yaho.com, Hotmail.com, Facebook.com – приблизно 129 долл. США, соціальних акаунтів VKontakte (VK.ru), Odnoklasniki (OK.ru) – 194 долл. США.

Останнім часом змінилися також й підходи до цілей подолання мережевих периметрів. Замість того, щоб просто викрадати дані, кіберзлочинці шифрують їх з метою вимагання. При середній вартості викупу в 300 долл. США і кількості сплачених викупів, що становлять 2,9% від всієї кількості зафіксованих випадків [5], розрахунковий валовий дохід від програм-шифрувальників складає 34 млн. долл. США на компанію. Розквіту даної стратегії сприяє зростання популярності крипто-валют і електронних платежів, використання яких значно ускладнює завдання пошуку та ідентифікації зловмисників. За оцінкою ФБР, в 2016 році віртуальне вимагання увійшло в число найприбутковішого хакерського програмного забезпечення (ПЗ) з передбачуваною прибутковістю в 1 млрд долл. США (рис.4).

Такий стан справ вимагає динамічної адаптації системи ІБ до поточних і постійно мінливих загроз, а також до вимог, завдань і масштабів сучасної економіки та бізнесу. Це, у свою чергу, потребує виокремлення декількох основних тверджень, що визначають пріоритетні напрямки з підготовки спеціалістів з інформаційної та кібернетичної безпеки відповідно до визначеного ландшафту глобальних ризиків в інформаційній сфері.

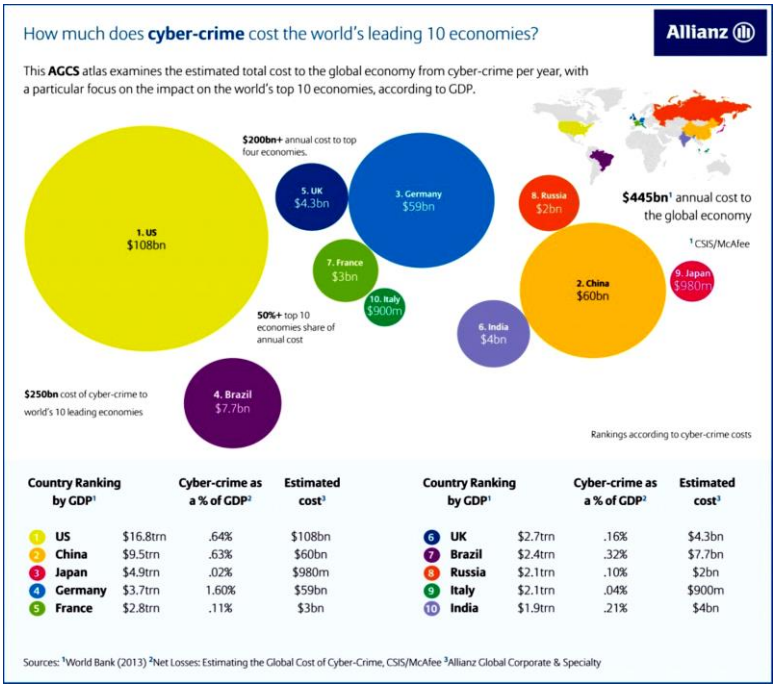

Рис.4. Вартість наслідків кіберзлочинності для 10 провідних економік світу

Твердження 1. Модель загроз повинна враховувати той факт, що при таргетованій атаці зловмисники досягнуть 100% успіху. Ґрунтуючись на даній аксіомі повинні бути внесені відповідні зміни в інфраструктуру IT та ІБ, а, з дуже високим ступенем імовірності, і в деякі бізнес процеси, які можуть виявитися критичними в разі успішної кібератаки.

Твердження 2. Інфраструктура IT та ІБ повинна вибудовуватися на основі багато ешелонованих організаційно-технічних шарів безпеки. На сьогоднішній день можна визначити такі основні напрями, які повинні потрапити в сферу пріоритетної уваги:

постійний контроль наявності вразливостей, оцінка існуючих ризиків і організація процесу оперативного розгортання наявних оновлень системного і прикладного програмного забезпечення;

постійний моніторинг і управління правами доступу користувачів до ресурсів IT інфраструктури, впровадження систем багатофакторної аутентифікації на базі PKI і електронних ключів, обмеження прав адміністраторів;

забезпечення захисту периметра мережі IT інфраструктури, контроль доступу користувачів до Інтернет ресурсів, фільтрація пошти, установка файєрволів нового покоління і систем запобігання вторгнень;

сегментування інфраструктури IT по логічним групам і розділення по зонам безпеки, обмеження доступу з мережі Інтернет до особливо критичних сегментів;

організація «білих списків» і введення часового інтервального контролю на доступ користувачів до критичних ресурсів IT інфраструктури;

контроль бездротових мереж і управління правами доступу до них користувачів;

розробка ефективних парольних політик і впровадження для користувачів інструменту ефективного управління створенням, зберіганням і зміною паролів;

безперервний моніторинг систем безпеки, активне виявлення і протидія атакам, впровадження систем моніторингу і аналізу подій (SIEM) та запобігання витоків інформації (DLP), пріоритетне розгортання систем ІБ, які здатні скоротити час виявлення та забезпечити мінімізацію наслідків успішних атак;

шифрування критичних даних і управління зберіганням та захистом від несанкціонованого доступу до секретних ключів користувачів;

організація системи резервного копіювання критично важливих даних і оцінка їх уразливості до успішних атак, слід враховувати можливості локального і «хмарного зараження» (cloud poisoning) резервних копій;

тестування на проникнення, розробка планів та процедур реагування на інциденти;

безперервний захист і навчання кінцевих користувачів, проведення їх стрес-тестування шляхом проведення навчань з атак і відпрацювання дій користувачів на таке тестування.

Чи охоплює цей перелік всі організаційно-технічні заходи? Безумовно, ні. В сфері інформаційної безпеки постійно з'являються нові підходи, ідеї і рішення. Пріоритети повинні задаватися політиками безпеки на основі постійної оцінки поточних загроз. Чи вистачить нам фінансових і матеріальних ресурсів, щоб протистояти або хоча б мінімізувати загрози, що постійно зростають і динамічно змінюються? І на це питання доводиться давати негативну відповідь. Як виходити з положення, що склалося на даний момент? Тільки безперервною оцінкою ризиків і «раціональним» управлінням наявними фінансовими і технічними ресурсами відповідно до прийнятих політик безпеки. На додаток до цього доцільно більш активно оцінювати можливості і вводити в шари безпеки продукти ІБ Open Source (за наявності).

На вирішення цього та низки інших завдань в рамках проекту Європейської Комісії під назвою Горизонт 2020 в поточному році планується виділити біля €450 млн. Загальний же обсяг інвестицій в забезпечення інформаційної та кібернетичної безпеки очікується в межах €1,8 млрд. до 2020 року. Як результат, річний приріст інвестицій в безпеку до кінця 2020 року має зрости приблизно на 9,8%.

Ініціативи європейської комісії спрямовані передусім на захист від кібератак та підвищення конкурентоздатності сектора IT-безпеки. Про це сповіщає Help Netsecurity з посиланням на віце-президента Digital Single Market Андруса Ансипа. У найближчих планах Єврокомісії – створити центри швидкого реагування на кіберзагрози, які були б спроможні використовувати:

1) засоби забезпечення безпеки інформаційного і кіберпросторів (рис.5);

2) процедури хмарних обчислень та аналітику великих даних;

3) методи страхування кіберризиків та застосування ризик орієнтованого підходу до організації й забезпечення безпеки;

4) алгоритми обміну інформацією про актуальні загрози з партнерами тощо.

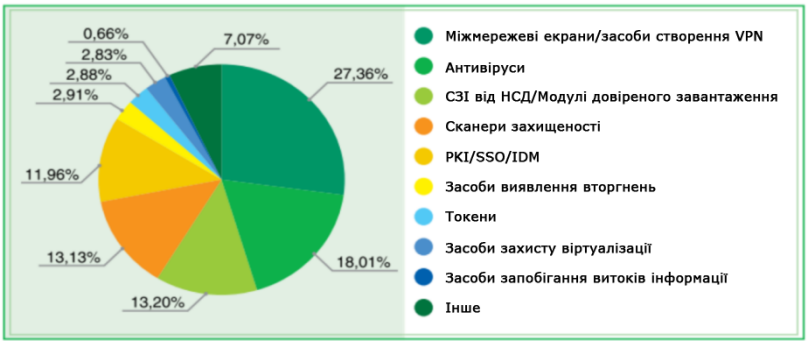

Рис.5. Структура витрат, які провідними країнами світу вкладаються нині у забезпечення безпеки інформаційного і кіберпросторів за класами продуктів

Зважаючи, що найближчим часом не менше 30% даних буде зберігатися в «хмарі», обсяг доступної пам'яті кожні чотири роки буде збільшуватися у 10 разів, а кількість злочинів у кіберпросторі щорічно буде збільшуватися не менш ніж на 10%, – в Україні, в умовах обмеженого фінансування та реального зростання числа кібернетичних атак на IT інфраструктури державних і корпоративних структур, доцільно мати власну оперативну координуючу структуру, яка б Згідно «Плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України» (далі – План),

затвердженого розпорядженням Кабінету Міністрів України від 24.06.2016 №440, забезпечувала б оцінку ефективності використання та вироблення рекомендацій, а також надавала технічну та методичну допомогу щодо:

по-перше, «формування переліку міжнародних стандартів, стандартів ЄС та НАТО у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки, які потребують перекладу та гармонізації» (п.п. 3 Плану);

по-друге, «участі у заходах щодо зміцнення міжнародного співробітництва у сфері кібербезпеки ….» (п.п. 5 Плану);

по-третє, «розроблення пропозицій щодо впровадження спеціальностей та дисциплін з кібербезпеки у програмах навчання вищих навчальних закладів для потреб органів сектору безпеки і оборони» (п.п. 21 Плану).

Хоча відповідальність за вирішення цих завдань у Плані чітко визначено й покладено на органи виконавчої влади, а також на силові структури та служби спеціального призначення нашої держави (СБУ, МО, МВС, ДССЗЗІ, Національну поліцію тощо), таким центром з розробки і впровадження новітніх технологій могли б виступити Вищі навчальні заклади (далі – ВНЗ) України, які займаються підготовкою фахівців з інформаційної та кібернетичної безпеки. Цілком зрозуміло, що такий крок неможливий без швидкої зміни програм підготовки фахівців згідно із змінами глобального ландшафту загроз.

Зважаючи, що нашій державі конче потрібні сучасні програми підготовки фахівців з інформаційної та кібернетичної безпеки, які здатні швидко адаптуватися до сучасних ризиків та загроз, ВНЗ будуть вимушені ставити перед собою нові амбітні завдання й формувати базис у вигляді:

компетенцій (соціально-особистісних, інструментальних, загальнонаукових та професійних);

виробничих функцій (дослідницьких, проектувальних, організаційних, управлінських, технологічних, контрольних, прогностичних та технічних) та типових задач, що їм відповідають;

умінь, якими мають володіти випускники та фактично закласти фундамент для їх практичної роботи за напрямками організації та забезпечення кібернетичної безпеки.

Навчальні програми в свою чергу повинні мати прикладне наповнення з відповідним фінансуванням (замовлення на конкретні розробки з державного та корпоративного секторів та наукові гранти) і стати інтерактивними – оперативно враховувати нові ризики в сфері інформаційної та кібернетичної безпеки.

Нині ж, нажаль, залишається констатувати, що потенціал ВНЗ у цих процесах (щодо п.п. 3 та 5 Плану), зокрема провідних ВНЗ міста Києва – Київського національного університету ім. Тараса Шевченка, Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського», Національного авіаційного університету та Державного університету телекомунікацій, залишається не задіяним. Водночас залишається не зрозумілим, чому в Плані наголос робиться лише на кібербезпеку, а не на інформаційну безпеку в цілому, яка є більш широким поняттям порівняно зі спеціальністю 125 – «кібербезпека» (нині у відповідності до «Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти», затвердженого постановою КМ України від 29 квітня 2015 р. № 266 спеціальність 125 – «кібербезпека» належить до галузі знань 12 – «Інформаційні технології»).

Висновок

1) Глобалізація і висока ефективність перспективних ІТ технологій підвищує імовірність реалізації сучасних інформаційних і кібернетичних загроз й сприяє, як результат, виникненню загальному світовому колапсу.

2) Кібератаки все частіше стають інструментом швидкого досягнення необхідних результатів як в економічній, так і політичній сферах.

3) Залучення ВНЗ України до опрацювання та вирішення нагальних проблем критично важливих галузей і секторів національної економіки та обороноздатності нашої держави, шляхом:

приведення існуючої системи національних стандартів захисту інформації у відповідність сучасним міжнародним вимогам;

розробки єдиного освітнього стандарту з інформаційної (кібернетичної) безпеки;

створення національного науково-технічного центру з інформаційної та кібернетичної безпеки й покладення на нього завдань з розроблення і впровадження нових технологій з інформаційної та кібернетичної безпеки в державному, корпоративному та науковому секторах;

опрацювання питань розвитку в нашій державі комплексної системи підготовки і перепідготовки кадрів з інформаційної (кібернетичної) безпеки, необхідного рівня та кваліфікацій - *дозволить створити державну систему інформаційної і кібербезпеки, а також сприятиме надійному та ефективному функціонуванню державного і корпоративного секторів національної безпеки та економіки України, підвищенню боєздатності та боєготовності її Збройних Сил*.

Література

1. Всесвітній економічний форум. The Global Risks Report 2017 12th Edition. – Davos 2017. [Електронний ресурс] – Режим доступу: https://www.weforum.org

2. Из-за атаки хакеров Минфин и Госказначейство потеряли 3 терабайта данных. [Електронний ресурс] – Режим доступу: http://biz.censor.net.ua/n3017228

3. Underground Hacker Markets. Annualreport – April 2016. [Електронний ресурс] – Режим доступу: http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf

4. Каждый п’ятий сотрудник компании готов продать учетные данные. [Електронний ресурс] – Режим доступу: http://www.securitylab.ru/news/480306.php

5. Форум Cisco - Технології кібербезпеки, Київ, 8 грудня 2016

6. 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

Надійшла 15.02.2017 р. Рецензент: д.т.н., с.н.с. Грищук Р.В.