Міністерство освіти і науки України
Тернопільський національний економічний університет
Юридичний факультет
Кафедра економічної безпеки та фінансових розслідувань

МІЖДИСЦИПЛІНАРНА КУРСОВА РОБОТА

на тему:

“Кіберзлочинність як основна загроза економічній безпеці України”

Студента групи МФЕБм – 11
Галузі знань 07 – Управління та адміністрування
Спеціальності 073 “Менеджмент”
Ковальчука О. В.

Керівник: к.е.н., доцент Олійничук О. І.

Національна шкала _____
Кількість балів: _____Оцінка: ECTS _____

Члени комісії _____ _____
(підпис) (прізвище та ініціали)
_____ _____
(підпис) (прізвище та ініціали)
_____ _____
(підпис) (прізвище та ініціали

м. Тернопіль – 2017 рік

ЗМІСТ

ВСТУП

Актуальність теми. Широке використання сучасних інформаційних технологій у державних та недержавних структурах, а також у суспільстві в цілому, висуває вирішення проблем інформаційної безпеки в число основних. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини.

Залучення комп'ютерних технологій до все більшої кількості сфер діяльності держави наближає Україну не тільки до світових стандартів та тенденцій, але й до їх негативних наслідків. Економіка та безпека країни все більше залежать від технічної інфраструктури та її захищеності. Для підвищення ефективності боротьби з кіберзлочинністю Україна досить давно почала відповідні роботи, необхідні для створення власної стратегії кібербезпеки. Світовий досвід у цій області закликає до створення системи глобального обміну інформацією. Як свідчать результати досліджень та численних суспільних опитувань, питання кіберзлочинності непокоїть не тільки державу в цілому, а й кожного окремо взятого її мешканця. У цьому сенсі вивчення досвіду зарубіжних країн, які мають достатній досвід боротьби з кіберзлочинами, є досить актуальним.

Види комп'ютерних злочинів надзвичайно різноманітні. Це і несанкціонований доступ до інформації, що зберігається в комп'ютері, і введення в програмне забезпечення "логічних бомб", які спрацьовують при виконанні певних умов і частково або повністю виводять з ладу комп'ютерну систему, і розробка та розповсюдження комп'ютерних вірусів, і розкрадання комп'ютерної інформації. Комп'ютерний злочин може відбутися також через недбалість у розробці, виготовленні та експлуатації програмно-обчислювальних комплексів або через підробку комп'ютерної інформації.

Питання кіберзлочинності з різних точок зору вивчається багатьма вченими. Особлива увага цій проблемі приділяється у західних країнах. Вивчення вітчизняними вченими та дослідниками стану наукової розробленості проблем

співпраці та взаємодії правоохоронних органів різних держав у боротьбі з кіберзлочинністю, також не стоїть на місці. Втім, їх дослідження свідчать, що на сучасному етапі спеціальні дослідження з проблем кіберзлочинності є не достатньо активними. Проте необхідно відзначити, що окремі аспекти такої співпраці розглядалися в наукових роботах Ю. М. Батуріна, П. Д. Біленчука, В. Б. Вєхова, В. О. Голубєва, М. Д. Діхтяренко, Б. Х. Толеубекова і деяких інших вчених.

Метою курсової роботи є дослідження проблемних аспектів кіберзлочинності в сучасних умовах дисбалансу економічних процесів.

Основними завданнями курсової роботи є:

– дослідити понятійний апарат кіберзлочинності та кіберзлочинів, охарактеризувати види кіберзлочинів;

– провести оцінку сучасного стану, структури, динаміки кіберзлочинності у сучасних умовах розвитку;

– проаналізувати міжнародний досвід протидії кіберзлочинності на двох рівнях – міжнародному і національному;

– обгрунтувати основні проблеми чинного законодавства щодо кібербезпеки.

Об’єктом дослідження є кіберзлочинність, її тенденції та особливості в сучасних ринкових умовах.

Предметом дослідження є теоретико-прикладні аспекти кіберзлочинності як основної загрози економічній безпекці країни.

Методи дослідження. Методологічною основою цієї роботи є діалектичний метод вивчення процесів і явищ в системі кіберзлочинності. Характер поставлених дослідницьких завдань зумовив необхідність використання також таких методів, як наукового пізнання, економіко-статистичний, порівняльно-правовий, кількісного аналізу й експертних оцінок, графічний.

1. Теоретико-концептуальні аспекти кіберзлочинності у сучасних умовах дисбалансу економічних процесів

Кіберзлочинність – це сукупність комп'ютерних злочинів, де комп'ютерна інформація становить предмет злочинних посяань. Ці діяння чинять замах на безпеку сфери комп'ютерної інформації, постаючи одним із найбільш небезпечних і шкідливих явищ сучасного світу [9].

Зокрема, якщо згідно із дослідженням міжнародної компанії McAfee (МакАфі), у 2008 р. прибутки від кіберзлочинності сягали 104 млрд. доларів США, то відповідно до бюлетеня, опублікованого ФБР у 2016 р., вони перевищили 1 трильйон доларів, що в десятки разів випереджає за прибутковістю торгівлю зброєю і наркобізнес. Тому боротьба з комп'ютерною злочинністю є одним із найважливіших завдань сучасності [23].

Зазначимо, що ефективна боротьба проти транснаціональної комп'ютерної злочинності та кібертероризму вимагає тісного, швидкого, ефективного й функціонального міжнародного співробітництва усіх державних структур (і щонайперше правоохоронних органів) у розслідуванні такого роду злочинів.

Перші значущі кроки на шляху налагодження міжнародного співробітництва у протидії кіберзлочинності Україна зробила на початку XXI ст., коли 23 листопада 2001 р. в Будапешті наша держава разом із 30-ма іншими державами підписала Європейську конвенцію "Про кіберзлочинність". Представники країн, які підписали зазначену конвенцію, усвідомлюючи глибокі зміни, викликані переходом на цифрові технології та глобалізацією комп'ютерних мереж, стурбовані ризиком того, що комп'ютерні мережі й електронна інформація можуть бути використані для вчинення злочинів, вважаючи, що ефективна боротьба проти кіберзлочинності вимагає тісного, швидкого та ефективного, функціонального міжнародного співробітництва у розслідуванні таких злочинів, погодилися з необхідністю вжиття конкретних заходів у кожній країні [6].

Означеною конвенцією передбачається надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційно-телекомунікаційних

технологій як на внутрішньому, так і міжнародному рівнях. Згідно з цим документом, сторони співпрацюють шляхом застосування відповідних міжнародних угод із кримінальних питань, укладених на основі єдиного або взаємного законодавства, а також внутрішнього законодавства з метою розслідування правопорушень, пов'язаних із комп'ютерними системами та даними і збиранням доказів у електронній формі.

Наступним важливим кроком України на шляху до налагодження міждержавної співпраці у досліджуваній сфері є ратифікація 7 вересня 2005 р. зазначеної Конвенції із Додатковим протоколом до неї від 28 січня 2003 р., якою передбачене надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційно-телекомунікаційних технологій як на внутрішньодержавному, так і міжнародному рівнях; укладення домовленостей щодо дієвого міжнародного співробітництва. У зв'язку з цим одним із нагальних завдань органів державної влади і управління нашої держави варто вважати приведення чинних механізмів міжнародної взаємодії у відповідність до положень вищезгаданої Конвенції.

В Україні створена і діє досить розгалужена система забезпечення безпеки інформації, її захисту. Наявна певна законодавча база, яка складається із Законів України "Про інформацію", "Про захист інформації в автоматизованих інформаційних системах", "Про державну таємницю" тощо. Є чинними низка указів Президента та постанов Кабінету Міністрів України, якими регульовано конкретні напрями діяльності в галузі захисту інформації.

Одним із останніх кроків на цьому шляху стало ухвалення Президентом України 21 вересня 2012 р. закону "Про внесення змін до Закону України "Про ратифікацію Конвенції кіберзлочинності". За цим законом Міністерство внутрішніх справ України стає єдиним органом, який має повноваження щодо створення цілодобової контактної мережі для надання невідкладної допомоги в розслідуванні справ, пов'язаних із кіберзлочинністю, а також у виявленні осіб, звинувачуваних у цьому, та зборі доказів для цих справ [8].

Суттєвим внеском у справу розвитку міжнародної співпраці є діяльність міжнародних правоохоронних структур. До прикладу, Генеральний Секретаріат

Інтерполу ще 1994 р. задля того, щоб інформація з інших держав мобільно і в доступній формі (мова спілкування, специфічні терміни, коди злочинів тощо) надходила до національних спецпідрозділів, а також із метою оперативного обміну такими даними між країнами рекомендував державам-членам цієї організації створити Національний центральний консультативний пункт із проблем комп'ютерної злочинності. В Україні такий підрозділ з'явився 1996 р. на базі НЦБ Інтерполу.

Аналіз практики викриття та розслідування кримінальних справ у сфері високих технологій свідчить, що найбільш поширеними видами злочинів, пов'язаних із використанням комп'ютерних технологій на території сучасної України, є: злочини у сфері комп'ютерних та Інтернет-технологій – 26 %, злочини у сфері функціонування електронних платежів чи платіжних карток – 16 %, злочини у сфері телекомунікацій – 11 %, злочини у сфері використання комп'ютерних технологій при скоєнні традиційних злочинів – 47 %. До того ж самостійним видом злочинного промислу стало викрадення ідентифікаційних даних інших осіб, використовуючи які, правопорушники набувають доступ до чужих банківських рахунків, безоплатно отримуючи послуги Інтернет-провайдерів та операторів зв'язку. Такі злочини характеризуються високим рівнем технічного забезпечення, латентністю, організованістю, наявністю міжрегіональних та міжнародних зв'язків [4].

У сучасних умовах комп'ютерна злочинність має здебільшого організований і міжнародний характер, базується на стрімкому розвитку і використанні телекомунікаційних засобів повідомлень. Близько 62 % комп'ютерних злочинів вчинюються в складі організованих груп, часто на території декількох країн. Комп'ютерна злочинність також характеризується невпинним нарощуванням і вдосконаленням способів учинення злочинів, кожен із них має безліч способів реалізації [9, с. 49].

Безперечно, що розкрити такого роду злочини і викрити осіб, котрі їх скоїли, без допомоги правоохоронних органів держав-партнерів практично неможливо. З метою забезпечення ефективної протидії злочинності у сфері високих технологій

МВС України впродовж усього періоду незалежного розвитку нашої держави повсякчас уживало організаційних і практичних заходів щодо забезпечення ефективної протидії цьому сучасному виду транснаціональної злочинності.

Основні зусилля були спрямовані передусім на законодавче забезпечення боротьби з комп'ютерними злочинами і створення відповідної нормативно-правової бази; профілактику, супроводження розслідування і розкриття резонансних правопорушень у сфері комп'ютерних технологій; напрацювання методик документування і розкриття злочинів означеної категорії, проведення семінарів і тренінгів для працівників спецпідрозділів; налагодження ефективної взаємодії з міжбанківськими установами, телекомунікаційними компаніями, зацікавленими центральними державними і правоохоронними органами інших країн із метою документування злочинних груп, що мають міжнародні зв'язки.

Аналіз тенденцій і динаміки комп'ютерної злочинності в Україні дозволяє дійти висновку, що найбільш ураженими цим явищем слід вважати регіони з розвинутою інформаційною інфраструктурою, де населення широко застосовує телекомунікаційні технології (Автономна Республіка Крим, Донецьк, Дніпро, Одеса, Львів, Харків). Лідером у цій сфері є місто Київ, де перебуває майже 60 % усієї української Інтернет-аудиторії [7].

Характерною рисою злочинів, скоєних за допомогою комп'ютерних систем і телекомунікаційних мереж, є їх транскордонність, тому в основі розкриття та документування таких протиправних посягань, як нами вже зазначено вище, лежить ефективне співробітництво з правоохоронними органами інших держав і міжнародними організаціями, які спеціалізуються на протидії кіберзлочинності.

У сучасних реаліях ці завдання покладені на Департамент боротьби з кіберзлочинністю і торгівлею людьми, створений у липні 2010 р. Новостворений підрозділ зосередив основні зусилля на боротьбі з комп'ютерними злочинами проти конституційних прав і свобод людини й громадянина (комп'ютерне піратство, різноманітні способи порушення таємниці електронних повідомлень і неправомірний доступ до автоматизованих систем підрахунків голосів тощо); на боротьбі з комп'ютерними злочинами у сфері економіки (різні форми розкрадання

шляхом неправомірного доступу до автоматизованих систем забезпечення діяльності, передусім, фінансових установ, розкрадання коштів у міжнародній міжбанківській системі електронних платежів, дії, спрямовані на виготовлення кредитних або розрахункових карток, тощо); з комп'ютерними злочинами проти державної безпеки (наприклад, такі суспільно небезпечні діяння, як неправомірний доступ до державної таємниці на електронному носії, незаконний збір різного роду інформації тощо).

До актуальних питань сьогодення належить і поширення шахрайських дій, пов'язаних із рекламою так званих програм-шпигунів, «телефонних сканерів», перехоплювачів коротких текстових повідомлень, програм для виявлення місцеперебування терміналів стільникового зв'язку, що набуває популярності у зловмисників завдяки відносній нескладності вчинення таких посягань. Департамент, попри нетривалий час своєї діяльності, вже має позитивну практику припинення функціонування таких ресурсів у випадках причетності громадян України до використання коротких сервісних номерів із метою розповсюдження протиправного контенту.

Протидія злочинам у сфері високих інформаційних технологій неможлива без забезпечення належного рівня співпраці з Інтернет-провайдерами як основним витоком оперативної та доказової інформації. Отже, першочерговим завданням підрозділу боротьби з кіберзлочинністю в сучасних умовах уповні небезпідставно вважаємо залучення суб'єктів ринку телекомунікації до виявлення, документування та припинення злочинів. Із метою вдосконалення такої діяльності працівники служби беруть участь у функціонуванні робочої групи з питань взаємодії громадських організацій і державних структур у протидії кіберзлочинності, яку створено при Інтернет-асоціації України.

У перспективі досягнення згоди з суб'єктами ринку телекомунікації щодо впровадження позитивного зарубіжного досвіду, а саме створення системи добровільного обмеження доступу користувачів (абонентів) до інформаційних ресурсів із забороненим контентом, зокрема, з дитячою порнографією. У зв'язку з цим Департамент провадить відповідну системну роз'яснювальну роботу з

провідними операторами стільникового зв'язку, контент-провайдерами, хостінговими компаніями, реєстраторами доменних імен.

Міжнародне співробітництво у сфері запобігання та протидії кіберзлочинності не обмежується контактами з іноземними правоохоронними органами. У напрямку впровадження міжнародних стандартів у цій сфері Департамент наразі активно розвиває співпрацю з представниками Ради Європи та Європейського Союзу, іншими державними та неурядовими організаціями [12].

Ще одним пріоритетним напрямом роботи Департаменту є боротьба з комп'ютерними злочинами у сфері економіки. Серед основних завдань на цьому напрямку діяльності необхідно назвати протидію легалізації тіньових доходів. Аналіз схем відмивання коштів свідчить про значну зацікавленість організованої злочинності у використанні можливостей електронних платіжних систем, які дозволяють здійснювати миттєві перекази коштів із забезпеченням практично повної анонімності контрагентів. Особливий інтерес у світлі проблеми становить і те, що електронні платіжні системи не належать до розряду суб'єктів первинного фінансового моніторингу, а тому не зобов' язані інформувати наглядові органи про виявлення підозрілих транзакцій, зберігати відомості про транзакції, а також дані, що дозволяють ідентифікувати клієнта.

З метою протидії легалізації коштів, одержаних від злочинної діяльності, Департамент налагодив співпрацю з представництвами найбільш поширених в українському Інтернет-просторі електронних платіжних систем та кредитно-фінансовими установами, які надають послуги з обслуговування суб'єктів електронної комерції та мають дані про факти шахрайств, втручань у роботу комп'ютерних систем та інших протиправних посягань, учинених із використанням високих технологій.

Не менш важливим напрямом діяльності підрозділу боротьби з кіберзлочинністю є протидія обігу дитячої порнографії та сексуальному розбещенню дітей, учинюваним із використанням телекомунікаційних мереж. Доречно зазначити, що на цьому напрямі діяльності зусилля оперативного складу

зосереджені не лише на виявленні осіб, причетних до вчинення злочину, але й на ідентифікації жертв сексуальної експлуатації [12].

Позитивним прикладом такої роботи слугує співпраця з Агентством боротьби з організованою злочинністю Великобританії (БОСА) щодо причетності підданих Об'єднаного Королівства до вчинення розпусних дій стосовно українських неповнолітніх. З метою ідентифікації дітей, потерпілих від сексуальної експлуатації, поліцією Об'єднаного Королівства було надано копію вилучених у злочинців порноматеріалів. У ході аналізу отриманої інформації та подальшої перевірки вдалося встановити, що протизаконний контент виготовлено на території Київської області. У подальшому оперативні працівники ідентифікували та опитали шістьох неповнолітніх, залучених до зйомок порнографічного характеру й розпусних дій, які підтвердили факти сексуальної експлуатації, вчинені фігурантами. За цими фактами порушено кримінальну справу.

З метою превенції таких протиправних посягань спільно з правозахисними організаціями "Ла-Страда" та "ECPAT" реалізуються ініціативи щодо просвітницької діяльності, спрямованої на запобігання комерційній сексуальній експлуатації дітей в Інтернеті, створено "гарячу лінію" з питань безпеки дітей в глобальній комп'ютерній мережі. Плідна співпраця триває і в рамках меморандуму "Про взаєморозуміння", підписаного між Міністерством внутрішніх справ та компанією "Майкрософт Україна" щодо інтенсифікації заходів, спрямованих на боротьбу з розповсюдженням "дитячої порнографії" в мережі Інтернет.

Доречним буде зазначити, що цей відділ у складі силового відомства МВС України є надзвичайно молодим. Тому проблема номер один, яка постала перед Департаментом боротьби з кіберзлочинністю і торгівлею людьми МВС України, – проблема формування кадрів. Це пов'язано з тим, що фахівці, які працюватимуть у цій сфері, повинні бути як оперативниками, так і фахівцями з комп'ютерної техніки. Вочевидь, що підготовка кваліфікованих кадрів для зазначеного підрозділу – одне з нагальних завдань вищих навчальних закладів МВС України. Принагідно зазначимо, що ця проблема є досить ефективно вирішуваною. Позитивний досвід підготовки фахівців для підрозділів боротьби з правопорушеннями у сфері інтелектуальної

власності та високих технологій, накопичений у Донецькому юридичному інституті Луганського державного університету внутрішніх справ, де підготовка фахівців зазначеного профілю провадиться з 2003 р. [12].

Безумовно, специфіка протидії таким протиправним посяганням у сучасних умовах вимагає особливого підходу до комплектування підрозділу боротьби з кіберзлочинністю. Зокрема, такі працівники, на додаток до знань у сфері високих інформаційних технологій, навичок отримання інформації та збору доказів у електронній формі, повинні на достатньому рівні володіти іноземними мовами.

Слід зазначити, що наявна вітчизняна нормативно-правова база у сфері протидії злочинам в кіберпросторі лише частково задовольняє потреби часу та не завжди охоплює всі ключові елементи, які необхідні для ефективної протидії кіберзлочинам всіх рівнів складності. На сьогоднішній день в Україні діє низка Законів України та нормативних документів різних рівнів, що охоплюють проблеми забезпечення кібербезпеки держави. У ряді міждержавних нормативно-правових актів визнано, що кіберзлочинність становить загрозу не тільки національній безпеці окремих держав, а загрожує людству та міжнародному порядку.

Таким чином, можна констатувати, що вітчизняне нормативно-правове забезпечення у сфері інформаційної безпеки оперує дефініціями “кібертероризм”. Виокремлення поняття “кібертероризм” в якості самостійного є однією з найбільш дискусійних проблем в кібербезпековій сфері. Це обумовлено, по-перше, надзвичайною політизацією терміну, а по-друге – необхідністю чітко (та практично застосовано) виписати його ключові параметри так, щоб під їх дію не можна було підвести звичайні комп’ютерні злочини чи комп’ютерне хуліганство.

На сьогоднішній день в Україні протидія тероризму та боротьба із його проявами здійснюються на базі Закону України “Про боротьбу з тероризмом”, в якому тероризм визначений як “суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров’я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей”. Крім того, в

даному ж Законі наведено поняття “технологічний тероризм”, що включає в себе “злочини, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров’я людей речовин, засобів електромагнітної дії, комп’ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об’єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру” [2, с. 110]. Окремі положення даного визначення включають в себе компоненти, що можуть бути віднесені до “кібертероризму” (“…застосування засобів електромагнітної дії, комп’ютерних систем…”), однак внаслідок своєї недеталізованості не можуть бути в повному обсязі використані в практичній роботі правоохоронних органів. У додатках А, Б містяться визначення ключових термінів в сфері кібербезпеки профільними відомствами та науковими установами.

Серед запропонованих визначень кібертероризму найбільше відповідає чинній редакції Закону України “Про боротьбу з тероризмом” пропозиція Служби безпеки України. Водночас дане визначення потребує певного уточнення і в кінцевому вигляді може бути представлено наступним чином: “Кібертероризм – суспільно небезпечна діяльність, що здійснюється в кіберпросторі (або із використанням його технічних можливостей) з терористичною метою і полягає у свідомому, цілеспрямованому залякуванню населення та органів влади або вчинення інших посягань на життя і здоров’я людей”.

2. Оцінка впливу кіберзлочинності на систему безпеки банківських установ країни

У зв’язку із значним розвитком ІТ – технологій загальна чисельність способів атаки на банківські операції, котрі безпосередньо пов’язані з рахунками, зростає в геометричній прогресії, як і кількість охочих випробувати їх.

Нещодавно Ендрю Хелдейн (керівник відділу фінансової стійкості та стабільності Банку Англії) зазначив, що на сьогоднішній день найвпливовіші банки Великобританії бояться кіберзлочинів дужче боргової кризи. Також він зазначив, що хоча проблема кіберзлочинності є досить популярною і значущою станом на сьогодні, проте сама система захисту проти хакерських посягань у банківському секторі ще й зараз перебуває тільки у зародковому стані, адже фінансисти зазвичай більше дбають про ліквідність, ніж про безпеку. Однак, останні випадки кіберпограбувань (для прикладу – вкрадені хакерами кошти з рахунків у банках США на суму 45 млн. дол., змусили замислитися керівництво установ про створення нових способів і використання наявних щодо протидії комп’ютерним атакам.

На сучасному етапі ми не можемо заперечити важливості інформаційних технологій, котрі, безумовно, заполонили практично усі сфери життєдіяльності. Слід зазначити, що, така їх роль несе з собою, крім позитивних, ще й негативні явища та тенденції. Беручи до уваги статистичні дані, можна прийти до висновку, що українці все більше використовують у процесі своєї життєдіяльності блага інформаційної ери, намагаючись при цьому використовувати усі можливості електронної взаємодії через електронні засоби, або за допомогою мережі Інтернет (як приклад – спілкування, торгівля, отримання заробітної плати, оплата рахунків).

Попри зручність та швидкість засобів зв’язку, використання їх спричинило новий вид злочинів, котрі прийнято називати – кіберзлочини. Жертвами осіб, котрі вчиняють ці злочини у віртуальному просторі, стають не тільки юридичні чи фізичні особи, але і цілі відомства та держави. При чому, безпека тисяч осіб може опинитись у прямій залежності від декількох злочинців.

Кіберзлочини є п’ятим за розміром видом економічної злочинності в Україні та світі після незаконного привласнення майна, корупції та хабарництва, недобросовісної конкуренції та маніпуляції з фінансовою звітністю (рис.2.1.).

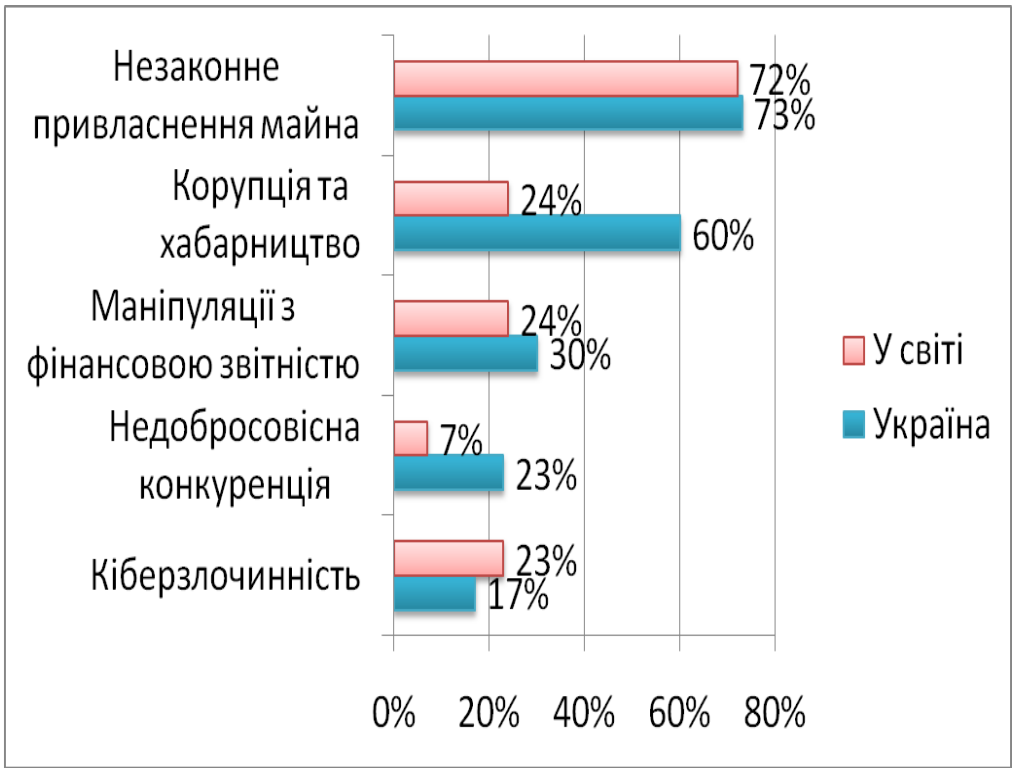

Рис. 2.1. П’ять найпоширеніших економічних злочинів в Україні та світі станом на 01.01.2016 р. [23]

Кіберзлочинність для нашої держави становить серйозну небезпеку, якою, для прикладу не була ще 5 років тому, оскільки, незважаючи на зусилля правоохоронних органів у боротьбі з кіберзлочинами, їх кількість постійно зростає.

Немає жодної держави, котра була б в змозі протистояти такому виду злочинів самостійно. Тому необхідною є активізація міжнародної співпраці по цьому питанні. Експерти зазначають, що саме хакери у зовсім недалекому майбутньому змістять тероризм і стануть загрозою номер для країн, адже, незважаючи на те, що злочини відбуваються у віртуальному світі, збиток вони завдають справжній.

Фінансовий сектор економіки, тобто банки та їх послуги, вважається одним із найбільш уразливих до кіберзлочинів.

Злочинці, як і в реальному так і у віртуальному світі не байдужі до чужого майна, звідси і випливає така їхня зацікавленість до питомої ваги цінностей пересічних громадян та юридичних осіб у банках.

Зростання популярності Інтернет – банкінгу спонукає шахраїв вигадувати найбільш витончені способи заволодіння чужими коштами. І справа не тільки в технічній стороні справи, а також в обізнаності та володінні масивом персональних даних клієнтів банку, які дуже часто опиняються в руках злочинців через необачність і довірливість громадян.

Найбільш поширеними злочинами в банківській сфері є шахрайство з використанням платіжних карток та їх реквізитів і шахрайство з використанням дистанційного банківського обслуговування (система “ клієнт – банк ”). Середній показник таких злочинів у країнах Європейського союзу складає 0,07 %, в Україні у 2015–2016 рр. кількість подібних злочинів сягала 0,045 % всіх операцій із платіжними картками (рис. 2.2).

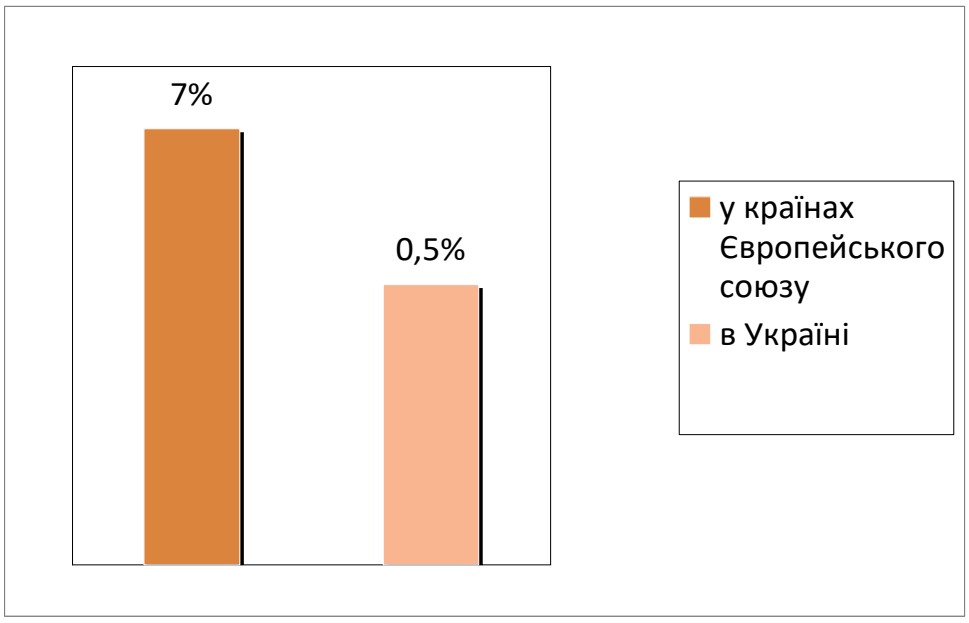

Рис. 2.2. Середній показник шахрайства з використанням платіжних карток та їх реквізитів [3]

Фахівці розглядають ці показники як показники злагодженої роботи правоохоронців і банків у протидії кіберзлочинності, проте не слід забувати, що в Україні більшість громадян після кризи 2009 р. не довіряють свої кошти фінансовим

установам, дуже багато людей не залишають на пластикових картках навіть заробітну плату, яку їм перераховують на спеціальних рахунок.

За даними Нацбанку України у 2016 році число протиправних операцій із платіжними картками в українських банках зросло до 9,8 тис. порівняно з 7,6 тис. у 2015 році, та 2,9 тис. у 2014 році, а обсяг неправомірного списання коштів збільшився майже в півтора рази і досяг 9,1 млн. грн. [23].

Варто зазначити, що банки і платіжні системи намагаються не показувати реальних збитків понесених від хакерських атак з метою збереження довіри клієнтів. Достовірний обсяг злочинності такого типу, на сьогоднішній день, оцінити достатньо важко.

Статистика, отримана від банків НБУ, показує лише збитки, відображені в балансі, але приховує зафіксовані правоохоронними органами і банками випадки шахрайських дій.

Вартий уваги і той факт, що кіберзлочини не обов'язково вчиняються особами, котрі не мають відношення до банківської установи. Тобто такі злочини можуть вчинятися і співробітниками банків, котрі, маючи доступ до усіх персональних даних клієнтів, так би мовити, "зливають" конфіденційну інформацію шахраям, отримуючи, при цьому, певну винагороду. Це розповсюджена проблема великих структур будь – якої з форм власності.

Тому для боротьби з кіберзлочинами мають значення засоби захисту як від зовнішнього, так і від внутрішнього втручання в банківські системи.

Специфіка даного виду злочинності полягає у:

– відносній комфортності, тобто готування та скоєння злочину здійснюється, практично не відходячи від " робочого місця ";

– доступності – у зв'язку з тенденцією постійного зниження цін на комп'ютерну техніку;

– географії скоєння злочинів, яка є досить широкою, але враховуючи те, що основна кількість комп'ютерів розташована у великих населених пунктах, то саме на них і припадає "левова частка" злочинності;

– віддаленості об’єкту злочинних посягань – він може знаходитись за тисячі кілометрів від місця скоєння злочину.

Якщо прослідкувати розвиток кіберзлочинності початку 2000-их років, то в цей період кіберзлочинці, або шахраї, котрі використовують дані платіжних карток, і скоюють свої злочини у мережі Інтернет прирівнювали свою діяльність до діяльності “Робін Гуда”, і вони звертали увагу на те,що вони забирають гроші у багатих і віддають їх відповідно бідним людям, яким ці гроші, на їхню думку, більш потрібні [6, с. 15].

Проте, на сучасному етапі, ми спостерігаємо, що грошові кошти викрадають так само і у людей, котрим вкрай необхідна грошова допомога, для прикладу, на лікування тяжкої хвороби.

Враховуючи вище сказане, на початку 2016 року, Незалежна асоціація банків України (НАБУ) запустила проект “Протидія кіберзлочинності”, покликаний підвищити обізнаність клієнтів банків про безпечну поведінку. Партнерами проекту виступили НБУ, МВС та 19 комерційних банків. Однак, і цей проект, нещодавно був зламаний хакерами.

За словами Генерального секретаря Інтерполу Рональда Ноубла, кібернетична злочинність вже ввійшла до переліку найбільш серйозних загроз з тих, з якими доводилося стикатися поліції. Міжнародне співтовариство перебуває сьогодні на етапі пошуку методів боротьби з цією проблемою, напрацювання єдиної політики з даного питання. Небезпеку кіберзлочинності як для всього світу, так і для України усвідомлюють правоохоронні органи нашої держави. Адже вважається, що в Україні кіберзлочинність сьогодні є однією з найбільших загроз національній безпеці в інформаційній сфері [22].

Для протистояння кібершахраям створюються спеціальні підрозділи і структури. Їхні повноваження постійно розширюють, а технічні можливості посилюють. Останній приклад – Європейський центр боротьби з кіберзлочинністю, який запрацював на початку 2016 року.

Варто зазначити, що Компанія Trend Micro Inc., Світовий лідер в технологіях хмарної безпеки, оголошує про початок співпраці з Інтерполом в рамках проведеної агентством глобальної програми по боротьбі з кіберзлочинністю.

Сучасні кіберзагрози стають все більш складними і вузьконаправленими. Адже вже йдеться про справу не з хакерами – одинаками, а з цілими мережами, які працюють по всьому світу і здатні здійснювати добре скоординовані атаки за лічені хвилини.

Ефективна протидія цій новій “інтелектуальній” різновидності злочинності вимагає глибоких технічних знань і можливості вести розслідування на міжнародному рівні. Правоохоронні органи потребують ефективного управління своїми ресурсами, включаючи організацію спільних проектів, що охоплюють різні юрисдикції та сектора економіки. Це дозволить накопичувати технічний досвід, створювати інструменти та інфраструктуру для боротьби з кіберзагрозами і зміцнення цифровий безпеки.

Не зважаючи на те, що кіберзлочинність являється відносно новим видом, з-поміж усіх відомих на сьогоднішній день суспільно небезпечних діянь, але вона постійно крокує в ногу з часом, удосконалюючись при цьому, що, безумовно, ускладнює процес виявлення та протидії їй.

Потрібно враховувати, що на практиці кошти, втрачені таким шляхом, достатньо важко відшкодувати, адже винну особу знайти дуже важко, а банк нестиме відповідальність лише у разі, що його вина була доведена.

На сучасному етапі банки плідно співпрацюють із правоохоронними органами щодо попередження такого виду злочинності, як кіберзлочинність, проте вітчизняне законодавство містить значні прогалини у цій сфері. Саме тому необхідно бути пильними і ставитись до своїх персональних даних та платіжних карток із обережністю, адже, в першу чергу, це наші кошти та заощадження.

3. Міжнародний досвід протидії кіберзлочинній діяльності в умовах макроекономічної нестабільності

У 2016 році американська компанія – розробник антивірусного програмного забезпечення McAfee, що належить Intel Corporation, виступила спонсором у створенні глобального звіту про стан світової кібербезпеки. Звіт, який був складений брюссельською компанією Security & Defence Agenda, вперше повідомив у відкритих джерелах про поточну готовність до кібератак інформаційних систем різних країн. Звіт був складений спеціально для того, щоб допомогти урядам та організаціям зрозуміти, наскільки вони кібернетично захищені в порівнянні з іншими країнами [27].

Базою для складання звіту були дослідження групи експертів у складі 80 фахівців з двадцяти семи країн. Вони надали компанії Security & Defence Agenda офіційні висновки про поточну готовність до кібератак інформаційних систем різних країн.

Крім групи експертів, до дослідження були залучені представники 250 світових лідерів у галузях IT-технології, інформаційної безпеки, захисту інформації, боротьби з кіберзлочинністю та ін. з 21 країни. Технологією дослідження передбачалося та було виконане їх анонімне опитування. За результатами роботи групи експертів та після обробки результатів опитування, Security & Defence Agenda провела ранжування та встановила рейтинг по 5-бальній системі. При цьому була досліджена поточна готовність до кібератак інформаційних систем 23 країн. Стан готовності для окремих країн був продемонстрований на прикладі рейтингу McAfee, який там використовується у якості основного засобу боротьби з кіберзлочинами - табл. 3.1.

Таблиця 3.1

Стан готовності до кібератак інформаційних систем окремих країн [27]

Країна	**Рейтинг**
1. Англія	5
2. Фінляндія, Ізраїль, Швеція	4,5
3. Данія, Естонія, Франція, Німеччина, Нідерланди, Іспанія, Великобританія, США	4
4. Австралія, Австрія, Канада, Японія	3,5
5. Китай, Італія, Польща, Росія	3
6. Бразилія, Індія, Румунія	2,5
7. Мексика	2

Найвищий результат, тобто 4,5 бали, було поставлено всього 3 країнам, які мають досить невелику площу: Швеції, Ізраїлю та Фінляндії. Ще 8 країн, включаючи США, Великобританію, Францію та Німеччину, отримали друге місце з 4 балами. Росія та Польща зайняли 4 місце з 3-бальним результатом. З тих даних звіту Security & Defence Agenda, неясно, чи були виставлені якісь бали для України.

Зі звіту Security & Defence Agenda можна виділити результати опитування експертів. Статистика свідчить про наступне:

– 57% світових експертів вважають, що в кіберпросторі відбувається “гонка озброєнь”;

– 36% вважають, що кібербезпека є важливішою проблемою, ніж протиракетна оборона;

– 43% визначили кібернетичне створення перешкод або нанесення збитків життєво важливим інфраструктурам, як найбільшу загрозу з катастрофічними економічними наслідками;

– 45% респондентів вважають, що кібербезпека настільки ж важлива, як безпека кордонів держави;

– 56% відмічають, що існує необхідність вирішення проблеми підготовки кваліфікованих кадрів з питань боротьби з кіберзлочинністю.

Звіт Security & Defence Agenda містить велику кількість зауважень від групи експертів. Найбільш суттєві з них це:

– необхідність глобального обміну інформацією в режимі реального часу;

– приватному та державному секторам потрібні фінансові стимули для поліпшення кібернетичної безпеки;

– правоохоронним органам по боротьбі з транскордонною кіберзлочинністю потрібно більше повноважень;

– необхідна методична доробка та впровадження у технології боротьби з кіберзлочинністю кращих практик інститутів міжнародної безпеки;

– існуюче дипломатичне упорядкування глобальних кібердомовленостей повинне стати більш адресованим;

– для допомоги громадянам потрібно удосконалити та розширити мережу кампаній з інформування населення про методи захисту від кібератак.

Практично всі фахівці кожної з 27 країн, які були опитані в ході складання звіту, одностайно зійшлися у тому, що для підвищення ефективності боротьби з кіберзлочинністю необхідний глобальний обмін інформацією. Крім того, всі вони відзначили необхідність не просто забезпечення обміну інформацією, а саме його оперативність та швидкість у прийняті управляючих рішень.

Європейське агентство з мережевої та інформаційної безпеки (англ.: European Network and Information Security Agency – ENISA) у своїй “Програмі надійності та захисту ключової інформаційної інфраструктури” (англ.: Cisco International Internship Program – CIIP), як і експерти, які були залучені Security & Defence Agenda, також наполягає на необхідності налагодження співпраці з метою гарантій узгодженості характерних методик кіберборотьби [5].

На сьогоднішній день у багатьох зарубіжних країнах налагоджена система співробітництва та обумовлена необхідність обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністб на ключові позиції.

Для України така тенденція є, в цілому, позитивною: поки власна стратегія щодо захисту кіберпростору тільки розробляється, надзвичайно цінною є можливість ознайомлення з досвідом країн, які працюють в зазначеному напрямку не перший рік. І хоча загальний вигляд такої стратегії може сильно варіюватися

залежно від політики та технічних суб'єктивних факторів, багато чого залишається цілком придатним. Так, навіть при поверхневому огляді стратегій кібербезпеки різних країн можна виділити об'єднуючі ключові позиції [5]:

– побудова урядової моделі, спрямованої на забезпечення кібербезпеки;

– визначення адекватного механізму, в основному, у вигляді суспільно-державного партнерства, який дозволить приватним та державним зацікавленим сторонам обговорювати та затверджувати політики, пов'язані з проблемою кібербезпеки;

– планування та визначення необхідних політик та регулюючих механізмів, чітке позначення ролей, прав і відповідальності для приватного та державного сектора у сфері протидії кіберзлочинності;

– визначення цілей та способів розвитку державних можливостей, а також необхідної законодавчої бази для участі у міжнародній боротьбі з кіберзлочинністю;

– визначення ключових інформаційних інфраструктур, у тому числі основних активів, сервісів та взаємозалежностей;

– підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв і розробка механізмів захисту для ключових інформаційних інфраструктур;

– розробка системного й інтегрованого підходів до державного управління ризиками;

– визначення цілей інформаційних програм і затвердження їх у якості пріоритетних, покликаних прищепити користувачам нові моделі поведінки та моделі роботи;

– доказ необхідності нової програми освіти, в якій робиться акцент на навчання ІТ-фахівців та професіоналів в області кібербезпеки;

– розвиток міжнародної співпраці.

Пропозиції щодо вдоскосконалення вітчизняного законодавства протидії кіберзлочинності:

1. Доцільним є проведення засідання Ради національної безпеки і оборони з метою більш повного обговорення на найвищому рівні проблем забезпечення

кібернетичної безпеки України. Це додатково дозволить формалізувати та прискорити процес підготовки законопроекту “Про кібернетичну безпеку України”, перевівши контроль за його виконанням на президентський рівень.

2. Під час підготовки законопроекту “Про кібернетичну безпеку України” та змін до чинного законодавства (з метою посилення можливостей реагування на кіберзагрози) варто максимально обережно поставитись до питань, що можуть трактуватись як заходи, спрямовані на контроль за мережею Інтернет або його обмеження в надзвичайних умовах, оскільки це може призвести до посилення тиску на політичне керівництво держави як з боку опозиційних сил так і зовнішніх суб’єктів.

3. Одночасно з підготовкою законопроекту “Про кібернетичну безпеку України” доцільним є розпочати підготовку і “Стратегії кібернетичної безпеки України”. Це дозволило б Президенту України, одночасно їх ухваленням згаданого законопроекту Верховною Радою України, оперативно закінчити формування основних концептуальних документів в даній царині.

4. Таке завдання може потребувати залучення до основної робочої групи додаткових державних та наукових установ, однак в цілому дозволить інтенсифікувати згаданий процес підготовки. Крім того, більш активне залучення наукових установ дозволить частково вирішити проблему необхідності проведення “громадського обговорення”.

5. При розгляді змін, які необхідно вносити в чинне законодавство з метою оптимізації системи кіберзахисту держави, варто розглянути можливість внесення до Закону України “Про інформацію” поняття “інформація про об’єкти критичної інфраструктури” з метою забезпечення правоохоронних органів (і зокрема – Єдиної загальнодержавної системи протидії кіберзлочинності) необхідною інформацією про стан об’єктів критичної інфраструктури, що знаходяться в приватній власності [7].

Оскільки жодна держава не може захистити себе, вживаючи заходів тільки на національному рівні, для комплексної протидії кіберзлочинності необхідні:

– гармонізація кримінального законодавства про кіберзлочини на міжнародному рівні;

– розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з урахуванням транскордонного проблеми;

– налагоджене співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні;

– механізм вирішення юрисдикційних питань у кіберпросторі [6].

Таким чином, міжнародне співробітництво є ключовим моментом у ліквідації правового вакууму, існуючого між розвитком інформаційних технологій та реагуванням на них законодавства. Процес вироблення заходів на міжнародному рівні, як показує досвід, сам по собі є комплексною проблемою. Однак це єдиний шлях забезпечити безпеку користувачів і держави від електронних посягань, а також ефективно розслідувати і переслідувати кіберзлочини.

ВИСНОВКИ

Отже, кіберзлочинність – це проблема, з якою стикнулася планета у XXI столітті, і яка обіцяє рости та поглинати все більше коштів. Незважаючи на усі заходи, що приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки порушників та зменшуючи кошти пересічних громадян. Саме тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців.

Термін “кіберзлочинність” в офіційних нормативно-правових документах не визначений. Разом з тим, саме поняття постало в лексиконі правоохоронних органів розвинених держав Європи і світу і має на увазі злочинність у сфері комп’ютерної інформації і телекомунікацій, незаконний обіг радіоелектронних і спеціальних технічних засобів, поширення неліцензійного програмного забезпечення для ЕОМ, а також деякі інші види злочинності.

Проблема профілактики і стимулювання кіберзлочинності в Україні є комплексна проблема. На сьогоднішній день закони повинні відповідати вимогам, що пред’являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній та вагомий.

У сучасних умовах комп’ютерна злочинність має здебільшого організований і міжнародний характер, базується на стрімкому розвитку і використанні телекомунікаційних засобів повідомлень. Близько 62 % комп’ютерних злочинів вчинюються в складі організованих груп, часто на території декількох країн. Комп’ютерна злочинність також характеризується невпинним нарощуванням і

вдосконаленням способів учинення злочинів, кожен із них має безліч способів реалізації.

Ефективна боротьба проти транснаціональної комп'ютерної злочинності та кібертероризму вимагає тісного, швидкого, ефективного й функціонального міжнародного співробітництва усіх державних структур у розслідуванні такого роду злочинів.

На сьогоднішній день у багатьох зарубіжних країнах налагоджена система співробітництва та обумовлена необхідність обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністб на ключові позиції.

Для України така тенденція, в цілому, є позитивною: поки власна стратегія щодо захисту кіберпростору тільки розробляється, надзвичайно цінною є можливість ознайомлення з досвідом країн, які працюють в зазначеному напрямку не перший рік. І хоча загальний вигляд такої стратегії може сильно варіюватися залежно від політики та технічних суб'єктивних факторів, багато чого залишається цілком придатним.

Так, навіть при поверхневому огляді стратегій кібербезпеки різних країн, можна виділити об'єднуючі ключові позиції:

– побудова урядової моделі, спрямованої на забезпечення кібербезпеки;

– визначення адекватного механізму, в основному у вигляді суспільно-державного партнерства, який дозволить приватним та державним зацікавленим сторонам обговорювати та затверджувати політики, пов'язані з проблемою кібербезпеки;

– планування та визначення необхідних політик та регулюючих механізмів, чітке позначення ролей, прав та відповідальності для приватного та державного сектора у сфері протидії кіберзлочинності;

– визначення цілей та способів розвитку державних можливостей, а також необхідної законодавчої бази для участі у міжнародній боротьбі з кіберзлочинністю;

– визначення ключових інформаційних інфраструктур, у тому числі, основних активів, сервісів та взаємозалежностей;

– підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту для ключових інформаційних інфраструктур;

– розробка системного та інтегрованого підходу до державного управління ризиками;

– визначення цілей інформаційних програм та затвердження їх у якості пріоритетних, покликаних прищепити користувачам нові моделі поведінки та моделі роботи;

– доказ необхідності нової програми освіти в якій робиться акцент на навчання ІТ-фахівців та професіоналів в області кібербезпеки;

– розвиток міжнародної співпраці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авчаров И. В. Борьба с киберпреступностью / И. В. Авчаров // Информатизация и информационная безопасность правоохранительных органов. XI межд. конф. – М., 2012. – С. 191 – 194.

2. Бабанін С. В. Комп'ютерні злочини за кримінальним законодавством України, США та Польщі // Співпраця поліції/міліції зі службами безпеки Інтернет-сайтів (аукціонів, соціальних мереж тощо) у боротьбі з Інтернет-злочинністю на підставі національного законодавства та законодавства, яке діє у Європейському Союзі: Тези доповідей міжнар. наук.-практ. конф. – Хмельницький, 2010.

3. Безпека банківської діяльності : монографія / Казакова Н. Ф., Панфілов В. І., Скачек Л. М., Скопа О. О., Хорошко В. О. ; за ред. проф. Хорошко В. О. – К. : ПВП «Задруга», 2013. – 282 с.

4. Войціховський А. В. Міжнародне співробітництво у боротьбі з кіберзлочинністю [Електронний ресурс] // Портал: Національна бібліотека імені В. І. Вернадського. – Режим доступу www/ URL: http://www.archive.nbuv.gov.ua/portal/.../PB-4_26.pdf

5. Голубев В. А. Угроза кибертерроризма: факторы и противодействие / В. А. Голубев // Актуальш проблема политики. – Одесса, 2012. – С. 76 - 86.

6. Голубев В. А. Проблемы борьбы с преступлениями в сфере использования компьютерных технологий : [учеб. пособие] / Голубев В. А., Гавловский В. Д. , Цимбалюк В. С.; под общ. ред. Р. А. Калюжного. – Запорожье : ЗИГМУ, 2002. – 292 с.

7. Гвоздецький В. Проблеми міжнародного співробітництва в протидії злочинності у сфері високих технологій // Вісник Академії управління МВС. – 2007. - № 2-3. – С. 6.

8. Государственные стратегии кибербезопасности [Електронний ресурс]. // Портал: Security Lab. – Режим доступу \www/ URL: http ://www. securitylab.ru/

9. Ибрагимов В. Кибертерроризм в Интернете до и после 11 сентября: оценка угроз и предложения по их нейтрализации / В. Ибрагимов. // Компьютерная

преступность и Кибертерроризм. Исследования, аналитика. Вып. 1. – Запорожье, 2004. – С. 56-61.

10. Иноземцев В. Л. К проблеме трансформации мирового порядка в XXI веке / В. Л. Иноземцев, Е. С. Кузнецова // Философские исследования. – 2001. - №3(32). – С. 4-23.

11. Конвенція про кіберзлочинність [Електронний ресурс]. - Режим доступу: zakon.rada.gov.ua.

12. Матеріали брифінгу в МВС України щодо новітніх напрацювань органів внутрішніх справ у боротьбі з кіберзлочинністю [Електронний ресурс]. – Режим доступу: mvs.gov.ua

13. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / Козлов В. Е. – М. : Горячая линия–Телеком, 2012. – 336 с.

14. Крылов В. В. Информационные компьютерные преступления : [учеб. и практ. пособие] / Крылов В. В. – М. : ИНФРА – М, 2007. – 276 с.

15. Крылов, В. В. Информационные компьютерные преступления / В. В. Крылов. – М.: Иифра-М – Норма, 2007. – 285 с.

16. Курушев М. Инициативы Европейской Комиссии по борьбе с киберпреступностью // М. Курушев // Уголовное право. – 2010. - № 1. – С. 124 – 125.

17. Ляпунов Ю. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов // Законность. – 2009. - № 1. – С. 8-15.

18. Мазуров В. А. Компьютерные преступления: классификация и способы противодействия / В. А. Мазуров. – М. : «Палеотип», «Логос», 2012. – 148 с.

19. Матвеева А. Компьютерные преступления / А. Матвеева // Человек и закон. – 2008. - № 2 – С. 44 – 54.

20. Медведовский И. Д. Атака на Интернет / Медведовский И. Д., Семьянов П. В., Леонов Д. Г. – 2-е изд., перераб. и доп. – М.: ДМК, 1999 – 334 с.

21. Наумов В. Б. Право и Интернет: Очерки теории и практики / В. Б. Наумов. – М. : Кн. дом Университет, 2002. – 430 с.

22. Еляков А. Электронный шпионаж / А. Еляков // Международная экономика и международные отношения. – 2009. - № 8. – С. 62–68.

23. Рост киберпреступности, кибертерроризма и электронного шпионажа тесно связан с вредоносными программами, направленными на хищение данных [Електронний ресурс]. — Режим доступу: http://www.niss.gov.ua/articles/454/

24. Про внесення змін до Закону України “Про ратифікацію Конвенції про кіберзлочинність”: Закон України // ВВР. – 2011. - № 5. – С. 32.

25. Стеблинська О. С. Актуальні проблеми комп’ютерної злочинності в Україні / О. С. Стеблинська // Співпраця поліції/міліції зі службами безпеки Інтернет-сайтів (аукціонів, соціальних мереж тощо) у боротьбі з Інтернет-злочинністю на підставі національного законодавства та законодавства, яке діє у Європейському Союзі: Тези доповідей міжнар. наук.- практ. конф. – Хмельницький, 2010.

26. Топ-10 країн Європи за кількістю Інтернет-користувачів [Електронний ресурс]. – Режим доступу: www.internetworldsstats.com.

27. McAfee and Security & Defence Agenda (SDA) Unveil Global Cyber Defense Report [Електронний ресурс] // Портал : An Intel Company. – Режим доступу \www/ URL :http://www.mcafee.com/

Додаток А

Визначення ключових термінів в сфері кібербезпеки профільними відомствами та науковими установами

1. Термін "кіберпростір"

Термін і визначення	Установа
Кіберпростір – середовище, сформоване у рамках поєднання віртуального і реального просторів пов'язаних між собою інформаційних, комп'ютерних та телекомунікаційних систем, а також мережевих технологій цивільного та/або військового призначення, які в процесах обробки, передачі й зберігання інформації використовують електромагнітний спектр і діють як єдине ціле.	Головне управління розвідки Міністерства оборони України
Кіберпростір (кібернетичний простір) – штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління і обробки інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи.	Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю Ради національної безпеки і оборони України
Кіберпростір - це віртуальний простір, сформований інформаційними, телекомунікаційними та інформаційно-телекомунікаційними системами (локальними комп'ютерами, локальними та глобальними мережами), у яких здійснюється виготовлення, зберігання, обробка, обмін та знищення інформації в електронному вигляді.	Служба безпеки України
Кіберпростір – віртуальний простір, створений комп'ютерною системою.	Інститут телекомунікацій і Національної академії наук України
Кіберпростір – метафорична абстракція, яка використовується у філософії та у сфері інформаційних технологій, що є (віртуальною) реальністю або окремим світом як «всередині» комп'ютерів, так і в комп'ютерних мережах.	Служба зовнішньої розвідки
Кіберпростір – віртуальний простір, в якому циркулюють електронні дані всіх комп'ютерів світу (мережева інфраструктура, радіоелектронні засоби та засоби електромагнітних випромінювань, які використовуються для передачі інформації)	Служба зовнішньої розвідки
Кіберпростір – глобальна електронна сфера, що характеризується використанням електромагнітного середовища, електронної техніки та інформаційних технологій для вирішення завдань управління та зв'язку.	Служба зовнішньої розвідки
Кіберпростір – середовище (поєднання віртуального та реального простору), яке формується у рамках пов'язаних між собою електронних систем (військові та цивільні комп'ютерні мережі, системи зв'язку та управління дротові та бездротові лінії комунікацій), які призначені для зберігання, модифікації та обміну інформацією.	Служба зовнішньої розвідки
Кіберпростір – це простір (середовище) здійснення функцій управління в живих організмах, машино-технічних системах і суспільстві. Кіберпростір – це інформаційний простір.	Центр воєнно-стратегічних досліджень

2. Термін “інформаційна інфраструктура” (“кіберінфраструктура”)

Термін і визначення	Установа
Кіберінфраструктура – сукупність організаційних і технічних структур та об’єктів, а також засобів їх взаємодії, що складають основу та забезпечують функціонування та розвиток кіберпростору	Головне управління розвідки Міністерства оборони України
Інформаційна інфраструктура держави – інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи всіх форм власності, які функціонують в державі.	Служба безпеки України
Кіберінфраструктура – мережа взаємопов’язаних інформаційних інфраструктур, телекомунікаційних мереж, комп’ютерних систем оброблення інформації, систем захисту інформації та інших компонентів, що дозволяє користувачам здійснювати у кіберпросторі різні види діяльності.	Служба зовнішньої розвідки
Кіберінфраструктура – сукупність інформаційних систем, ліній зв’язку, мереж і каналів передачі даних, засобів комунікації і управління інформаційними потоками, а також організаційних структур, правових і нормативних механізмів, що забезпечує її ефективне функціонування.	Служба зовнішньої розвідки

3. Термін “критична інформаційна інфраструктура” (“критична кіберінфраструктура”)

Термін і визначення	Установа
До критичної інформаційної інфраструктури належать наступні об’єкти інформаційної інфраструктури держави: державні електронні інформаційні ресурси, автоматизовані системи управління або електронні інформаційні ресурси де обробляється (зберігається) інформація що є власністю держави, або інформація, несанкціоновані дії щодо якої може створювати загрозу національній безпеці та обороноздатності країни (у тому числі відкрита інформація); автоматизовані системи управління, що використовуються суб’єктами Воєнної організації держави; телекомунікаційні системи загального користування; спеціальні телекомунікаційні системи; автоматизовані системи управління, що здійснюють керування виробничими та (або) технологічними процесами на об’єктах підвищеної небезпеки (у визначенні Закону України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру»); інформаційно-телекомунікаційні системи та автоматизовані системи управління, несанкціоноване втручання в роботу яких може загрожувати економічній, фінансовій, соціальній безпеці або завдати шкоди міжнародному іміджу держави.	Служба безпеки України
Критична кіберінфраструктура – це сукупність інформаційно-телекомунікаційних систем держави та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів держави (органи центрального та місцевого управління, енергетика, транспорт, зв’язок, банківська справа, підприємства, у ході діяльності яких використовуються та/або виробляються небезпечні речовини тощо) і безпеку громадян (правоохоронні структури).	Служба зовнішньої розвідки
Критично важлива інфраструктура – частина інформаційної або кіберінфраструктури, ураження або знищення якої може призвести до виникнення загроз національній безпеці шляхом повної	Головне управління розвідки Міністерства оборони

або часткової втрати працездатності інформаційним і кіберпросторами.	України

4. Термін "кібербезпека"

Термін і визначення	Установа
Кібербезпека – стан захищеності інформаційного і кіберпросторів в цілому або окремих об'єктів їх критично важливої інфраструктури від ризику стороннього кібернетичного впливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз особистим, корпоративним та/або національним інтересам.	Головне управління розвідки Міністерства оборони України
Кібербезпека – це стан захищеності кіберпростору від можливих кібератак.	Служба безпеки України
Кібербезпека (кібернетична безпека) – стан захищеності життєво важливих прав та інтересів людини, суспільства, держави в кіберпросторі від внутрішніх і зовнішніх протиправних посягань та загроз таких посягань.	Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю
Кібербезпека – система засобів забезпечення стану захищеності від застосування «психологічної кіберзброї» - інформаційного впливу на інформаційну та політичну інфраструктуру противника.	Служба зовнішньої розвідки
Кібербезпека – комплекс заходів, спрямованих на захищеність інформації та інфраструктури підтримки (обладнання, програмного забезпечення, даних і персоналу) від випадкових або навмисних дій природного або штучного характеру, які можуть завдати збитків суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації, інфраструктурі підтримки.	Служба зовнішньої розвідки
Кібербезпека – стан захищеності кібернетичної інфраструктури (сукупність організаційних, нормативно-правових, технічних та інших) заходів з метою запобігання кібератакам та забезпечення кібербезпеки.	Служба зовнішньої розвідки
Кібербезпека – стан, за якого досягнуто здатність (держави в цілому, певної сфери) утворити та підтримувати інформаційний простір необхідної повноти (достатності) з регламентованим доступом до IP для здійснення процесів управління визначеними сферами (галузями) діяльності, а також забезпечити його всебічний захист від зовнішніх та внутрішніх загроз	Центр воєнно-стратегічних досліджень

5. Термін "кіберзахист"

Термін і визначення	Установа
Кіберзахист - це процес забезпечення кібербезпеки.	Служба безпеки України
Кіберзахист – сукупність заходів захисту від різних проявів стороннього кібернетичного впливу власних інформаційного і кіберпросторів, інформаційних систем, мереж, сил, засобів та інших об'єктів критично важливої інфраструктури держави, ураження та/або знищення яких може поставити під загрозу суспільну і державну	Головне управління розвідки Міністерства оборони України

безпеку.	
Кіберзахист – багаторівневий захист комп'ютерів, комп'ютерних систем і мереж та захисту інформації, яким здійснюється виявлення порушень і збоїв роботи, спрацьовує система обмеженого доступу та вживаються інші заходи кібернетичної безпеки і протидії кіберзлочинності.	Служба зовнішньої розвідки
Кіберзахист - сукупність методів і заходів, що забезпечують функціонування кіберпростору та циркуляцію інформації в ньому за умов впливу загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.	Служба зовнішньої розвідки
Кіберзахист – реалізація у кіберпросторі комплексу організаційних, нормативно-правових, технічних та інших заходів з метою запобігання кібератакам та забезпечення кібербезпеки.	Служба зовнішньої розвідки

6. Термін "кібератака"

Термін і визначення	**Установа**
Кібератака - це цілеспрямовані дії по реалізації кіберзагроз.	Служба безпеки України
Кібератака – сукупність дій (операцій) протиборчих сторін у кіберпросторі, що реалізуються ними за рахунок використання комп'ютерної та/або спеціальної техніки й програмних засобів і мають за мету порушення штатного (нормального) режиму функціонування інформаційно-телекомунікаційних систем один одного.	Головне управління розвідки Міністерства оборони України
Кібератака – це послідовність дій, що застосовується будь-ким в комп'ютерних мережах для досягнення несанкціонованих цілей, тобто дія, спрямована на порушення правил функціонування комп'ютерних систем і мереж і т.п. у сфері інформаційних технологій.	Служба зовнішньої розвідки
Кібератака – дія в кіберпросторі, спрямована проти інформаційно-телекомунікаційної системи з метою впливу на неї шляхом порушення її функціонування, отримання контролю над системою, корекції, копіювання, вилучення, пошкодження, впровадження чи знищення даних, створення умов для зміни поведінки її користувачів.	Служба зовнішньої розвідки
Кібератака – дії, спрямовані на ураження комп'ютерних систем з метою порушення цілісності, доступності та конфіденційності інформації, що може призвести до порушення функціонування державних, фінансових, медичних установ тощо.	Служба зовнішньої розвідки
Кібератака – спосіб нападу у кіберпросторі або з його використанням.	Служба зовнішньої розвідки

7. Термін "кіберзлочин" ("кіберзлочинність")

Термін і визначення	**Установа**
Кіберзлочин - це кіберправопорушення, передбачене кримінальним законодавством, яке несе у собі суспільну небезпеку.	Служба безпеки України
Кіберзлочин – кримінальна дія здійснена у кіберпросторі з використанням засобів електронно-обчислювальної техніки.	Головне управління розвідки Міністерства оборони

	України
Кіберзлочин (кібернетичний комп'ютерний злочин) - протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер (наприклад спотворення інформації про стан об'єкту в каналі зворотного зв'язку, спотворення керуючого сигналу в каналі прямого зв'язку, використання шкідливого програмного забезпечення тощо); створення та використання у злочинних цілях певної кібернетичної (комп'ютерної) системи; використання у злочинних цілях існуючих кібернетичних (комп'ютерних систем).	Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю Ради національної безпеки і оборони України
Кіберзлочинність – злочини, головним інструментом яких є інформаційно-комунікаційні технології.	Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України

8. Термін "кібертероризм"

Термін і визначення	**Установа**
Кібертероризм – свідомі та цілеспрямовані дії осіб або організованих груп, що спрямовані на порушення функціонування інформаційних комп'ютерних систем і телекомунікаційних мереж та несанкціоновану модифікацію комп'ютерних даних з метою: дезорганізації роботи критично важливих елементів інфраструктури держави; дестабілізації суспільно-політичної обстановки в державі та/або ускладнення міжнародних відносин; створення небезпеки для життя і здоров'я людини або задля її залякування; завдання фінансово-майнових збитків або приведення до інших суспільно-небезпечних і негативних наслідків для суспільства та держави в цілому.	Головне управління розвідки Міністерства оборони України
Кібертероризм (комп'ютерний тероризм) передбачає інформаційні атаки на обчислювальні центри, центри управління воєнними мережами й медичними закладами, банківські та інші фінансові мережі, засоби передачі даних за допомогою комп'ютерних мереж. Інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, що здійснюються терористичними угруповуваннями або окремими особами, є основною формою кібертероризму.	Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю Ради національної безпеки і оборони України
Кібертероризм – суспільно небезпечні діяння у кіберпросторі, які полягають у свідомому, цілеспрямованому залякуванню населення та органів влади або вчинення інших посягань на життя і здоров'я людей з метою досягнення злочинних цілей.	Служба безпеки України
Кібертероризм – використання комп'ютерних мереж в якості засобу для порушення функціонування важливих національних інфраструктур (енергетичних, транспортних, урядових тощо) або примушення чи залякування уряду або цивільного населення.	Служба зовнішньої розвідки
Кібертероризм – навмисні, політично вмотивовані атаки на інформаційні комп'ютерні системи, комп'ютерні атаки та дані, що створюють загрозу загибелі людей, спричинення значної майнової шкоди або настання інших суспільно-небезпечних наслідків.	Служба зовнішньої розвідки

Кібертероризм – умисне перешкоджання функціонуванню автоматизованих систем управління державою, об’єктів критичної інфраструктури, вплив на громадян, у т.ч. для вирішення потреб терористичної діяльності (пропаганди, оперативного зв’язку тощо).	Служба зовнішньої розвідки

Додаток Б

Терміни та їх визначення, що пропонуються Національний інститутом стратегічних досліджень для включення до законопроекту “Про кібернетичну безпеку України”

1. Кіберпростір - об’єкти інформаційної інфраструктури що керуються інформаційними (автоматизованими) системами управління та інформації, що в них циркулює.

2. Кіберпростір держави - об’єкти інформаційної інфраструктури держави, що керуються інформаційними (автоматизованими) системами управління та інформації, що в них циркулює.

3. Інформаційна інфраструктура - сукупність об’єктів телекомунікаційних систем всіх форм власності.

4. Інформаційна інфраструктура держави - сукупність об’єктів телекомунікаційних систем всіх форм власності, що розташовані на території держави або доступ до яких здійснюється з території держави.

5. Критична інформаційна інфраструктура держави - сукупність інформаційно-телекомунікаційних систем держави та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів держави і безпеку громадян. До таких систем відноситься: державні електронні інформаційні ресурси, автоматизовані системи управління або електронні інформаційні ресурси де обробляється (зберігається) інформація що є власністю держави, або інформація, несанкціоновані дії щодо якої може створювати загрозу національній безпеці та обороноздатності країни (у тому числі відкрита інформація); автоматизовані системи управління, що використовуються суб’єктами Воєнної організації держави; телекомунікаційні системи загального користування; спеціальні телекомунікаційні системи; автоматизовані системи управління, що здійснюють керування виробничими та (або) технологічними процесами на об’єктах підвищеної небезпеки (у визначенні Закону України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру»); інформаційно-телекомунікаційні системи та автоматизовані системи управління, несанкціоноване втручання в роботу яких може загрожувати економічній, фінансовій, соціальній безпеці або завдати шкоди міжнародному іміджу держави.

6. Кібербезпека - стан захищеності кіберпростору в цілому або окремих об’єктів його інфраструктури від ризику стороннього кібернетичного впливу (кібератак), за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз особистим, корпоративним та/або національним інтересам.

7. Кіберзахист - сукупність методів і заходів організаційного, нормативно-правового та технічного характеру спрямованих на забезпечення кібербезпеки.

8. Кібератака – цілеспрямовані дії, які реалізуються в кіберпросторі (або за допомогою його технічних можливостей), що призводять (можуть призвести) до досягнення несанкціонованих цілей (порушення конфіденційності, цілісності, авторства, спостережності та доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість, психологічний та психічний стан громадян).

9. Кіберзлочин – кримінальна дія, відповідальність за яку передбачено кримінальним законодавством, яка здійснена (здійснюється) у кіберпросторі (або за допомогою його технічних можливостей).

Додаток В

Світовий збиток кібератак перевищує 600млрд. $