УДК 343.9

ГУЦАЛЮК М.В., *кандидат юридичних наук, с.н.с., доцент*,
Міжвідомчий науково-дослідний центр з проблем боротьби
з організованою злочинністю при РНБО України

ВДОСКОНАЛЕННЯ ЧИННОГО ЗАКОНОДАВСТВА З ПИТАНЬ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Анотація. *В статті досліджуються питання інформаційної безпеки та протидії кіберзлочинності. Пропонуються напрями вдосконалення чинного законодавства у даній галузі та запровадження безпечного сегменту Інтернет – ID-web.*

Ключові слова*: кіберзлочинність, кібербезпека, міжнародне співробітництво, ID-web.*

Аннотация. *В статье исследуются вопросы информационной безопасности и противодействия киберпреступности. Предлагаются направления совершенствования действующего законодательства в данной сфере и внедрения безопасного сегмента Интернет – ID-web.*

Ключевые слова: *киберпреступность, кибербезопасность, международное сотрудничество, ID-web.*

Summary. *The article deals with the issues of cybersecurity and cybercrime. The improvement of the legislation in this area and the introduction of safe ID-web Internet are proposed.*

Keywords: *cybercrime, cybersecurity, international cooperation, ID-web.*

Постановка проблеми. Поява інформаційно-комунікаційних технологій (далі – ІКТ) спричинила істотний вплив на розвиток як світової економіки, так і міжнародної безпеки. Ці технології дають змогу отримувати величезні економічні та соціальні вигоди. Разом з цим, вони також можуть використовуватися в цілях, несумісних з підтриманням безпеки, внаслідок чого в останні роки помітно підвищився рівень ризику щодо вчинення злочинів із використанням ІКТ.

Результати аналізу наукових публікацій. Експерти Всесвітнього економічного форуму в Давосі підготували та у січні 2017 року опублікували щорічну доповідь про глобальні ризики у світі під назвою “Global Risks Report 2017”. Виходячи з її концептів, на третьому місці за важливістю для світової спільноти перебувають технологічні ризики – крадіжки персональних даних, махінації з ними, масштабні кібератаки та кіберзлочинність [1].

Згідно зі звітом “2016 Norton Cyber Security Insights Report” американської компанії Symantec, світового лідера в галузі рішень інформаційної безпеки, у 2016 році тільки з 21-єї країни зазнали загроз від кіберзлочинності 689 мільйонів чоловік. Це явище стало настільки поширеним, що багато людей однаково побоюються он-лайн і реальних ризиків. Відповідно до досліджень Європолу, втрати держав-членів ЄС від кіберзлочинності складають 265 мільярдів євро в рік, а для світової економіки ця цифра становить близько 900 мільярдів євро. І це тільки фінансовий бік проблеми [2].

Виходячи із сучасних реалій, заслуговує на увагу позиція колишнього помічника генпрокурора з питань національної безпеки в Міністерстві юстиції США Джона Карліна, що однією із тенденцій поширення кіберзагроз у майбутні 3 – 5 років станутьсаме кіберзлочини за підтримки урядів, а також атаки, що можуть здійснюватися урядовими кібершпигунами заради отримання фінансової вигоди [3]. Це підтвердив і Генеральний секретар НАТО Йенс Столтенберг, який повідомив під час прес-конференції в Брюсселі

15 лютого 2017 року, що Альянс стикається з серйозними кібератаками, за якими стоять хакери, які діють не тільки у власних інтересах, а також й держави-агресора [4]. Це особливо небезпечно для України, яка стала своєрідним полігоном для відпрацювання таких атак. Наприклад, тільки протягом двох місяців наприкінці 2016 року було скоєно понад 6,5 тисячі кібератак на об’єкти п’яти відомств і 31 державного інформаційного ресурсу, багато з яких організовані зі сторони РФ [5].

Особливе занепокоєння сьогодні викликає можливість вчинення терористичних актів за допомогою ІКТ на об’єктах критичної інфраструктури. У 2015 та 2016 роках на енергетичний та фінансовий сектор України було здійснено низку потужних кібератак, які призвели до значних шкідливих наслідків. Питання забезпечення безпеки на об’єктах критичної інфраструктури розглянуте 13 лютого 2017 року під час головування України в Раді Безпеки ООН, де була прийнята відповідна Резолюція № 2341 (2017). У документі зазначено, що Рада Безпеки ООН рекомендує посилити інформованість про проблеми, які створюють терористичні атаки на об’єкти критичної інфраструктури, і закликає всі країни удосконалювати стратегії зменшення ризиків таких нападів; зміцнювати міжнародні партнерські відносини із зацікавленими сторонами, як державними, так і приватними, з метою обміну інформацією та досвідом для відновлення після заподіяної ними шкоди. Також усі держави, які в змозі робити це, повинні сприяти в забезпеченні ефективного нарощування потенціалу, професійної підготовки, технічної допомоги, передачі технологій і реалізації програм з тим, щоб всі держави могли досягти захисту критично важливих об’єктів інфраструктури від терористичних нападів [6].

В зв’язку з зазначеним сьогодні в Україні разом з докорінними змінами у зовнішньому та внутрішньому безпековому середовищі, появою нових викликів та загроз в умовах гібридної війни активно реформується сектор безпеки і оборони з урахуванням специфіки кіберпростору. Так, Указом Президента України від 26 травня 2015 року № 287/2015 затверджено Стратегію національної безпеки України, якою визначені основні пріоритети забезпечення кібербезпеки в державі.

З метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави окремим документом розроблена і затверджена Указом Президента України від 15 березня 2016 року № 96/2016 Стратегія кібербезпеки України.

Указом Президента України від 13 лютого 2017 року № 32/2017 затверджено Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”, у якому визначені термінові та короткострокові завдання Кабінету Міністрів України, правоохоронним органам щодо захисту інформації в інформаційно-телекомунікаційних системах, та зокрема на об’єктах критичної інфраструктури.

Дослідженням проблемних питань протидії кіберзлочинності займалися такі вітчизняні науковці, як Н.М. Ахтирська, П.Д. Біленчук., К.І. Бєляков, В.М. Бутузов, В.Д. Гавловський, М.А. Погорецький, В.Г. Хахановський, В.П. Шеломенцев, О.М. Юрченко та інші. Проте стрімкий розвиток інформаційних технологій та способів і методів протиправної діяльності у кіберпросторі спонукає для подальших досліджень.

Метою статті є продовження дослідження щодо протиправної діяльності в глобальній мережі Інтернет та надання пропозицій для удосконалення системи безпеки в українському сегменті глобальної мережі Інтернет.

Виклад основного матеріалу. Враховуючи зростаючі масштаби кіберзлочинності, з метою розробки юридичних механізмів протидії загрозам у комп’ютерних мережах у травні 2011 року Міжнародний союз електрозв’язку і Управління ООН з наркотиків та

злочинності підписали угоду про боротьбу з кіберзлочинністю. Для прийняття конкретних заходів, спрямованих на обмеження комп’ютерних загроз, ООН розробила Глобальну програму кібербезпеки, в якій визначено п’ять основних напрямів [7]:

1) правові заходи;
2) технічні та процедурні заходи;
3) організаційні структури;
4) програма підвищення компетентності;
5) міжнародне співробітництво.

У зв’язку з тим, що основною ознакою кіберпростору є відсутність міждержавних кордонів, особливого значення набуває правове регулювання суспільних відносин, які виникають під час виявлення та розслідування протиправної діяльності в ньому. Зловмисник може знаходитися в одній державі, активувати кібератаку з інформаційного ресурсу, розташованого в іншій, а збитки будуть завдані фізичній чи юридичній особі, яка знаходиться в третій державі. При цьому шкідливі програми можуть перетинати ще низку кордонів, ніяк не повідомляючи про це уповноважені державні органи.

Сьогодні можна виділити п’ять груп міжнародних і регіональних нормативно-правових актів, які регулюють суспільні відносини у сфері протидії кіберзлочинності. В них входять документи, розроблені під егідою:

- Ради Європи Європейського союзу,
- Співдружності Незалежних Держав або Шанхайської організації співпраці,
- міжурядових африканських організацій,
- Ліги арабських держав і (V) Організації Об’єднаних Націй.

Існують і інші теоретичні підходи щодо регулювання проблем кіберпростору. Так, науковець Джон Перрі Барлоу ще у 1996 році запропонував розробити та прийняти Женевську декларацію незалежності кіберпростору, яка б передбачала функціонування Міжнародного суду у зв’язку тим, що кіберпростір не належить до жодної країни і є інтернаціональним. Проте цей документ так і не був прийнятий [8].

Серед основних міжнародних нормативно-правових документів щодо протидії кіберзлочинності, у тому числі організованої, слід виокремити такі:

– Конвенція Організації Об’єднаних Націй проти транснаціональної організованої злочинності (United Nations Convention against Transnational Organized Crime), підписана у м. Палермо 12 грудня 2000 року та ратифікована із застереженнями і заявами Законом України від 04.02.04 р. № 1433-IV [9];

– Європейська конвенція про взаємну допомогу у кримінальних справах (European Convention on Mutual Assistance in Criminal Matters), підписана у м. Страсбурзі 20 квітня 1959 року та ратифікована із заявами і застереженнями Законом України від 16.01.98 р. № 44/98-ВР [10];

– Конвенція про кіберзлочинність (Convention on Cybercrime), підписана 23 листопада 2001 року в м. Будапешті і ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV [11].

Поряд з нормативно-правовим забезпеченням, заходи боротьби з кіберзлочинністю повинні також супроводжуватися середньостроковими і довгостроковими стратегічними цілями, спрямованими на захист інформаційних ресурсів і притягнення розробників злочинних схем до відповідальності.

Більшість країн розробили та затвердили відповідні нормативно-правові документи (стратегії), в яких визначаються напрями протидії загрозам в інформаційній сфері. До таких країн, зокрема, належать США, Франція, Німеччина, Великобританія, Канада, Японія та інші.

Надзвичайно великого значення захисту кіберпростору надає Організація Північноатлантичного договору (НАТО). У країнах Альянсу, економіка яких розвивається у складному середовищі, кіберзагрози стають усе більш поширеними, складними і руйнівними, а кібератаки стали частиною гібридної війни. НАТО і його союзники покладаються на сильну колективну оборону на основі тісного співробітництва між його учасниками і визначають кіберзахист одним з основних своїх завдань, а кіберпростір – як область операцій, в яких НАТО має захищати себе так само ефективно, як це робить у повітрі, на суші і на морі [12].

Належне місце займає кібербезпека і в Європейському Союзі. Стратегія кібербезпеки ЄС 2013 року стала першим всеохоплюючим документом Європейського Союзу в даній сфері. Документ охоплює усі аспекти кіберпростору: внутрішній ринок, правосуддя, внутрішню та зовнішню політику.

Пріоритетами міжнародної політики ЄС у кіберпросторі, як їх визначає Стратегія, є:

– свобода та відкритість: стратегія визначає принципи користування основоположними правами людини та громадянина у кіберпросторі;

– застосування законодавства ЄС у кіберпросторі у тій самій мірі, як і у фізичному світі. Відповідальність за безпеку кіберпростору лежить на всьому глобальному суспільстві: від пересічних громадян до держав;

– розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством [13].

Як уже зазначалося, усі розвинені країни з урахуванням міжнародних угод, розробляють свої власні нормативні документи з питань протидії кіберзлочинності та кібербезпеки. Найбільш розвинену систему таких нормативно-правових актів мають США. Не дивлячись на те, що в цій країні були прийняті одні з найперших у світі законів в даній галузі і сьогодні функціонують такі закони, як: Закон “Про злочини, пов’язані з засобами доступу” (Fraud and related activity in connection with access devices) [14], Закон “Про злочини, пов’язані з комп’ютерами” (Fraud and related activity in connection with computers) [15], Закон “Про перехоплення електронних повідомлень та прослуховування переговорів” (Wire and Electronic Communications Interception and Interception of Oral Communications) [16] тощо.

Законодавство США постійно вдосконалюється залежно від загроз, які постають перед суспільством. Так, наприклад, після терористичних актів 11 вересня 2001 року був прийнятий так званий “Патріотичний акт”, – The USA Patriot Act: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism). Відповідно до цього документа ФБР, Агентству національної безпеки були надані широкі права щодо електронного спостереження та розслідування кіберзлочинів, зокрема ст. 202 документа передбачала право на перехоплення голосових повідомлень при розслідуванні комп’ютерних злочинів, ст. 209 полегшувала доступ до електронних повідомлень (електронна пошта), ст. 210 розширила перелік даних, які відповідно до запиту можуть отримувати правоохоронні органи у провайдерів, наприклад, IP користувача, номер кредитної картки користувача, якою він оплачував інтернет-послуги тощо, що дало змогу ідентифікувати кіберзлочинців та відстежувати їх діяльність в мережі. Проте у 2015 році положення цього закону були відмінені у зв’язку з порушенням прав людини [17].

Нещодавно були прийняті Закон “Поширення інформації про кібербезпеку” (Cybersecurity Information Sharing Act (CISA), 2015 [18] та “Система покращення кібербезпеки критичної інфраструктури” (Framework for Improving Critical Infrastructure Cybersecurity) 2016 [19];

Для ефективного реагування правоохоронних органів на повідомлення про кіберзлочини необхідна дієва правова база для проведення слідчих дій та оптимальний баланс між дотриманням недоторканності приватного життя і повноваженнями з проведення розслідувань, оперативний доступ та засоби отримання електронних доказів у постачальників послуг мережі Інтернет, а також забезпечення належного навчання та технічних можливостей співробітників. З огляду на зазначене провідні країни світу формують спеціальні підрозділи протидії кіберзлочинності.

Так у США активно відбувається процес створення та реформування існуючих спеціалізованих підрозділів, серед яких:

– Відділ комп’ютерної злочинності та інтелектуальної власності Computer Crime And Intellectual Property Section (CCIPS) міністерства юстиції;

– Національна об’єднана група кіберрозслідувань – National Cyber Investigative Joint Task Force Федерального бюро розслідувань, яка проводить розслідування кібератак, терористичних операцій, втручань у комп’ютерні мережі з-за кордону;

– Цільова група протидії електронним злочинам Секретної Служби США (Secret Service on Electronic Crimes Task Forces).

У 2006 році був створений перший у світі підрозділ кібервійськ – Air Force Cyber Command, який у 2009 році реорганізовано в U.S. Army Cyber Command – структуру збройних сил США, мета якого – ведення кібервоєн [20].

Створення кіберкомандування США активізувало діяльність інших країн у цій сфері. У грудні 2009 року Південна Корея оголосила про створення підрозділу кібервійськ. Також активно розпочав підготовку до створення кібервійськ британський Центр урядового зв’язку. У 2010 році Китай створив підрозділ, що займається питаннями кібервійни та інформаційної безпеки. В РФ у 2014 році заснували війська інформаційних операцій для кібернетичного протиборства з супротивниками.

У Великобританії для розслідування злочинів у сфері інформаційних технологій у 2001 році був створений самостійний Національний центр протидії злочинам у сфері високих технологій – National High Tech Crime Unit (NHTCU). У 2006 році центр було введено до складу Агенції протидії організованій злочинності – The Serious Organised Crime Agency (SOCA), а з 2013 року він має назву National Cyber Crime Unit і діє у складі Національного агентства протидії злочинності (National Crime Agency) [21].

Також відповідно до Національного плану з кібербезпеки (National Cyber Security Plan) та прийнятої 1 листопада 2016 року Національної стратегії кібербезпеки Великобританії (National Cyber Security Strategy 2016-2021) [22] засновано Національний центр з кібербезпеки (National Cyber Security Centre), Лондонський офіс якого відкрито в лютому 2017 року [23]. Метою діяльності цього центру є надання консультацій і підтримки державному і приватним секторам в запобіганні кіберзагрозам.

Активну позицію щодо протидії кіберзагрозам займають і міжнародні організації, У січні 2013 року у структурі Європолу в Гаазі (Нідерланди) розпочав свою роботу Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre – EC3) [24]. Відповідаючи за стратегічний аналіз стану кіберзлочинності, формулювання політики і розробку законодавства, а також навчання правоохоронців, EC3 спрямовує свою діяльність на кіберзлочини, які:

– вчиняються організованими злочинними групами, зокрема які генерують великі злочинні доходи, наприклад, такі як інтернет-шахрайство;

– завдають серйозної шкоди жертвам, такі як он-лайн-сексуальна експлуатації дітей;

– впливають на критичну інфраструктуру та інформаційні системи в країнах ЄС, в тому числі кібератаки.

За кілька років з моменту свого створення ЕС3 вже зробив значний внесок у боротьбу з кіберзлочинністю: він брав участь у десятках резонансних операцій, в результаті яких відбулися сотні арештів. Співробітниками ЕС3 проаналізовано понад 800 тисяч файлів, переважна більшість яких виявилися шкідливими [25].

З метою протидії транснаціональній злочинності, у тому числі для розслідування кіберзлочинів, країни-члени Європейського Союзу об’єднали свої зусилля та створили Європейську організацію з питань юстиції (Євроюст), повноваження якої спрямовані на досягнення таких цілей: розвиток і покращення координації між компетентними органами держав-учасниць щодо дій із розслідування й кримінального переслідування на власних територіях з урахуванням будь-якого запиту, що надійшов від компетентного органу однієї з них, а також будь-якої інформації, наданої компетентним органом на підставі розпоряджень, виданих відповідно до установчих договорів; зміцнення співробітництва між компетентними органами держав-учасниць.

27 червня 2016 року в Брюсселі Україна підписала Угоду про співпрацю з Євроюстом. Підписи під документом поставили Генеральний прокурор України Юрій Луценко та Президент Євроюсту Мішель Конінкс. На церемонії підписання Угоди був присутній Президент України Петро Порошенко [26].

В Україні впродовж останніх років йде активне реформування та створення нових структур, які спрямовані на протидію кіберзлочинності. Сьогодні в Україні разом з докорінними змінами у зовнішньому та внутрішньому безпековому середовищі, появою нових викликів та загроз в умовах гібридної війни активно реформується сектор безпеки і оборони.

5 жовтня 2015 року був утворений Департамент кіберполіції – структурний підрозділ Національної поліції України, що спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп’ютерів), телекомунікаційних та комп’ютерних Інтернет-мереж і систем.

Указом Президента України від 7 червня 2016 року № 242/2016 сформований Національний координаційний центр кібербезпеки, робочий орган в Раді національної безпеки і оборони України, на який покладено координацію заходів суб’єктів забезпечення кібербезпеки.

Водночас залишаються поки що невирішеними низка актуальних завдань, що визначені Стратегією кібербезпеки.

Зокрема мова йде про невизначеність на законодавчому рівні таких понять, як кіберпростір, кіберзлочин, кібератака, об’єкти критичної інфраструктури та ін., що призводить до певних проблем в практичній діяльності правоохоронних органів, прокуратури та судів. Необхідно також вдосконалити систему збору, аналізу та оцінки електронних (цифрових) доказів.

Особливого значення набуває повна імплементація Конвенції про кіберзлочинність у частині наступних статей:

- Стаття 16 – Термінове збереження комп’ютерних даних, які зберігаються;
- Стаття 17 – Термінове збереження і часткове розкриття даних про рух інформації;
- Стаття 19 – Обшук і арешт комп’ютерних даних, які зберігаються;
- Стаття 20 – Збирання даних про рух інформації у реальному масштабі часу;
- Стаття 21 – Перехоплення даних змісту інформації.

Зазначені питання доцільно вирішити прийняттям Закону України “Про основні засади забезпечення кібербезпеки України”, проект якого знаходиться на розгляді в Верховній Раді України.

Однією з основних проблем протидії злочинності, у тому числі організованої у мережі Інтернет, є складність ідентифікації її користувачів. Адже злочинці, вчиняючи протиправні дії, використовують можливості анонімності у мережі Інтернет і завжди приховують своє справжнє ім’я. Наприклад, це можуть бути і адміністратори мережі “Синіх китів”, і педофіли, які зваблюють дітей через Інтернет, або зловмисники, що надсилають листи від імені державних установ, а насправді заражають комп’ютери вірусами з метою викрадення інформації або її шифрування для подальшого шантажу власника ресурсу.

У 2008 році був запропонований механізм під умовною назвою “ID-web” [27], який полягає у використанні біометричних властивостей людини для ідентифікації її в мережі Інтернет. Така ідентифікація дає змогу однозначно визначати, хто розмістив певну інформацію, хто прокоментував відповідну статтю або хто конкретно написав електронного листа. Для користувачів, які бажають залишатися анонімними, залишаються всі інші “ID не підтверджені” ресурси. Технологічні можливості для реалізації такої технології склалися після впровадження в Україні паспорта громадянина України у вигляді пластикової картки.

Реалізація відповідної системи ID-web на державному рівні надасть змогу зростання доступності процедур прямої демократії, а саме виконання п. 4.2 Національної стратегії сприяння розвитку громадянського суспільства в Україні на 2016 – 2020 роки [28] “Забезпечення ефективних процедур участі громадськості під час формування та реалізації державної, регіональної політики, вирішення питань місцевого значення” зокрема безпечним доступом до державних реєстрів, участі в обговоренні законодавчих ініціатив, формуванні петицій як до місцевих так і державних органів влади.

Подібну систему ідентифікації сьогодні активно використовують країни Прибалтики для забезпечення безпечного функціонування електронного урядування, Інтернет-банкінгу тощо. Кожен громадянин може отримати будь-яку інформацію про себе з державних інформаційних ресурсів он-лайн, використовуючи для ідентифікації користувача свою ID-картку та PIN-код.

На фоні зростання числа кібератак користувачі Інтернет починають втрачати довіру до паролів. Вони відкривають для себе нові технології та бажають використовувати їх для безпечного доступу до своїх даних. Так за он-лайн дослідженням організації “YouGov”, в Великобританії 56 % користувачів Інтернету бажають застосовувати біометричні методи аутентифікації замість традиційних паролів для цифрового банкінгу. Тільки 19 % опитаних назвали паролі пріоритетним методом захисту і лише 13 % зробили вибір на користь перевірочних питань [29].

Висновки.

З часу прийняття у березні 2016 року Стратегії кібербезпеки України в нашій державі досягнуто значних успіхів щодо організації протидії кіберзлочинності. Водночас залишається низка питань, які необхідно вирішити найближчим часом.

В зв’язку з підписанням Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, перш за все необхідно вдосконалити чинне законодавство відповідно до положень Конвенції про кіберзлочинність, прийняти відповідні нормативно-правові документи, які б законодавчо визначили термінологію

щодо кіберзлочинності, розробити ефективні механізми співробітництва з приватним сектором, особливо Інтернет-провайдерами з метою оперативного отримання електронних даних, необхідних для розслідування кіберзлочинів, активно розвивати міжнародне співробітництво у галузі протидії кіберзлочинності та розробити механізм функціонування захищеного Інтернету на основі ID-документів.

Використана література

1. The Global Risks Report 2017. – Режим доступу : //www3.weforum.org/docs/GRR17_Report_web.pdf

2. – Режим доступу : https://us.norton.com/cyber-security-insights-2016

3. Эксперт прогнозирует рост числа спонсируемых государствами киберпреступлений. – Режим доступу : //www.securitylab.ru/news/485310.php

4. НАТО: Кібератаки на альянс здійснюють держави. – Режим доступу : http://ua.korrespondent.net/world/3815528

5. Госструктуры подверглись 6500 кибератакам, к некоторым причастна Россия. – (Порошенко). – Режим доступу : http://biz.censor.net.ua/news/3018072

6. – Режим доступу : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/61 /PDF/N1703861.pdf?OpenElement

7. – Режим доступу : //www.itu.int/en/action/cybersecurity/Pages/gca.aspx

8. – Режим доступу : //www.eff.org/cyberspace-independence

9. Конвенція Організації Об’єднаних Націй проти транснаціональної організованої злочинності : Резолюція 55/25 Генеральної Асамблеї від 15 листопада 2000 року. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/995_789

10. Про ратифікацію Європейської конвенції про взаємну допомогу у кримінальних справах, 1959 рік, та Додаткового протоколу 1978 року до Конвенції № 1433-IV : Закон України від 04.02.04 р. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/44/98-%D0%B2%D1%80

11. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.05 р. № 2824-IV (2824-15). – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2824-15

12. – Режим доступу : //www.nato.int/cps/en/natohq/topics_78170.htm

13. – Режим доступу : //www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm

14. 618 U.S. Code § 1029 – Fraud and Related Activity in Connection with Access devices. – Режим доступу : //www.law.cornell.edu/uscode/text/18/1029

15. 718 U.S. Code § 1030 – Fraud and related activity in connection with computers. – Режим доступу : //www.law.cornell.edu/uscode/text/18/1030

16. 918 U.S. Code Chapter 119 – Wire and electronic communications interception and interception of oral communications. – Режим доступу : //www.law.cornell.edu/uscode/text/ 18/part-I/chapter-119

17. The USA Patriot Act: Preserving Life and Liberty. – Режим доступу : //www.justice.gov/ /ll/highlights.htm

18. Cyber Intelligence Sharing and Protection Act. – Режим доступу : https://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act.

19. Framework for Improving Critical Infrastructure Cybersecurity 2016. – Режим доступу : http://csrc.nist.gov/groups/SMA/forum/documents/january2016_presentations/Cybersecurity-Framework-for-FCSM-Jan-2016.pdf

20. – Режим доступу : //www.arcyber.army.mil/Pages/ArcyberHome.aspx

21. – Режим доступу : //www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit

22. – Режим доступу : //www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_ cyber_security_strategy_2016.pdf

23. – Режим доступу : //www.ncsc.gov.uk

24. – Режим доступу : //www.europol.europa.eu/ec3

25. – Режим доступу : //www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

26. Україна підписала угоду про співробітництво з Євроюстом: – Режим доступу : http://tsn.ua/politika/ukrayina-pidpisala-ugodu-pro-spivrobitnictvo-z-yevroyustom-680835.html

27. Гуцалюк М.В. Впровадження ID-web як необхідна умова безпеки в Інтернет // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2008. – № 18. – С. 265-269.

28. Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2016 – 2020 роки : Указ Президента України від 26.02.16 р. № 68/2016.

29. Пароли или биометрия : европейцы сделали свой выбор. – Режим доступу : http://psm 7.com/news/paroli-ili-biometriya-evropejcy-sdelali-svoj-vybor.html

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~