УДК 004.681.3

В.Л.Бурячок, Я.В. Невойт, Л.В.Бурячок

ВПЛИВ ЗАГРОЗ АНТРОПОГЕННОГО І ТЕХНОГЕННОГО ХАРАКТЕРА НА СТАН БЕЗПЕКИ ІТ-СИСТЕМ ТА СОЦІАЛЬНИХ ІНСТИТУТІВ ПРОВІДНИХ КРАЇН СВІТУ І УКРАЇНИ

У статті розглянуто основополагаючі закони створення та функціонування інформаційного і кібернетичного просторів. Акцентовано увагу на необхідності захисту критично-важливих сегментів та об'єктів економіки держав світу від загроз антропогенного і техногенного характеру, а також на тих завданнях які мають бути при цьому вирішені. Досліджено головні проблеми, які на сучасному етапі розвитку світового суспільства не дозволяють в повному обсязі це зробити. Проведено аналіз ролі та місця Україна та її головних суб'єктів у забезпеченні безпеки інформаційного і кібернетичного просторів. Запропоновано низку кроків для створення дієвої системи інформаційної та кібербезпеки на теренах нашої держави

Ключові слова: кібербезпека, інфраструктура, інформатизація, телекомунікації, економічний розвиток.

Вступ

Формування та розвиток сучасного інформаційного суспільства базується на синтезі двох інформаційно-комунікаційних технологій – комп'ютерної і телекомунікаційної та визначається двома простими, але дуже змістовними законами. Перший закон сформульовано одним із засновників корпорації Intel Гордоном Муром. Говорячи про те, що "… кількість транзисторів у процесорах збільшуватиметься вдвічі кожних півтора роки …", фактично пояснює формування на рубежі тисячоліть простору інформаційного. Другий закон належить Роберту Меткалфу, винахіднику найпоширенішої на сьогодні технології комп'ютерної мережі Internet. Говорячи про те, що "… цінність мережі знаходиться у квадратичній залежності від кількості вузлів, які є її складовими …" він фактично констатує, що основу сучасного інформаційного суспільства становлять ІТ системи та мережі різного призначення, домінування яких в усіх процесах життєдіяльності людства обумовило появу та формування простору кібернетичного (рис.1).

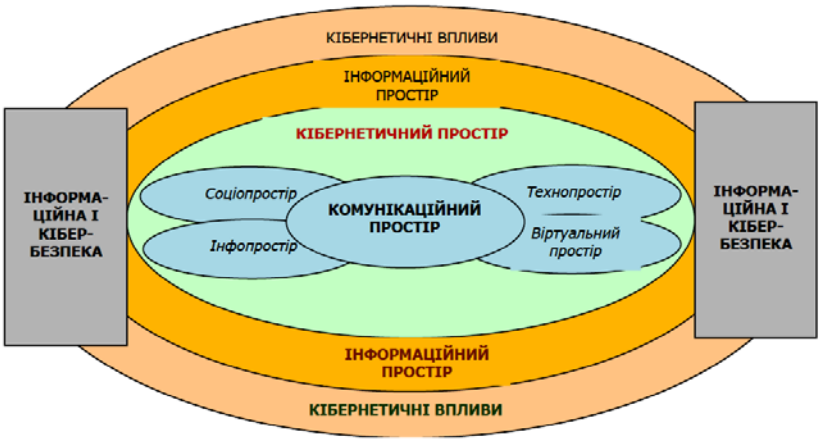

Рис. 1. Взаємозв'язок інформаційного і кіберпросторів

Вплив на ці глобальні субстанції, по-перше, відіграє суттєву роль в економічному і соціальному розвитку переважної більшості держав світу та свідчить про їх вступ до якісно нової фази протиборства у глобальному інформаційному просторі – кіберпротиборства й, по-друге, сприяє отриманню державами світу як значних переваг, так й виникненню низки проблем – передусім значної уразливості їх інформсфери від загроз, пов'язаних з особливостями існування та передачі інформації.

Зважаючи на таке мета статті полягає у визначенні впливу загроз антропогенного і техногенного характеру на стан безпеки ІТ-систем та соціальних інститутів, обґрунтуванні необхідності створення глобальної системи кібернетичної безпеки, відсутність якої може призвести до втрати політичної незалежності будь-якої держави світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її

національних інтересів інтересам протиборчої сторони [1,2], а також в необхідності підготовки кваліфікованих фахівців з проблем кіберзахисту.

Основна частина

Як відомо, саме вибухове зростання обсягів інформації, до яких отримали доступ пересічні громадяни, а також винайдення потужних комп'ютерів і вбудованих мікроконтролерів, що сприяло розвитку промисловості, привело переважну більшість країн світу не тільки до глобальної інтелектуалізації, але й зробило більш вразливими передусім критично-важливі сегменти та об'єкти їх економіки до загроз антропогенного і техногенного характеру, а також природних катаклізмів. Такими об'єктами нині є енергетичні і транспортні магістральні мережі, нафто- та газопроводи, канали швидкісного і урядового зв'язку, високотехнологічні підприємства та підприємства оборонно-промислового комплексу, центральні органи влади тощо. Порівняно з 2014 роком до переліку об'єктів критично-важливої інфраструктури, на які останнім часом здійснюється переважна більшість нападів, були додані заклади освіти та охорони здоров'я, а також фінансовий сектор. До таких об'єктів відносять й так звану кіберінфраструктуру, яка нині стала ключовим елементом функціонування сучасних розвинених держав, що обрали шлях побудови економіки, заснованої на знаннях.

Необхідність убезпечення державами світу ІКТ та ІТС, а також захисту ними власної критичної інфраструктури від внутрішніх і зовнішніх втручань та загроз, що реалізуються зловмисниками передусім через атаки нульової доби, атаки на провайдерів, атаки на мобільні пристрої тощо вимагає [3 – 5]:

по-перше, прийняття певних законодавчих актів, а також розробки стратегії виконання низки організаційних та інженерно-технічних заходів;

по-друге, створення відповідних органів, функції, повноваження та зона відповідальності яких має визначатися з урахуванням історичних традицій, національних пріоритетів і законодавства;

по-третє, вирішення найбільш важливих і загальних та, в тому чи іншому формулюванні, найбільш пріоритетних задач, що передбачають посилення боротьби з міжнародним тероризмом, забезпечення безпеки інформаційного та кіберпростору тощо.

Вирішення цих задач на сучасному етапі розвитку світового суспільства в повному обсязі не завжди вбачається можливим. Одними з головних проблем при цьому є нерозуміння державами світу необхідності створення глобальної системи інформаційної та кібернетичної безпеки (рис.2), а також відсутність узгоджених на міжнародному рівні визначень цих понять, що «… стримує міжнародні та національні зусилля з захисту мереж і комп'ютерних систем …» [7 – 12].

Рис. 2. Співвідношення понять безпеки в інформаційному та кіберпросторах

Саме про це черговий раз було відмічено в документах Всесвітньої повноважної конференції міжнародного союзу електрозв'язку WCIT- 2014 (респ. Корея, 20.10-7.11.14). Саме цей факт призвів до здійснення низки злочинів і терактів в інформаційному та кіберпросторах з використанням можливостей сучасних ІКТ та ІТС. Прикладами такому є:

1) події червня 1982 року, коли шляхом активації програмного забезпечення, отриманого радянськими розвідниками в Канаді, та у яке, як з'ясувалось пізніше, американці попередньо ввели помилкові дані, була проведена кібератака проти сибірського газопроводу. Після одержання команди ззовні програма перевищила режим роботи газопроводу настільки, що він вибухнув;

2) події 1995 року, коли з банку "Україна" шляхом проникнення в його мережу було викрадено майже 4 мільйони доларів, 1997 року – коли на декілька годин була заблокована робота Internet-провайдера "Глобал Юкрейн", 2000 року – коли була зафіксована інформаційна диверсія проти Internet-провайдера "ukr.net", 2012 року – коли відбулися масовані кібернапади на державні IP в ході виборчої кампанії в Україні;

3) події 2009 року, коли була виявлена цілеспрямована атака GhostNet з центром управління в Китаї, орієнтована на більш ніж сотню країн. Вторгнення відбувалися за допомогою повідомлення електронної пошти при відкритті якого запускалася шкідлива програма із прикріпленого файлу. Після установки вірус завантажував хакерський інструментарій Ghost Remote Administration Toolkit для дистанційного управління системами. Управляючий сервер у Китаї потім міг відправляти вірусу команди на передачу інформації з комп'ютерів жертв;

4) міждержавні інциденти 2010–2012 років, спричинені мережевими черв'яками Duqu, Flame та Stuxnet (табл.1).

Таблиця 1

Характеристик троянських вірусних програм "Stuxnet", "Duqu" та "Flame"

Можливості / тип	Вірусна програма		
	"Stuxnet"	"Duqu"	"Flame"
Дата застосування	червень - вересень 2010 року	вересень 2011 року	травень 2012 року
Призначення	Ураження автоматизованих систем управління атомною інфраструктурою Ірану (АЕС у м. Бушер та завод зі збагачення урану в м. Натанз)	Збір конфіденційної інформації про особливості функціонування стратегіч-но важливих ядерних та індустр. об'єктів	Цілеспрямований систематичний збір даних (офісні документи, креслення тощо), можливість модифікації інформації
Географія поширення	Іран, Норвегія, країни Близького Сходу	Близький Схід	
Спосіб розповсюдження	Мережа Інтернет, знімні носи інформації типу USB Flash Drive		
Мови програмування	Асемблер, С, С++	С, програмна архітектура Microsoft Visual C++	С, С++, ШІА
Обсяг файлу	до 0,5 Мб	від 0,06 до 0,23 Мб	понад 20 Мб
Розмір програмного коду	Близько 10 тис. рядків	6-8 тис. рядків	750 тис. рядків (базовий модуль - 650 тис. рядків /6 Мб/; найменший модуль -70 тис. рядків (170-зашифров.)
Принцип дії	Заснований на використанні вразливостей (помилок) ОС сімейства Microsoft Windows		
Можливість самодуб-лювання і самознищення	Самодублювання	Самодублювання та самознищення	Самознищення
Алгоритм маску вання присут-ності в системі	Використання фальшивих серти-фікатів компаній "Realtek Semicon ductof" та "JMicron Technology"	-	Використання дійсних сертифікатів компанії "Microsoft"
Інші особливості	Залучення до розробки значних технічних та фінансових ресурсів		

При цьому, наприклад, наслідком деструктивних дій вірусу Win32.Stuxnet, розробленого групою фахівців з Ізраїлю і США за участю представників Німеччини та Великобританії, стало гальмування ядерної програми Ірану. Цьому сприяло виявлення вірусом програмованих логічних контролерів в АСУ технологічними процесами станції

(Supervisory Control And Data Acquisition), а також можливість використання (для впровадження особливого коду у "залізо" ПЕОМ АЕС) чотирьох, невідомих раніше уразливостей "нульової доби" у діючих версіях ОС Windows та двох дійсних сертифікатів від компаній Realtek і JMicron. Саме наявність останніх надавала можливість Win32/Stuxnet тривалий час уникати антивірусних радарів;

5) події 2014 – 2015 років, коли мішенями DDoS-атак із застосуванням ботмереж ставали ресурси 76 країн світу (рис.3). Найдовша DDoS-атака, зафіксована в першому кварталі 2015 року, тривала при цьому 140 годин (близько шести днів), а найбільша кількість атак, які довелося винести одному ресурсу, становила 21 атаку, тобто приблизно по 2 на тиждень. 11 з 15 DDoS-атак були спрямовані на додаток, а не на інтернет-канал. Пікові навантаження в цей період перевищували 100 Гбіт/сек.

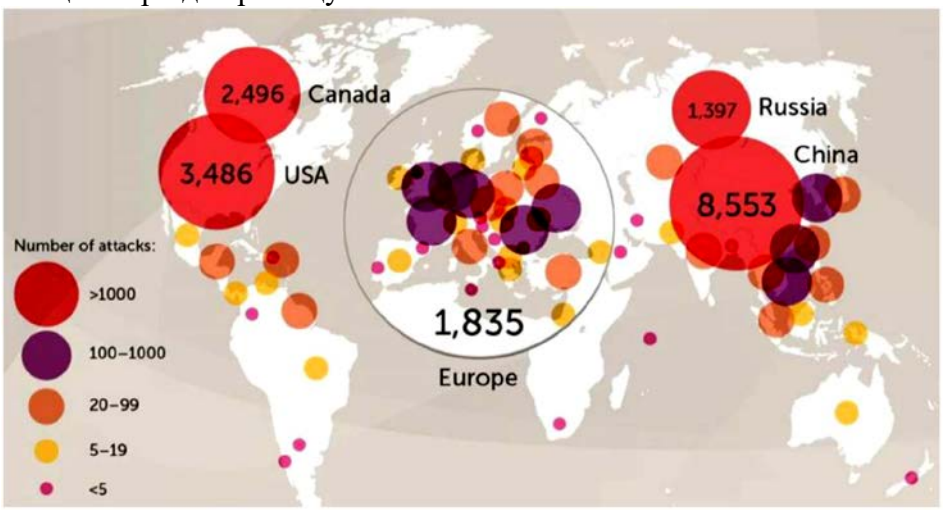

Рис. 3. Інтенсивні злочинів в інформаційному та кіберпросторах з використанням можливостей сучасних ІКТ та ІТС

Найчастіше жертвами хакерів в цей період були сервери на територіях Росії, Китаю, США та Канади, а також в країнах Європи та Азіатсько-Тихоокеанського регіону (рис.4).

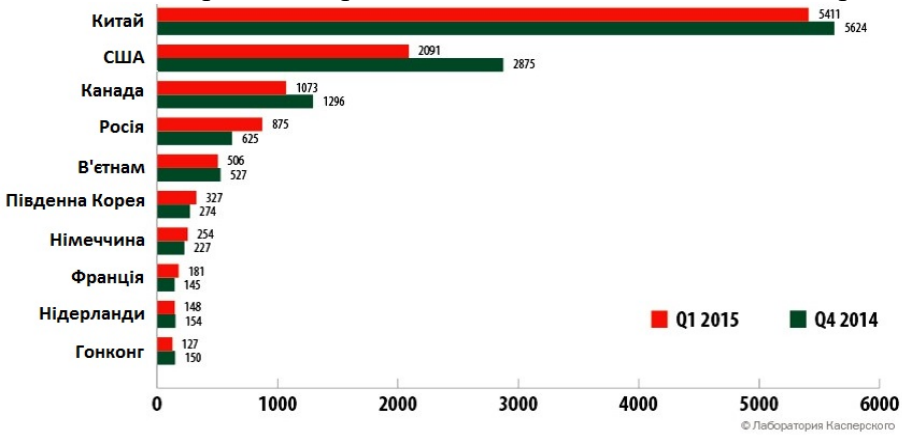

Рис. 4. Статистика злочинів у 2014-2015 р.р.

При цьому [10 – 17]:

1) 63% жертв були заздалегідь попереджені про прогалини в їх системах безпеки;
2) 38% жертв були атаковані вдруге відразу після відновлення від інциденту;
3) 52% жертв вважають, що до кінця 2015 року вони будуть атаковані повторно;
4) на відбиття атаки жертви витрачали в середньому 32 доби.

Серед низки можливих мотивів, на які розраховують сучасні кіберзлочинці та кібершахраї найбільш вживаними можуть бути: отримання слави або ідеологічної переваги; здійснення шпіонажу, помсти або шахрайства; фінансовий або матеріальний стимул тощо (рис.5). Чарльз Колоджі, віце-президент Security Products, IDC так охарактеризував такий

стан справ: “середовище кіберзлочинності більш за все зацікавлене у здійсненні фінансового шахрайства та крадіжці даних, кор-поративному шпигун- стві та підриві й навіть повному знищенні інфраструктури і процесів”.

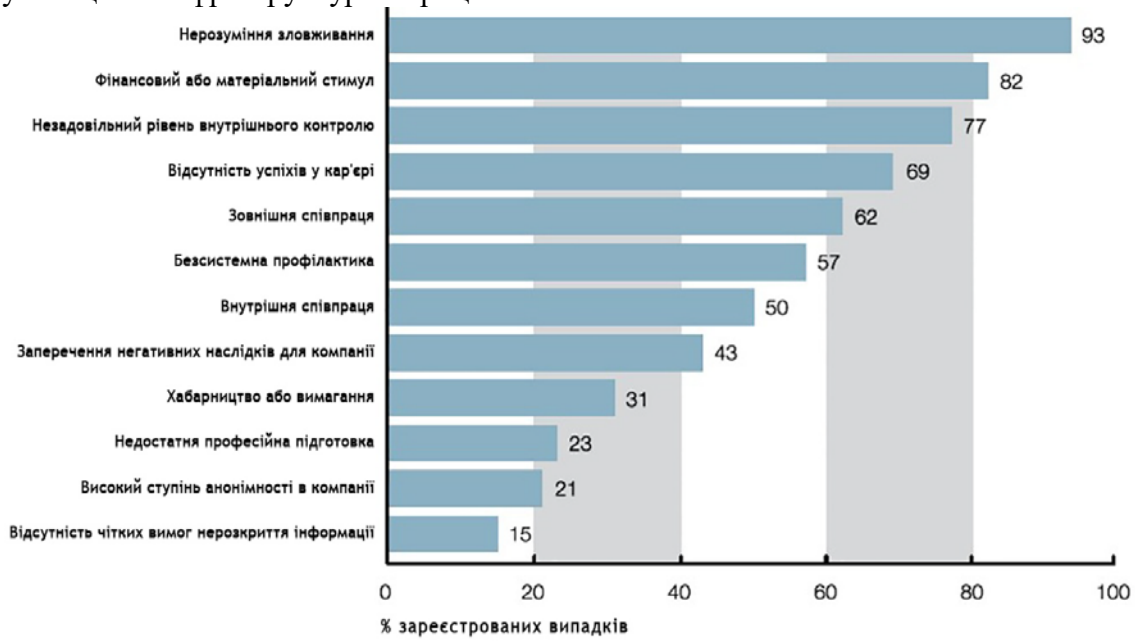

Рис. 5. Мотивація дій кіберзлочинців

Наслідком таких дій, навіть одного успішно завершеного вектора атаки, може стати або зупинка бізнесу, або його повна ліквідація (рис.6).

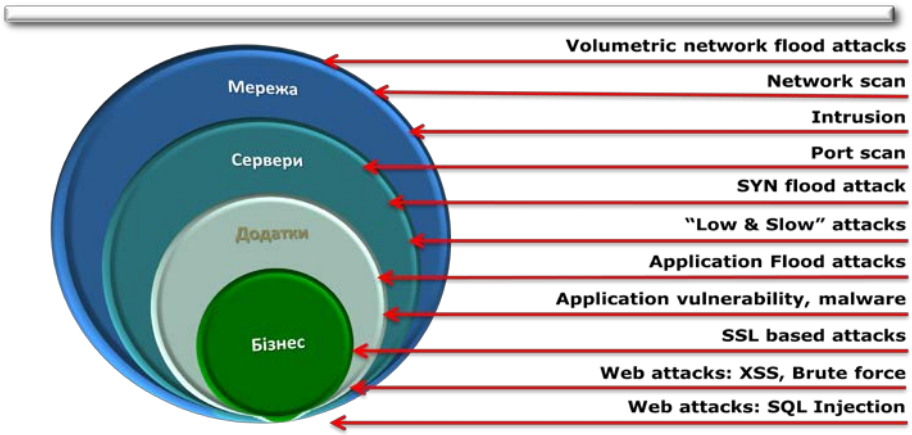

Рис. 6. Можливі наслідки від дій кіберзлочинців

При цьому, наприклад, згідно результатів досліджень проведених компанією Symantec, наслідками втрати бізнес інформації можуть бути (рис.7):

збільшення витрат (increased expenses);
зниження прибутку (decreased nevenues);
підрив торгової марки (brand damage);
втрата клієнтів (loss of customers).

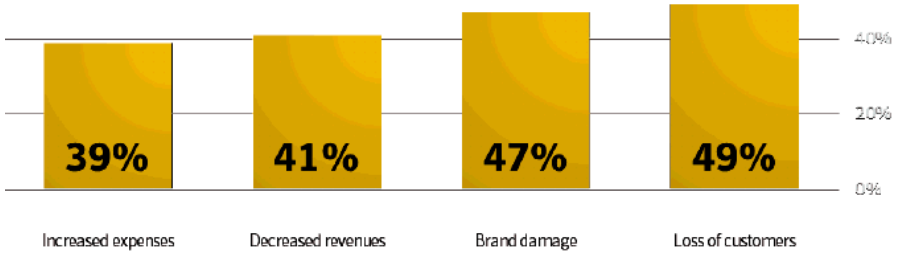

Рис. 7. Наслідки втрати бізнес-інформації для компанії

В умовах високої конкуренції щорічні світові збитки та репутаційні втрати від активних і скоординованих дій порушників, які застосовують кваліфіковано спроектовані засоби нападу, спричинені комп'ютерними вірусами, DoS та DDoS-атаками, розсиланням спаму, тощо, за оцінками організації McAfee, можуть становити від 290 до 750 мільярдів євро.

Цьому сприяло і сприяє те, що технології реалізації атак з року в рік стають все доступнішими, а нові уразливості, в тому числі критичні, виявляються останнім часом здебільшого в самих популярних додатках, а також в IT-системах, що обслуговують об'єкти фізичної, інформаційної та кіберінфраструктури. Зважаючи на таке найбільш важливим завданням сучасної інформаційної епохи на всіх рівнях, яке відіграватиме домінуючу роль у геополітичній конкуренції переважної більшості країн світу, нині є забезпечення кібербезпеки та миру у кіберпросторі. В провідних країнах світу робота в цьому напрямі ведеться з початку 80-х років минулого століття. Так, наприклад, транснаціональні компанії США в той період щорічно витрачали на утримання служб безпеки понад 2,5 млрд.$ (практично стільки, скільки і ЦРУ), а на закупівлю технічних засобів охорони – 800 млн.$. Кількість працівників служби безпеки корпорації "Дженерал моторз" налічувала близько 22 тисячі чоловік й була порівнянна із загальною чисельністю працівників ФБР. В наступні роки, з метою протидії новим загрозам і уразливостям, було досягнуто прогрес за рахунок впровадження нових заходів і засобів безпеки майже в усіх найважливіших інфраструктурних секторах світової економіки [15 – 21].

Ці заходи включали:застосування нових технологій безпеки, формування політик безпеки, забезпечення шифрування і аутентифікації тощо. Порівняльна оцінка результатів активності провідних країн світу щодо впровадження нових заходів і засобів безпеки засвідчує, що беззаперечним лідером у сфері забезпечення кібербезпеки та миру у кіберпросторі є Китай (60 %). За ним слідують Італія та Японія (рис.8).

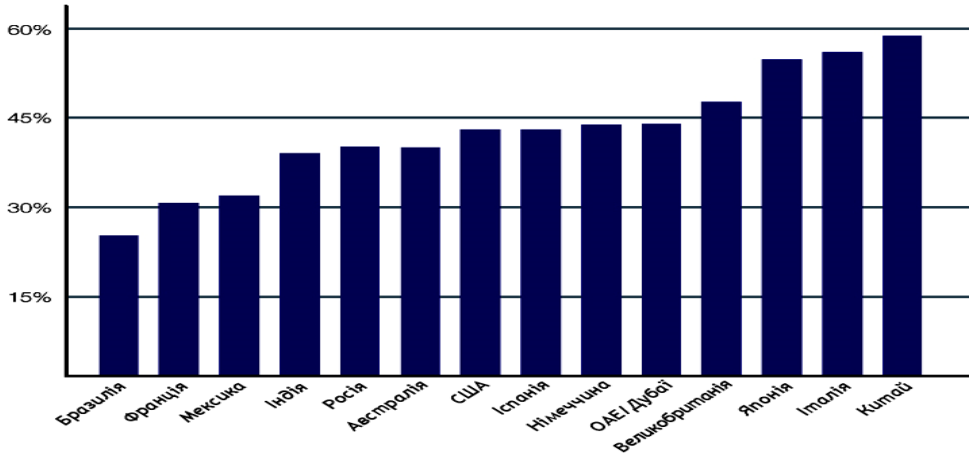

Рис. 8. Результати активності країн світу у впровадженні нових заходів і засобів безпеки

З викладеного можна зробити такі часткові висновки (рис.9).

Рис. 9. Результати аналізу стану безпеки в інформаційному і кіберпросторах

Разом з цим зростають й інвестиції в забезпечення інформаційної та кібербезпеки [7 – 21]. Так, наприклад, лише протягом 2014 -2015 років більшість держав світу (окремих компаній) збільшили власні бюджети на інформаційну та кібербезпеку приблизно на 35% (рис.10).

Рис. 10. Інвестиції в інформаційну і кібербезпеку

При цьому [7 – 21] як основні стратегічні напрями розвитку ІКБ вони пропонують використовувати (рис.11):

1) хмарні обчислення та аналітику великих даних,

2) страхування кібер-ризиків та застосу-вання ризик орієнтованого підходу до організації й забезпечення безпеки,

3) обмін інформацією про актуальні загрози з партнерами.

Рис. 11. Механізми забезпечення інформаційної та кібербезпеки

За прогнозами експертів у 2015 році обсяг ринку інформаційної та кібернетичної безпеки досягне рівня $106,3 млрд. На кінець 2017 року він становитиме $120,1 млрд., а до кінця 2020 року збільшиться до $170,2 млрд. Річний приріст інвестицій в ікб до 2020 року

зросте приблизно на 9,8%. Тим не менш реальність є такою, що витрати на інформаційну та кібербезпеку непорівнянні з ризиками втрат від впливу передусім антропогенних і техногенних загроз, а також загроз природного характеру.

Україна в рейтингу країн на які здійснювались кібератаки протягом останніх років посідає 4-9 місце (рис.12). За даними Kaspersky Security Network третина з українських користувачів (33,7%) зіштовхнулась при цьому останнім часом із загрозами, що розповсюджуються через Інтернет.

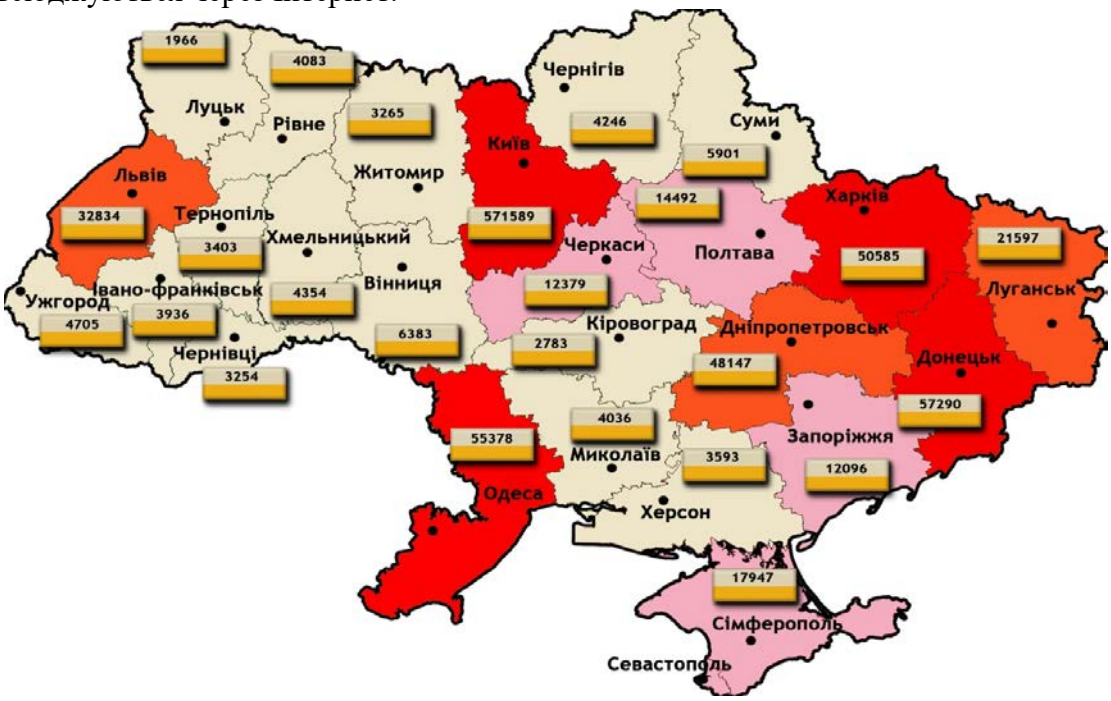

Рис. 12. Місце України у переліку країн з найбільшим ризиком зараження через Інтернет за даними Лабораторії Касперського

У 2014 році збиток від вторгнень в такі сегменти вітчизняної економіки, як газотранспортна система, водопровідні мережі, електромережі й т. ін. за результатами оцінки «регіональної» статистики скомпрометованості IP-адрес вітчизняного сегменту Internet, згідно даних CERT-UA, становив приблизно $ 200 тис. Як результат за рівнем втрат у грошовому еквіваленті наша держава з 17 місця у 2012 році опустилась у 2014 на 6-ту позицію й нині входить до 10-ки країн з найбільшим ризиком зараження через глобальну мережу (рис.13).

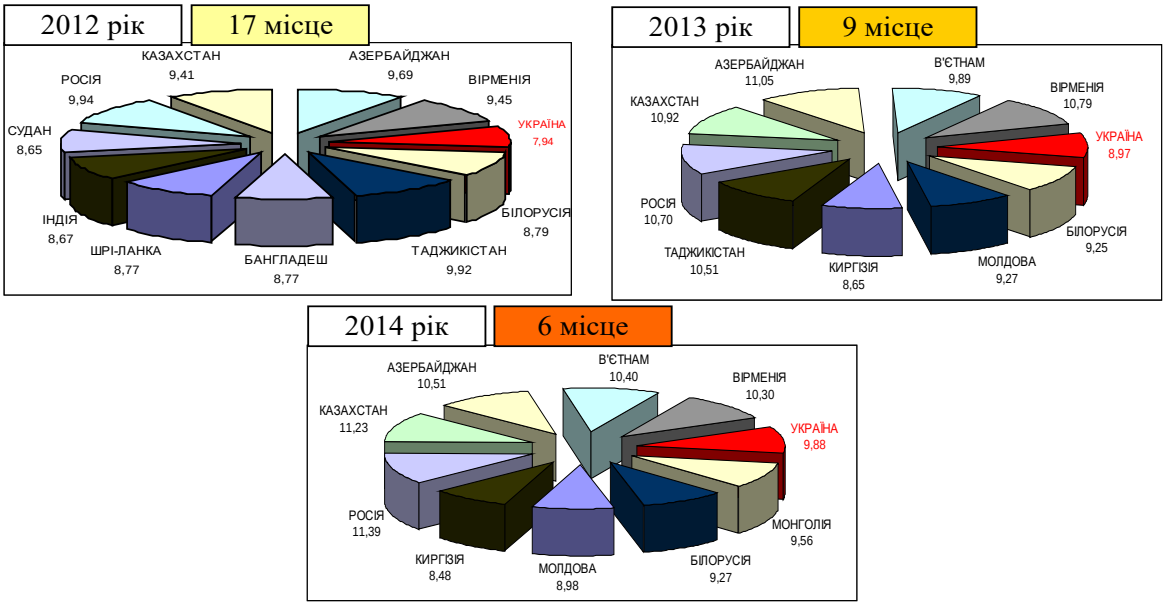

Рис. 13. Місце України у переліку країн з найбільшим ризиком зараження через Інтернет за даними Лабораторії Касперського

Зважаючи, що до кінця 2015 року приблизно 30% даних буде зберігатися в «хмарі», обсяг доступної пам'яті кожні чотири роки буде збільшуватися у 10 разів, а кількість злочинів у кіберпросторі щорічно збільшуватися не менш ніж на 10%, - саме приведе країни світу й Україну, зокрема, до нових хвиль зараження. Передусім це буде обумовлене появою нових злоякісних програм, які для обходу традиційних технологій безпеки використовуватимуть BIOS та інше вбудоване в обладнання програмне забезпечення, а також розробкою нових, більш сучасних методів їх застосування. У 2014 році результатом цього, згідно огляду «Ринок злочинів в сфері високих технологій: стан і тенденції 2014», стало "збагачення" хакерів з країн СНД на суму в понад 2,5 млрд.$. При цьому (табл.2):

Таблиця 2

Методи ""збагачення" хакерів

У СФЕРІ ВИКОРИСТАННЯ ПЛАТІЖНИХ СИСТЕМ	
скіммінг (***шимінг***) – незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток	***кардінг*** – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем
кеш-трепінг – викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки	
несанкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування	
У СФЕРІ ЕЛЕКТРОННОЇ КОМЕРЦІЇ ТА ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ	
фішинг – виманювання у користувачів Інтернету їх логіків та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти тощо	***онлайн шахрайство*** – заволодіння коштами громадян через Інтернет-аукціони, Інтернет-магазини, сайти та телекомунікаційні засоби зв'язку
У СФЕРІ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ	
піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті	***кардшарінг*** – надання незаконного доступу до перегляду супутникового та кабельного телебачення
У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
соціальна інженерія – технологія управління людьми в Інтернет просторі	***мальваре*** – створення та розповсюдження вірусів і шкідливого ПЗ
протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства	***рефайлінг*** – незаконна підміна телефонного трафіку

В Україні такому стану справ сприяє:

по-перше, відсутність єдиного державного органа, який би в масштабах країни координував питання пов'язані з інформаційною та кібербезпекою в цілому. Це приводить до:

1) неможливості побудови ефективної СЗІ, а також до стримування розвитку системи керування ІТ та електронним урядуванням;

2) неефективної витрати коштів, що виділяються на розвиток системи ІКБ;

3) розбіжностей у використанні основних положень правової бази в сфері ІКБ;

по-друге, невідповідність існуючої системи національних стандартів захисту інформації сучасним міжнародним вимогам. Це приводить до неможливості гарантування дієвості фінансово обґрунтованих і надійних мір захисту інформації (в Україні - КСЗІ, в усьому іншому світі - спеціальні галузеві стандарти або ж окремі керівництва для малого бізнесу, які визначають процес побудови системи ІКБ);

по-третє, відсутність процедури обміну інформацією про можливі способи проведення кібератак на державні організації й приватний бізнес. Це приводить до неможливості детального дослідження кібератак і, як результат, до необхідності створення певної координуючої структури, яка повинна проводити моніторинг і попереджати випадки порушення ІКБ, а також галузевих центрів, які будуть реагувати на кібератаки, специфічні для різних галузей інфраструктури держави - медіа, енергетики тощо;

по-четверте, використання неліцензованого програмного забезпечення. Це приводить до неправильного конфігурування систем захисту й використання їх при DOS і DDOS-атаках в ході інформаційного та кіберпротиборства;

по-п'яте, відсутність процесу ефективного публічного обговорення державних

ініціатив в сфері інформаційної та кібербезпеки серед експертів галузі. Це приводить до того, що фахівці в сфері ІКБ, навіть за наявності достатніх компетенцій і знань, не завжди здатні до реалізації мір із забезпечення інформаційної та кібербезпеки.

Тим не менш впродовж останніх років Україна робить певні кроки у напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю. Нормативно-правову базу у цих сферах діяльності складає:

Конвенція Ради Європи про кіберзлочинність [6], ратифікована Законом України від 7.09.2005 року № 2824-IV;

Закони України «Про інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики», «Про об'єкти підвищеної небезпеки»;

Укази Президента України, зокрема про: Доктрину інформаційної безпеки, Стратегію національної безпеки України та Воєнну доктрину України;

окремі Постанови Кабінету Міністрів та Рішення РНБОУ;

державні та міждержавні стандарти з інформаційної безпеки (рис.14).

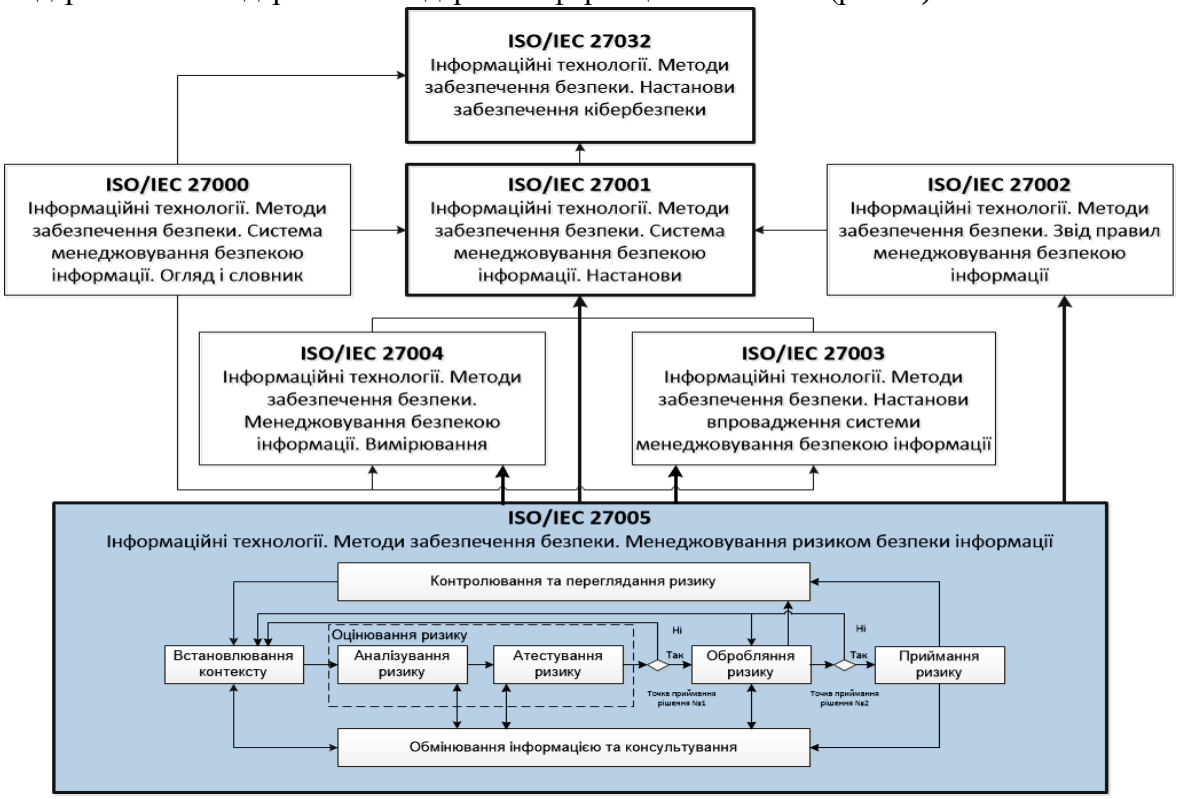

Рис. 14. Система стандартів в сфері інформаційної та кібербезпеки

При цьому ключова роль у забезпеченні кібербезпеки покладається на:

1) Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та ІТ систем;

2) Закон України «Про Основні засади розвитку інформаційного суспільства України на 2007-2015 роки» у запропонованих змінах до якого указується на необхідність створення національної системи кібербезпеки;

3) запропонований Міністерством внутрішніх справ (МВС) законопроект «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України», яким має бути запроваджено низку термінів, пов’язаних із кібербезпекою;

4) Указ президента України № 449/2014 від 01.05.2014 Про рішення Ради національної безпеки і оборони України від 28.04.2014 р. "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України";

5) Указ президента України № 744/2014 від 24.09.2014 Про рішення Ради національної безпеки і оборони України від 28.08.2014 р. "Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності".

Практичними кроками щодо реалізації існуючої нормативно-правової бази стало створення: по-перше, у 2007 році в складі Державної служби спеціального зв'язку та захисту інформації України - *Державного Центру захисту інформаційно-телекомунікаційних систем*; по-друге, у червні 2009 року при Службі безпеки України на базі спеціального підрозділу для боротьби з кіберзагрозами - *Національного контактного пункту формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені кіберзлочини* (на виконання статті 35 Конвенції про кіберзлочинність) й, по-третє, у липні 2010 року в структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми - *Департаменту боротьби з кіберзлочинністю*. Певним узагальнюючим кроком в цьому напрямку стала пропозиція СБУ створити (на виконання Указу Президента України «Про виклики та загрози національній безпеці України у 2011 р.» від 10.12.2010 року № 1119/2010) Єдину загальнодержавну систему протидії кіберзлочинності. Діяльність цих структур окрім переліченої вище нормативно-правової бази регламентується такими документами, як:

1) Кримінально-процесуальний Кодекс України (розмежовує кому і яким правопорушенням слід займатися);

2) Кримінальний Кодекс України («називає» правопорушення та визначає відповідальність за них);

3) наказ Адміністрації Держспецзв'язку від 10.06.2008 № 94, який зареєстровано в Міністерстві юстиції України від 7 липня 2008 року за № 603/15294 та який регламентує документ під назвою «Порядок діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків НСД до державних ІР в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»

Згідно з цими документами СБУ опікується глобальними питаннями нацбезпеки, МВС – безпекою громадян та кримінальними правопорушеннями в кіберсфері, а Держспецзв'язку відповідає за захист інформації, телекомунікацій та автоматизованих інформаційних систем в нашій державі (рис.15).

Рис.15. Завдання основних суб'єктів забезпечення кібербезпеки

На військовому рівні завдання щодо:

- планування та реалізації заходів протидії і нейтралізації кіберзагроз національним інтересам України у воєнній сфері;

- приведення систем кібернетичної безпеки об'єктів критично важливої інформаційної та кібернетичної інфраструктури держави до функціонування в особливий період та в умовах воєнного стану;

- впровадження новітніх IT технологій у сфері оборони, - покладені на МО та ГШ ЗС України (зок-рема на Головне управління зв'язку та інформаційних систем ГШ ЗСУ, Центральне управління захисту інфор-мації та криптології ЗСУ, ГУР МОУ тощо).

Водночас, зважаючи на:

складність структури ІКТ та національного кіберпростору;

ускладненість щодо розмежування воєнних і цивільних об'єктів критичної інфраструктури держави в інформаційному та кіберпросторах;

значну уразливість інфосфери України через надмірно широке впровадження до неї західних програмних продуктів (зокрема фірми Microsoft) та використання матеріально-технічних засобів іноземного виробництва;

відсутність у вітчизняному законодавстві визначень перш за все таких термінів, як "кібервійна", "кіберзахист" та "кібербезпека";

непрозорість розподілу обов'язків між певними відомствами, правоохоронними органами і силовими структурами України, що спеціалізуються на проблемах кіберзахисту та відсутність загальнонаціонального координаційного центру, який був би спроможним узгоджувати і координувати їх діяльність тощо, -

боротьба з кіберзлочинністю та організація протидії кіберзлочинам в нашій державі залишається організаційно розпорошеною.

З метою вирішення цієї проблеми та впорядкування відповідного нормативно-правового поля, державними безпековими інституціями проводиться цілий ряд превентивних заходів. Так, наприклад:

1) Службою безпеки України на виконання Указу Президента України «Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року № 1119/2010 було запропоновано створити Єдину загальнодержавну систему протидії кіберзлочинності, головними завданнями якої має бути: моніторинг та реагування на загрози безпеці кіберпростор; нівелювання вразливостей кіберпростору та розслідування кіберзлочинів; захист критично важливої, інформаційної та кіберінфраструктури тощо;

2) у рамках реформування підрозділів Міністерства внутрішніх справ в Україні планується створити кібернетичну поліцію. Її основним завданням буде: реалізація державної політики у сфері протидії кіберзлочинності; протидія кіберзлочинам, зокрема – у сфері використання платіжних систем, електронної комерції та господарської діяльності, а також інтелектуальної власності та ІБ; завчасне інформування населення про появу новітніх кіберзлочинів; впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини; реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів; участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності; участь у міжнародних операціях та співпраця в режимі реального часу тощо.

На найближчу перспективу, з урахуванням рішень РНБО України, заплановано:

розробити стратегію кібербезпеки України, яка має чітко визначити мету, завдання та пріоритети такої діяльності, а також структури, відповідальні за реалізацію заходів щодо протидії кібервпливам;

розробити Закон України "Про кібернетичну безпеку України";

створити Національний центр кіберзахисту та протидії кіберзагрозам.

Проте, вирішити ці завдання повною мірою на сучасному етапі розвитку української державності не вбачається можливим. Одним із низки проблемних питань є відсутність достатньої кількості кваліфікованих фахівців з проблем кіберзахисту [21 – 26]. Про незадовільне кадрове забезпечення передусім силових відомств, незважаючи на те, що ціла низка вищих навчальних закладів України здійснює підготовку фахівців за різноманітними спеціальностями галузі знань 1701 «Інформаційна безпека», було проголошено в аналітичній доповіді Національного інституту стратегічних досліджень при Президентові України «Кібербезпека: світові тенденції та виклики для України». Про це свідчать й результати аналізу нещодавно виведених з обігу стандартів вищої освіти у галузі знань 1701 Інформаційна безпека, зокрема, освітньо-кваліфікаційної характеристики та освітньо-професійної програми за напрямом 6.170101 Безпека інформаційних і комунікаційних систем, аудит яких показує, що професійні компетентності, задекларовані в цих галузевих стандартах, неповною мірою враховують стан та перспективу розвитку методів і засобів забезпечення кібербезпеки. Саме тому проблема формування проблема формування профілю навчання бакалаврів і магістрів щодо кібербезпеки, вважається нині надзвичайно актуальною.

Імовірно цей факт став й відправною точкою для внесення змін до «Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти», які призвели до ліквідації галузі знань «Інформаційна безпека» та введення в галузі знань «ІТ» нової безпекової спеціальності «Кібернетична безпека». Імплементація її в освітній процес дасть змогу сформувати базис у виді [27 – 29]:

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

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

умінь, якими мають володіти випускники (бакалаври і магістри) та фактично закласти фундамент для їх практичної роботи за напрямом організації та забезпечення кібернетичної безпеки.

Найбільш цікавими з точки зору майбутніх працедавців при підготовки фахівця (професіонала) за спеціальністю «кібернетична безпека» можуть стати знання, викладені в дисциплінах, що подані в табл.3.

Таблиця 3

Низка дисциплін, запропонованих до впровадження в освітній процес підготовки фахівців із кібербезпеки

ОКР «бакалавр»	ОКР «магістр»
«Кібернетичний простір»; «Основи інформаційної та кібербезпеки» (ІКБ); «Кібернетичне право»; «Хмарні технології в системах ІКБ»; «Програмне забезпечення систем ІКБ»; «Криптографічні механізми ІКБ»; «Інформаційна та кібербезпека сучасного підприємства»; «Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів»	«Безпека хмарних технологій та мережевої інфраструктури»; «Безпека безпроводових і мобільних мереж» «Програмне забезпечення мережевої безпеки» «Виявлення злоякісного програмного забезпечення та відновлення інформації» «Безпека Web-ресурсів» «Пентестінг та етичний хакінг «Розслідування інцидентів інформаційної безпеки»

Такий підхід до появи нових стандартів вищої освіти України, які б регламентували галузеві кваліфікаційні вимоги до випускника ВНЗ за напрямом 6 (8).125 – «Кібернетична безпека» дозволить визначити нормативний термін і зміст навчання та нормативні форми державної атестації, а також встановити вимоги до змісту, обсягу й рівня освіти та професійної підготовки такого випускника. При цьому:

- *фахова підготовка фахівців з інформаційної і кібербезпеки* для потреб як силових структур та органів державного управління, так і виробничої та банківської сфери має проводитись у єдиній системі освіти України;

- *спеціальна підготовка офіцерського складу ЗС України та інших силових структур* із загальних питань – в системі командирської підготовки та на курсах

підвищення кваліфікації.

Висновок

Сучасний етап розвитку суспільства характеризується зростанням ролі інформаційної сфери, що уявляє собою сукупність інформації, відповідної інфраструктури, а також суб'єктів, які збирають, накопичують, обробляють формують, поширюють інформацію. Інформаційна сфера, як системотворчий фактор життя суспільства, активно впливає на стан політичної, економічної, національної, оборонної й інших складових безпеки будь-якої країни світу. Це потребує адекватного стану як інформаційної, так й кібернетичної безпеки.

Будь-які спроби осмислити проблеми інформаційної та кібербезпеки впираються перш за все у відсутність єдиної термінологічної бази. Це, в свою чергу, потребує чіткого розмежування з одного боку понять кіберпростору й з іншого – простору інформаційного, з одного боку кібербезпеки й з іншого – безпеки інформаційної та інформаційно-психологічної, а також будь-яких інших видів діяльності, кінцевою метою яких є вплив на людину, групи людей або суспільство в цілому за рахунок інформаційно-комунікаційних технологій. Реалізація цих завдань має поєднувати низку заходів щодо:

проведення інформаційно-пропагандистської кампанії про значимість проблематики кібербезпеки;

вдосконалення нормативно-правового та понятійно-термінологічного апарату кібербезпеки;

створення механізму моніторингу кібернетичних втручань і загроз, а також своєчасного прийняття рішень щодо реагування на їх прояви;

забезпечення безпеки державних IP та надійності об’єктів критично-важливої інфраструктури;

підтримки вітчизняних виробників програмно-апаратного забезпечення;

підвищення компетентності фахівців різних сфер діяльності у питаннях кібербезпеки;

організації міжнародного співробітництва у сфері кібербезпеки тощо.

Список використаних джерел

1. A Solution-based Examination of Local, State, and National Government Groups Combating Terrorism and Cyberterrorism. By: Matusitz, Jonathan; Breen, Gerald-Mark. Journal of Human Behavior in the Social Environment, Feb2011, Vol. 21 Issue 2, p109-129, 21p. [Електронний ресурс]. – Режим доступу: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN.

2. Руководство по кибербезопасности для развивающихся стран. [Електронний ресурс]. – Режим доступу: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-r.pdf.

3. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

4. National Strategy to Secure Cyberspace. U.S. government via Department of Homeland Security. February 2003. p. 16. Retrieved 2008-05-18. [Електронний ресурс]. – Режим доступу: ttp://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

5. ITU's Global Cybersecurity Agenda: An International Framework for Cybersecurity. - Geneva : ITU, 2007. - 46 pp.. [Електронний ресурс]. – Режим доступу: http://www.itu.int/osg/csd/cybersecuritv/gca/index.html.

6. Про ратифікацію Конвенції про кіберзлочинність: за станом на 14.10.2010 р. / Закон, затверджений ВР України 07.09.2005, № 284-IV. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2824-15. Офіц. вид. – К.: Відомості Верховної Ради України від 10.02.2006.

7. Trend micro озвучила прогнозы по информационной безопасности на 2015 год. [Електронний ресурс]. – Режим доступу: http://www.infobezpeka.com/news/Trend-Micro-ozvuchila-prognozy-po-informacionnoy-bezopasnosti-na-2015-god/

8. В KASPERSKY LAB спрогнозировали действия киберпреступников на 2015 год. [Електронний ресурс]. – Режим доступу: http://www.infobezpeka.com/news/V-Kaspersky-Lab-sprognozirovali-deystviya-kiberprestupnikov-na-2015

9. MCAFEE LABS: в 2015 году предвидится активное использование эксплойтов и техник обхода. [Електронний ресурс]. – Режим доступу: http://www.antiviruspro.com/company/news/231/134617/

10. Аналитики GARTNER рассказали о том, что ждет мир через три-пять лет. [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/newstext.php?news_id=106919

11. Отчет HP по информационной безопасности в 2013 году. [Електронний ресурс]. – Режим доступу: http://xakep.ru/2014/02/04/61990/

12. Рынок кибербезопасности вырастет до $170 млрд к 2020 году. http://digital.report/ryinok-kiberbezopasnosti-vyirastet-do-170-mlrd-k-2020-godu/

13. KASPERSKY SECURITY BULLETIN 2014. [Електронний ресурс]. – Режим доступу: https://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/

14. Отчет McAfee Labs об угрозах. [Електронний ресурс]. – Режим доступу: http://www.mcafee.com/ru/resources/reports/rp-quarterly-threat-q3-2014.pdf

15. Прогноз угроз McAfee® Labs на 2014 год. [Електронний ресурс]. – Режим доступу: http://www.mcafee.com/ru/resources/reports/rp-threats-predictions-2014.p df

16. Security Management for Business. [Електронний ресурс]. – Режим доступу: http://blog.algosec.com

17. CyberEdge Group Отчет о противодействии киберугрозам за 2015 г. [Електронний ресурс]. – Режим доступу: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/2015-cyberthreat-defense-report-executive-summary-ru.pdf.

18. ITU-T 2015. Security in Telecommunications and Information Technology. [Електронний ресурс]. – Режим доступу: http://www.itu.int/ITU-T/edh/files/security-manual.pdf

19. CERT-UA-Інформаційна-безпека. [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/pdf/Брошура-CERT-UA-Інформаційна-безпека.pdf

20. В поисках асимметричных ответов: киберпространство в гибридной войне. [Електронний ресурс]. – Режим доступу: http://gazeta.zn.ua/internal/v-poiskah-asimmetrichnyh-otvetov-kiberprostranstvo-v-gibridnoy-voyne-_.html

21. Buryachok V., Bogush V. Guidelines for the development and implementation training profile «cyber security» in Ukraine // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 126– 131.

22. В. М. Богуш. Модель професійних компетентностей для профілю навчання «безпека інфокомунікацій». Зв'язок, № 3, 2011. – с. 11– 18

23. Бурячок В.Л. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах. / В.Л.Бурячок, Козачок В.А., Бурячок Л.В., Складанний П.М./ Науково-технічний журнал «Сучасний захист інформації» Державного університету телекомунікацій. № 3, 2015, с. 4 - 12

24. Сисоєв В. Аналіз рівня освіти та підготовки фахівців з управління ІТ та інформаційної безпеки в Україні. Режим доступу: http://www.auditagency.com.ua/blog/ISACA_research_ Education.pdf.

25. Ю. Г. Даник, Ю. М. Супрунов. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки україни. Збірник наукових праць ЖВІ НАУ «Інформаційні системи». Випуск 5. 2011. С.5-22

26. Міночкін А. І. Інформаційна боротьба: сучасний стан та досвід підготовки фахівців / А. І. Міночкін // Оборонний вісник. – К. : Центр воєнної політики та політики безпеки, 2011. – № 2. – С. 12–14.

27. http://cert.gov.ua/pdf/Брошура-CERT-UA-Інформаційна-безпека.pdf

28. Алексєєв М.М. Формалізація процесу забезпечення кібернетичної безпеки держави. / М.М.Алексєєв./ Науково-технічний журнал «Сучасний захист інформації» Державного університету телекомунікацій. № 4, 2014, с. 59 - 66

29. Бурячок В.Л. Рекомендації щодо побудови та запровадження профілю навчання «кібернетична безпека» в Україні. / В.Л.Бурячок, В. М. Богуш // Безпека інформації" Національного авіаційного університету. Том 20,2(2014). с.126 – 131

Надійшла 21.11.2015 р. Рецензент: д.т.н., проф. Толубко В.Б.