ПРОБЛЕМИ КРИМІНАЛЬНОГО ПРАВА ТА КРИМІНОЛОГІЇ

УДК 004.9

КІБЕРВІЙНИ: ОСНОВНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Бараненко Роман Васильович
кандидат технічних наук, доцент,
професор кафедри професійних та спеціальних дисциплін
(Херсонський факультет
Одеського державного університету внутрішніх справ,
м. Херсон, Україна)

Поляков Володимир Сергійович
старший викладач кафедри професійних та спеціальних дисциплін
(Херсонський факультет
Одеського державного університету внутрішніх справ,
м. Херсон, Україна)

Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Створення розвиненого й захищеного інформаційного середовища є неодмінною умовою розвитку суспільства та держави. Останнім часом в багатьох країнах все більше уваги приділяється проблемам захисту інформації та пошуків шляхів її вирішення.

Розглянуто основні складові інформаційної безпеки та саму систему інформаційної безпеки як низку підсистем.

Визначено об'єкти та суб'єкти інформаційної безпеки. Надано перелік загроз інформаційній безпеці. Проаналізовано принципи забезпечення інформаційної безпеки держави.

Розглянуто поняття «інформаційної війни» як одного з різновидів військових дій. Розглянуто поняття критичної інфраструктури, проаналізовано загрози та методи захисту, наведено усереднений сценарій протиправних дій та приклади кібератак на критичну інфраструктуру держави-супротивника.

Ключові слова: інтернет, комп'ютерні злочини, інформаційна безпека, кібератака, кібервійна, критична інфраструктура.

КИБЕРВОЙНЫ: ОСНОВНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Бараненко Роман Васильевич
кандидат технических наук, доцент,
профессор кафедры профессиональных и специальных дисциплин
(Херсонский факультет Одесского государственного университета внутренних дел,
г. Херсон, Украина)
Поляков Владимир Сергеевич
старший преподаватель кафедры профессиональных и специальных дисциплин
(Херсонский факультет Одесского государственного университета внутренних дел,
г. Херсон, Украина)

Информационная безопасность играет важную роль в обеспечении интересов любого государства. Создание развитой и защищенной информационной среды является непременным условием развития общества и государства. В последнее время во многих странах всё больше внимания уделяется проблемам защиты информации и поисков путей ее решения.

Рассмотрены основные составляющие информационной безопасности и сама система информационной безопасности как совокупность подсистем.

Определены объекты и субъекты информационной безопасности. Дан перечень угроз информационной безопасности. Проанализированы принципы обеспечения информационной безопасности государства.

Рассмотрено понятие «информационной войны» как одной из разновидностей военных действий. Рассмотрено понятие критической инфраструктуры, проанализированы угрозы и методы защиты, приведены усредненный сценарий противоправных действий и примеры кибератак на критическую инфраструктуру государства-противника.

Ключевые слова: интернет, компьютерные преступления, информационная безопасность, кибератака, кибервойна, критическая инфраструктура.

CYBERWARS: THE MAIN PROBLEMS TO PROVIDE OF STATE'S INFORMATION SECURITY

Baranenko Roman Vasilyovich,
candidate of technical sciences, assistant professor,
professor of department of professional and special disciplines,
(Kherson Faculty of Odessa State University of Internal Affairs,
Kherson, Ukraine)
Polyakov Volodymyr Sergiyovych,
senior lecturer of department of professional and special disciplines,
(Kherson Faculty of Odessa State University of Internal Affairs,
Kherson, Ukraine)

Information security plays an important role in securing the interests of any state. Creation of a developed and protected information environment is an indispensable condition

for the development of society and the state. Recently, in many countries, more and more attention is paid to the problems of information security and searching the ways to solve it.

Information security is a state of protection of the information environment of a society, which ensures its formation, use and development in the interests of citizens, organizations, and the state.

Information security has three main components: confidentiality, integrity and availability.

The information security system today has a number of subsystems. The study of scientific-theoretical and practical problems of information security will determine and solve the problem of creating an information security system that would function effectively.

Depending on the type of threats, information security can be considered as ensuring the state of protection of personality, society, state from the influence of poor-quality information; information and information resources from unlawful influence of unauthorized persons; information rights and freedoms of man and citizen.

The objects and subjects of information security are considered. The threats to information security are listed. The principles of ensuring information security of the state are analyzed.

The most dangerous threats to public interests in the information society are the uncontrolled proliferation of information weapons. The concept of "information war" as one of the varieties of military actions is considered. Among the new most important means of "information warfare" today are called various mathematical, software tools such as "viruses" and "bookmarks", means of remote erasure generators of electromagnetic pulses of information recorded on magnetic media, means of uncontrolled connection to closed information networks, etc.

The concept of critical infrastructure is considered, threats and methods of protection are analyzed, the averaged scenario of unlawful actions and examples of cyber attacks on the critical infrastructure of the enemy state are presented.

Keywords: cyberattack, computer crimes cyberwar, information security, Internet, critical infrastructure.

Вступ і постановка проблеми. Розвиток інформаційних технологій активізував зміщення акцентів на «інформаційні» аспекти суспільного життя. Основною цінністю для суспільства стають інформаційні ресурси. У зв'язку з цим питання забезпечення інформаційної безпеки отримують все більшу актуальність.

Гібридна війна, ключовим елементом якої є інформаційний чинник, формує довгострокові виклики для Української держави. У нещодавно проголошеній «Стратегії реформ – 2020» заявлено про необхідність реформи системи національної безпеки і оборони, одним з ключових пріоритетів якої має стати кібернетична безпека [1].

Аналіз попередніх досліджень. Серед зарубіжних вчених вагомий внесок у розгляд питання забезпечення інформаційної безпеки держави внесли Г. Кіссінджер, З. Бжезинський, Л. Браун, Ч. Флавін, Х. Френч. Серед вітчизняних дослідників хотілося б відзначити праці О. Сосніна, В. Грубова,

В. Домарьова, В. Ліпкана, В. Косевцова, І. Бінько, В. Мунтіяна, Г. Почепцова, О. Литвиненко та інших.

Дослідженням інформаційної безпеки України займалися також В. Беляков, М. Демкова, Л. Задорожня, В. Кирик, А. Крутських, Н. Кушакова-Костицька, А. Леваков, Е. Макаренко, В. Роговець. Особливо важливі питання для осмислення інформаційної безпеки як виду соціально важливої діяльності середовища охарактеризовані в працях вітчизняних вчених: В.П. Горбуліна, Г.В. Іващенка, Б.А. Кормича, М.Б. Левицької, В.М. Лопатіна, Ю.Є. Максименко, А.І. Марущака, Г.В. Новицького, А.А. Стрельцова.

Метою даної роботи є визначення заходів забезпечення інформаційної безпеки держави.

Об'єктом дослідження є система інформаційної безпеки як сукупність явищ та процесів, захист яких є метою діяльності відповідних служб. Предметом дослідження є характеристика елементів, критеріїв та заходів забезпечення системи інформаційної безпеки.

Основний матеріал. Необхідно розглядати правове забезпечення інформаційної безпеки в якості самостійного комплексного напрямку правового регулювання, здійснюваного в рамках реалізації державної політики в галузі забезпечення інформаційної безпеки, що утворюється сукупністю інститутів і норм інформаційного, конституційного, цивільного, адміністративного та кримінального права, що регулюють відносини в сфері протидії загрозам безпеки об'єктів національних інтересів в інформаційній сфері [2].

Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Створення розвиненого й захищеного інформаційного середовища є неодмінною умовою розвитку суспільства та держави. Останнім часом у світі відбуваються якісні зміни в процесах управління, зумовлені інтенсивним впровадженням сучасних інформаційних технологій. Разом з цим посилюється небезпека несанкціонованого втручання в роботу інформаційних систем, і вагомість наслідків такого втручання дуже сильно зросла. Як наслідок, в багатьох країнах все більше уваги приділяється проблемам захисту інформації та пошуків шляхів її вирішення [3].

У найзагальнішому випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави [4].

За іншим визначенням інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та недостовірність інформації, що використовується; негативний

інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання й порушення цілісності, конфіденційності та доступності інформації» [5].

Згідно з [6] під інформаційною безпекою розуміється: по-перше, здатність держави, суспільства, соціальної групи забезпечити з визначеною імовірністю достатні й захищені інформаційні ресурси, надійність функціонування інформаційно-комунікативних систем в інтересах стійкого розвитку суспільства; по-друге, протистояти інформаційним небезпекам і загрозам, негативним інформаційним впливам на суспільну й індивідуальну свідомість, психіку людей, а також на інформаційні структури; по-третє, виробляти особистісні й групові навички і вміння безпечного поводження; по-четверте, підтримувати постійну готовність до адекватних мір в інформаційному протиборстві.

Інформаційна безпека має три основні складові: конфіденційність, цілісність і доступність. Конфіденційність належить до захисту чутливої інформації від несанкціонованого доступу. Цілісність означає захист точності і повноти інформації та програмного забезпечення. Доступність – це забезпечення доступності інформації і основних послуг для користувача в потрібний для нього час [7].

Система інформаційної безпеки сьогодні є низкою підсистем. Вивчення науково-теоретичних та практичних проблем інформаційної безпеки дозволить визначити та розв'язати завдання щодо створення системи інформаційної безпеки, яка б функціонувала ефективно.

В залежності від виду загроз інформаційну безпеку можна розглядати як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб; інформаційних прав і свобод людини і громадянина [8].

Згідно з [8] об'єктами інформаційної безпеки можуть бути: свідомість, психіка людей; інформаційні системи різного масштабу й різного призначення. До соціальних об'єктів інформаційної безпеки зазвичай відносять особистість, колектив, суспільство, державу, світове товариство. До суб'єктів інформаційної безпеки відносяться:

– держава, що здійснює свої функції через відповідні органи;

– громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки відповідно до законодавства.

Інформаційна безпека особистості – це захищеність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ і т.ін [9].

Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи і т.ін.) відносно небезпечних (дестабілізуючих, деструктивних, що вражають державні інтереси і т.ін.) інформаційних впливів, причому як з впровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи [4].

Доктрина інформаційної безпеки України визначає на сучасному етапі такі реальні й потенційні загрози інформаційній безпеці [10]:

1) у зовнішньополітичній сфері:

– поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;

– прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують сталому та безпечному функціонуванню інформаційно-телекомунікаційних систем;

– зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;

2) у сфері державної безпеки:

– негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканості кордонів України;

– використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками;

– несанкціонований доступ до інформаційних ресурсів органів державної влади;

– розголошення інформації, яка становить державну та іншу, передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

3) у воєнній сфері:

– порушення встановленого регламенту збирання, обробки, зберігання й передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;

– несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;

– реалізація програмно-математичних засобів із метою порушення функціонування інформаційних систем у сфері оборони України;

– перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління;

– інформаційно-психологічний вплив на населення України, зокрема на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

4) у внутрішньополітичній сфері:

– недостатня розвиненість інститутів громадянського суспільства, недосконалість партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;

– негативні інформаційні впливи, зокрема із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість;

– поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації.

Враховуючи, що сьогодні кіберпростір стає ареною конфліктів між державами, організаціями та приватними особами за сучасних умов активізації міжнародних терористичних, екстремістських організацій та злочинних структур, які використовують інформаційні технології для реалізації своїх злочинних намірів, забезпечення інформаційної безпеки є однією з найважливіших складових системи забезпечення національної і міжнародної безпеки [11].

Під інформаційним середовищем розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на три основні предметні частини [4]:

– створення і розповсюдження вихідної та похідної інформації;

– формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;

– споживання інформації;

та дві забезпечувальні предметні частини:

– створення й застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;

– створення й застосування засобів і механізмів інформаційної безпеки.

Забезпечення інформаційної безпеки – це сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в інформації.

Принципами забезпечення інформаційної безпеки держави є:

– законність, дотримання балансу інтересів особистості, суспільства й держави;

– взаємна відповідальність суб'єктів забезпечення інформаційної безпеки;

– інтеграція систем національної та міжнародної безпеки.

Загрози державним інтересам виявляються у вигляді отримання протиправного доступу до інформації, що складає державну таємницю, або до інформації, що має конфіденційний характер, розкриття якої призведе до збитків або репутаційних втрат.

Найнебезпечнішими загрозами державним інтересам в інформаційному суспільстві є неконтрольоване розповсюдження інформаційної зброї.

Інформаційна зброя є сукупністю засобів, методів і технологій, що забезпечують можливість силового впливу на інформаційну сферу супротивника з метою руйнування його інформаційної та управлінської інфраструктури.

Враховуючи, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства загалом, нав'язуватися чужі інтереси, мотиви, спосіб життя, на перший план виходить аналіз сутності та форм проявів скритого агресивного впливу, вияву дій, що мають цілеспрямоване агресивне спрямування та які суперечать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах [12].

З огляду на активізацію впровадження інформаційно-комунікаційних технологій (ІКТ) до всіх критично важливих сфер життєдіяльності людини та держави, протистояння у кіберпросторі шляхом проведення кібернетичних атак (ударів) виходить на більш високий рівень міждержавних відносин. Крім того, це призводить до трансформації державної політики більшості провідних держав у питанні контролю за власним кіберпростором та посиленні яскраво виражених обмежувальних тенденцій [13].

Захист інформаційного суверенітету держави тісно пов'язаний із поняттям інформаційної безпеки, що означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільству інформації, включаючи контроль над рекламою; захист національного інформаційного простору від зовнішньої інформаційної експансії [3].

Згідно з [14] інформаційна безпека суспільства забезпечується його захистом від шкідливих інформаційних впливів в ході інформаційної війни, яка має відносно суспільства, наступні цілі: 1) тактичну, тобто нав'язати свою політичну волю через ідеологічну, психологічну обробку народу, армії, військово-політичного керівництва країни в інтересах створення необхідної громадської думки; 2) стратегічну, тобто змінити спосіб життя, роз'єднати

народ, знищити морально-політичний потенціал суспільства й зруйнувати державу зсередини шляхом ідеологічної революції, руйнування національної самосвідомості, розмивання почуттів патріотизму, культури, традицій, історичної пам'яті, підриву духовно-етичних засад. Шкідливий інформаційний вплив на суспільство реалізується в основному через ЗМІ, в т.ч. електронні комунікації, шляхом створення та впровадження штампів, доступних для розуміння людини, ігри на почуттях страху, надії, роздратування та інших, що викликають стан агресії або безвиході. Формується прагнення піти з реального світу, замінити його традиційно штучним (алкоголізм, наркоманія, прихід до деструктивних сект) або віртуальним (телевізійний, комп'ютерний), посилення соціально-політичних, економічних і духовних колізій.

В розвинутих країнах концепція інформаційної війни є складовою воєнної доктрини, що обумовлює спеціальну підготовку особового складу і окремих підрозділів для проведення інформаційних операцій; практика міжнародних, регіональних та етнічних конфліктів виявила унікальність застосування інформаційної зброї для впливу на міжнародне співтовариство та для боротьби за геополітичні інтереси [15].

«Інформаційна війна» є одним з різновидів військових дій: дій, прийнятих для досягнення інформаційної переваги в інтересах національної військової стратегії та здійснюваних шляхом впливу на інформацію та інформаційні системи противника при одночасному захисті власної інформації та своїх інформаційних систем [16].

Досі в світі не вироблено загальноприйнятого визначення «інформаційної зброї». До характерних рис інформаційного зброї можна віднести її якісну універсальність, радикальність впливу, доступність. Вона відрізняється широким вибором часу й місця застосування. Для її приведення в дію не потрібно великих армій, що робить інформаційну війну порівняно економічною. Її застосування носить знеособлений характер, легко маскується під звичайну діяльність. Одночасно важко визначити її «зворотну адресу» й національну приналежність. Агресія може фактично здійснюватися державами «чужими руками» або таким чином, що в якості відповідального за інформаційний напад буде підставлено невинну державу [17].

Інформаційна зброя не знає географічних відстаней, підриває традиційне поняття державних кордонів, роблячи їх технологічно проникними. Використання цієї зброї може відбуватися досить приховано («буденно»), не доводячи справу до оголошення «гарячої» війни; не потребує великої й видимої підготовки. Часом жертва може навіть не усвідомлювати, що знаходиться під інформаційним впливом. До того ж, у зв'язку з відсутністю систем і методик, що оцінюють загрозу і заздалегідь

попереджають про підготовлюваний напад, ускладнюється можливість протидіяти такій агресії [17].

Серед нових найбільш важливих засобів «інформаційної війни» сьогодні називають різні математичні, програмні засоби типу «вірусів» і «закладок», засоби дистанційного стирання генераторами електромагнітних імпульсів інформації, що записана на магнітних носіях, засоби неконтрольованого підключення до закритих інформаційних мереж та ін.

За даними видання The Daily Beast [18], згідно зі звітом ФБР, кібервійська КНР є «найбільшою цілісною загрозою США у сфері кібертероризму» та силою, що вже зараз може володіти потенціалом «знищувати життєво важливу інфраструктуру, отримувати доступ до банківських, комерційних, військових та оборонних баз даних».

Під життєво важливою – критичною – інфраструктурою розуміються «системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з перерахованого вище» [19].

З-поміж загроз критичній інфраструктурі називають пандемії, промислові аварії, терористичну та злочинну діяльності, кібератаки, стихійні лиха тощо [20].

На сьогодні захист критичної інфраструктури ствердився як важливий напрям політики у сфері безпеки країн-членів ЄС і НАТО. Двома основними чинниками, що сформували концепцію захисту критичної інфраструктури, є такі [21]:

– посилення боротьби з міжнародним тероризмом;

– забезпечення безпеки у процесі розроблення та реалізації основних проектів у області інфраструктури для транспортування нафти, нафтопродуктів, газу й інших стратегічних сировинних матеріалів.

Розглядаючи набір потенційних сценаріїв військових дій з використанням мережного середовища (Інтернет) в самій загальній постановці, як взаємодіючих факторів, що характеризують «типовий профіль» такого сценарію можна виділити наступні [22]:

– суб'єкт дії – персона і (або) група осіб, що мають на меті проведення терористичних дій проти об'єкта (об'єктів), і (або) сукупність їх агентів в мережному середовищі первинного об'єкта атаки, що діють з використання прихованих каналів передачі інформації [23];

– предмет дії – мережна інфраструктура (фізичне середовище передачі даних, комунікаційні засоби та програмне забезпечення), які можуть надавати доступ до інформаційно-обчислювальних ресурсів системи;

– мета дій – використовувати предмет дії (мережну інфраструктуру) для деструктивного впливу на об'єкт (об'єкти), результатом якого будуть різні наслідки (ґрунт для шантажу, замах на життя людей, руйнування вторинних об'єктів і т.п.);

– первинний об'єкт – комп'ютерний комплекс для відносно вузької, але стратегічно важливої або, наприклад, здатної прямо впливати на здоров'я людей, сфери застосування; велика інтегрована система розподілених інформаційно-обчислювальних ресурсів для обслуговування національно значущою сфери діяльності (економіка, промисловість, тощо...), наприклад, енергетична (в т.ч., атомна), транспортна (повітряна або залізнична) система або її елементи (місцеві, регіональні);

– вторинний об'єкт – персона або група людей, матеріальні об'єкти різного призначення, інформаційні системи, які можуть бути схильні до деструктивних дій з боку первинних об'єктів, аж до знищення.

Усереднений сценарій протиправних дій при цьому повинен, як правило, містити [22]:

– дії, що забезпечують неавторизований доступ до інформації з високим рівнем секретності;

– знищення, модифікацію або заміну програмного коду, що забезпечує нормальне (регламентоване) функціонування системи;

– обмеження доступу зовнішніх або внутрішніх агентів системи безпеки, здатних оперативно запобігти зловмисним діям.

При визначенні потенційних елементів критичної інфраструктури враховують такі чинники та характеристики [24]:

1) масштаб (географічне охоплення території, для якої втрата елемента критичної інфраструктури викликає значну шкоду) – міжнародний, національний, регіональний або територіальний;

2) тяжкість можливих наслідків за такими показниками:

– вплив на населення (кількість постраждалих, загиблих, осіб, які отримали серйозні травми, а також чисельність евакуйованого населення);

– економічна шкода (вплив на ВВП, розмір економічних втрат – прямих і непрямих);

– екологічна шкода (вплив на населення і навколишнє середовище);

– взаємозв’язок з іншими елементами критичної інфраструктури;

– політичний ефект (втрата впевненості в дієздатності влади);

– тривалість впливу (як саме й коли виявлятимуться збитки, пов’язані із втратою чи відмовою об’єктів критичної інфраструктури).

Забезпечення безпеки критичної інфраструктури є складною проблемою для кожної держави і, посилаючись на думку американського дослідника Теда Льюіса [25], головними викликами в цьому напрямі варто назвати такі:

– значущість кожного із секторів критичної інфраструктури та її самої в цілому;

– управління безпекою за умов взаємозалежності діяльності урядових органів, державного й приватного секторів, а також регулюючих та економічних чинників;

– обмін інформацією, який уже на стадії збору та співставлення необхідних даних є значною проблемою, оскільки державні органи є здебільшого вертикально орієнтованими структурами, які переважно накопичують інформацію, а елементи критичної інфраструктури розпорошені між державою та чималою кількістю приватних компаній;

– взаємозалежність елементів і секторів критичної інфраструктури внаслідок притаманних їм комплексних різнорівневих взаємодій та взаємозв'язків.

Зважаючи на те, що більшість систем критичної інфраструктури має мережну архітектуру, Т. Льюіс вважає, що захищати необхідно передусім головні «вузли» цих систем [25]. Саме у такий спосіб з'являється можливість дотримуватися «правила 80-20%», за яким 80% ресурсів мають витрачатися на 20% території країни, а також використовувати теорію мереж для організаційних і фізичних структур, призначених для організації захисту критичної інфраструктури.

В Україні критична інфраструктура включає ті матеріальні чи віртуальні (інформацію, що зберігається в реєстрах, базах даних, інформаційних системах органів влади, або передається засобами Національної системи конфіденційного зв'язку) об'єкти й системи, від стабільного функціонування яких залежить можливість досягнення національних інтересів держави [26].

Існує три рівня небезпечних дій в кіберпросторі [27]:

– простий неструктурований: можливість проводити основні кібератаки проти окремих систем, що використовують інструменти, створені кимось іншим;

– просунуто-структурований: можливість проводити більш складні кібератаки проти декількох систем або мереж і, можливо, модифікувати або створювати базові інструменти злому;

– комплексно-координований: можливість до скоординованих кібератак, здатних викликати масове руйнування проти інтегрованих гетерогенних систем захисту (в тому числі криптографічних). Можливість створювати складні інструменти злому.

Прикладом кібератаки на критичну інфраструктуру держави є вірус Stuxnet, головною метою якого стало ураження програмованих логічних контролерів, які використовуються для автоматизації технологічних

процесів на заводі зі збагачення урану у місті Нетенз в Ірані. Розповсюджувався вірус тільки через операційні системи Windows, оскільки використовував деякі вразливості цієї системи. Найцікавішим є те, що його було запрограмовано на самоліквідацію 24 червня 2012 року.

За деякими версіями вірус Stuxnet на підприємство приніс один з контрактних робітників використовуючи USB-флешку. Вірус досить швидко розповсюджувався, оскільки мав декілька шляхів зараження:

1) USB-*флешка*. На інфікованому комп'ютері працює програма, яка копіює вірус на флешку, для подальшого її запуску на інших комп'ютерах. Якщо на флешці уже є будь-яка версія Stuxnet – вона переписувалась на більш нову. Головним є те, що заражені таким чином накопичувачі стартували шкідливе програмне забезпечення тільки на 3 різні комп'ютери. Після цього вірус з флешки видалявся. Залежно від версії Stuxnet використовувались два способи копіювання інформації на новий комп'ютер для зараження;

– за допомогою файлу autorun.inf, який зазвичай присутній на медіа-носіях і являє собою лист задач до виконання, який Windows відкриває автоматично для програвання музики чи відео, Stuxnet додавав безпосередньо у цей файл, поряд із нормальними командами, свій код, замість того щоб використовувати окремий файл. Тому, коли Windows почала перевіряти валідність команд в файлі autorun.inf – такий спосіб перестав працювати;

– використовуючи файли .lnk, тобто звичайні ярлики Windows. Stuxnet копіював dll бібліотеку і завантажувач для неї на зовнішній носій, а також створював чотири ярлики. Вони використовувались для завантаження вірусу на новий комп'ютер, коли користувач переглядає інформацію на диску. Саме чотири ярлика було необхідно, оскільки кожен з них використовувався для різних версій Windows.

2) WinCC. Stuxnet шукав комп'ютери, на яких було встановлено Siemens WinCC – інтерфейс для SCADA-системи. Він підключався за допомогою прописаного до WinCC пароля, і нападав на його базу даних за допомогою SQL-команд, щоб завантажити й запустити свою копію на комп'ютері з WinCC.

3) Через *мережні ресурси*. Stuxnet також поширювався за допомогою загальних папок Windows. Маючи доступ до локальної мережі, вірус копіював шкідливі файли до усіх відкритих папок на віддалених комп'ютерах. Для кожного з файлів задавався точний час його запуску. За різними версіями це могло тривати від двох хвилин до наступного дня.

4) Через *принтери загального користування*. Служба диспетчера друку Windows на той час мала вразливість, завдяки якій можна було відправляти віддалені команди на інші комп'ютери в мережі. Використовуючи це вікно в

безпеці Windows, Stuxnet копіював файли з вірусом на інші машини, а потім запускав їх.

Stuxnet може оновити себе від заражених проектів Step7. Якщо заражений проект відкрито, і його версія Stuxnet є новішою за ту, що вже встановлено на комп'ютері, то версію буде оновлено.

Крім того, Stuxnet використовує вбудовану P2P мережу для поновлення старих екземплярів до останньої версії, існуючої в локальній мережі на поточний день. Кожна копія запускає сервер RPC (Remote Procedure Call), і прослуховує з'єднання. Інші копії вірусу, з'єднуючись через своїх клієнтів RPC, можуть оновити себе, якщо їх версія старіша, або оновити сервер, якщо він старіший.

Після того, як Stuxnet встановлюється на комп'ютері, він намагається зв'язатися з одним з двох серверів через HTTP:

- www.mypremierfutbol.com
- www.todaysfutbol.com

Він посилає свою IP-адресу й корисні дані, що включають зокрема, інформацію про базову операційну систему, ім'я хоста комп'ютера та доменне ім'я, прапор, який вказує, чи Siemens Step7 або WinCC, які є метою Stuxnet, встановлено на комп'ютері.

Сервер може відповісти, відправивши скрипт-файл для Windows, який він може вказати для завантаження до поточного процесу або до іншого через RPC. Це дозволяє авторам Stuxnet оновлювати його віддалено, або запустити абсолютно нові шкідливі програми на заражених комп'ютерах. Передача даних на сервер і з сервера відбувалася в зашифрованому вигляді.

Stuxnet не є шкідливим для звичайних користувачів, так як його мета полягає в тому, щоб змінити Simatic PLC виробництва компанії Siemens. Step7 програми, які керують і контролюють ці програмовані логічні контролери (PLC), використовують бібліотеку з ім'ям s7otbxdx.dll для зв'язку з фактичним PLC, щоб читати або змінювати його зміст (коди). Stuxnet отримує контроль над усіма запитами, надісланими до PLC, оточивши цю бібліотеку. Крім того Stuxnet записує свій власний шкідливий код, щоб орієнтуватися на певні конкретні PLC. Він приховує свій шкідливий код від користувачів шляхом повернення оригінальних блоків коду замість модифікованих блоків при запиті на читання.

Код Stuxnet інфікує програмовані логічні контролери трьома послідовностями атак, названих A, B і C в звіті Symantec. Послідовності A і B однакові, лише з невеликими відмінностями, і мають ті ж самі ефекти. Послідовність C є більш просунутою, але є неповною й ніколи не виконується. Послідовності A і B виконують свої атаки запуску роторів центрифуг при дуже низьких і високих частотах (таких, як 2 і 1410 Гц, відповідно). Цікаво відзначити, що період, в який вони командують

центрифугам обертатися на цих швидкостях, досить короткий (50 і 15 хвилин, відповідно), і відокремлені один від одного: близько 27 днів між атаками. Це, можливо, вказує на те, що архітектори хотіли якомога довше залишатися не поміченими.

Хоча часу, протягом якого центрифуги сповільнювалися або прискорювалися, ймовірно, не було достатньо для того, щоб реально досягти мінімального й максимального значень, вони як і раніше призводили до значних уповільнень і швидкісних злетів. Повільної швидкості достатньо, щоб призвести до неефективно переробленого урану, а високі швидкості, можуть призвести центрифуги до фактичного знищення, так як вони працювали на межі максимальної швидкості.

Stuxnet приховувався від персоналу заводу шляхом установки руткітів на заражених комп'ютерах Windows, і на заражених програмованих логічних контролерах, для того, щоб приховати свої файли. Встановивши драйвер на комп'ютерах Windows, він приховує себе, маніпулюючи запитами, надісланими до пристроїв.

Перехоплюючи виклики s7otbxdx.dll, Stuxnet приховує шкідливий код, що він записує на програмовані логічні контролери для саботажу центрифуг, а також захищає ці шкідливі коди від перезапису. Перед тим як шкідлива програма запускає процедуру атаки, він записує нормальні робочі частоти центрифуг і передає ці записані дані до програми-монітору під час атаки. Результатом є те, що система показує нормальну роботу замість оповіщення персоналу про аномальні частоти, на яких центрифуги насправді працюють. Stuxnet також змінює деякі процедури на програмованих логічних контролерах, запобігаючи безпечному завершенню роботи системи, навіть якщо оператор виявить, що система не працює в нормальному режимі.

Однак на практиці практично неможливо довести, що такі дії відповідають критеріям кібертероризму, хоча й діяльність вірусу Stuxnet дійсно могла створити небезпеку для життя працівників ядерних об’єктів. Але без добровільного зізнання про політичні мотиви організаторів дану дію вкрай складно класифікувати як кібертероризм, швидше, як кібердиверсію [28].

З міжнародно-правової точки зору важливо знайти відповідь на запитання: чи можна акти кіберагресії прирівняти до тих актів «збройного насильства», що підпадають під дію ст. 2(4) Статуту ООН, й чи можна кібератаки вважати тотожними «збройним нападам», що підпадають під дію ст. 51 Статуту ООН. А головне питання полягає в тому, як з міжнародно-правової точки зору розрізнити ситуації, коли країна діє у кіберпросторі з метою власної оборони від тих ситуацій, коли вона є агресором, і що означає в даному разі «міра припустимої самооборони» [28].

Висновки. Введення до міжнародної політики поняття «кібервійна» свідчить про кінець традиційної світової системи гарантії безпеки та вразливість державних суверенітетів. На сьогодні застосування кіберзброї дозволяє досягти необхідної політичної мети з мінімальними затратами. А без міжнародного співробітництва з питань регулювання кіберпростору наш світ має всі шанси постати на порозі нової світової війни. Але війни таємної.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Стратегія розвитку України – 2020: [Електронний ресурс] / Офіційний веб-портал Президента України. – Режим доступу: http://www.president.gov.ua. – Назва з екрана.

2. А.А. Стрельцов. Цель, структура и методы правового обеспечения информационной безопасности Российской Федерации // Научные и методологические проблемы информационной безопасности (сборник статей). Под ред. В.П. Шерстюка. – М.: МЦНМО, 2004. – С.47-65.

3. Степко О.М. Аналіз головних складових інформаційної безпеки держави // Науковий вісник Інституту міжнародних відносин НАУ. – Сер. : Економіка, право, політологія, туризм. – 2011. – Вип. 1(3). – С.90-99.

4. Лук'янова В.В., Інформаційна безпека в умовах розвитку інформаційної системи /В.В. Лук'янова, А.Ю. Лаутар //Вісник Хмельницького національного університету. – 2013. – №2. Т.3 – С. 97-101.

5. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 р.р.: [Закон України: офіц. текст: за станом на 9 січня 2007 р.] // Відомості Верховної Ради України (ВВР). – 2007. – № 12. – Ст. 102.

6. Пучков О.О. Інформаційна безпека у контексті сьогоднішніх реалій: філософський аспект // Гуманітарний вісник ЗДІА. – 2015. – № 60. – С. 239-245.

7. Информационная безопасность [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Information_security.

8. Сутність інформаційної безпеки та захисту інформації [Електронний ресурс]. – Режим доступу: http://5ka.at.ua/load/pravo/sutnist_informacijnoji_bezpeki_ta_zakhistu_informaciji_kursova_robota/49-1-0-24790.

9. Я. Жарков Небезпеки особистості в інформаційному просторі / Жарков Я. // Юридичний журнал. – № 2/2007. [Електронний ресурс]. – Режим доступу: http://www.justinian.com.ua/print.php?id=2554.

10. Національна безпека України [Текст] : нормат.-прав. акт. / авт.-упоряд.: Я.Й. Малик, О.І. Береза, М.Ф. Криштанович. – Львів: ЛРІДУ НАДУ, 2010. – С. 511, 512.

11. Марков В.В. Напрями діяльності НАТО у справі протидії кіберзлочинності / В.В. Марков, О.В. Караченцев // Право і безпека. – 2014. – № 4 (55). – С. 119-123.

12. Роговец В. Информационные войны в современном мире: причины, механизмы, последствия / В. Роговец // Персонал [Текст]. – 2000. – № 5. – С. 33-38.

13. Косогов О.М., Сірик А.О. Сучасна політика безпеки кіберпростору в умовах його мілітаризації // Сучасні інформаційні технології у сфері безпеки та оборони. – 2015. – №3 (24). – С. 181-186.

14. Камытов К.Т. Понятие информационной безопасности и угрозы в информационной сфере // «Вестник КГЮА». – 2013. – Вып. 1.

15. Міжнародна інформаційна безпека : Сучасні виклики та загрози [Текст]. – К.: Центр вільної преси, 2006. – 916 с.

16. Леваков А. Пентагон готовится к «информационной войне» // Красная звезда. – 1995. – 17 октября.

17. А.В. Крутских. Война или мир: международные аспекты информационной безопасности // Научные и методологические проблемы информационной безопасности (сборник статей). Под ред. В.П. Шерстюка. – М.: МЦНМО, 2004. – С. 85-96.

18. China's Secret Cyberterrorism [Електронний ресурс]. – Режим доступу: http://www.thedailybeast.com/blogs-andstories/2010-01-13/chinas-secret-cyber-terrorism/full.

19. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism : USA PATRIOT ACT. – 2001 [Електронний ресурс]. – Режим доступу: http://frwebgate.access.gpo.gov.

20. Critical Infrastructure Resilience Strategy / Australian Government [Електронний ресурс]. – Режим доступу: http://www.tisn.gov.au.

21. Бірюков Д.С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д.С. Бірюков, С.І. Кондратов. – К.: НІСД, 2012. – 96 с.

22. В.А. Васенин Информационная безопасность и компьютерный терроризм // Научные и методологические проблемы информационной безопасности (сборник статей). Под ред. В.П. Шерстюка. – М.: МЦНМО, 2004. – С. 67-83.

23. Грушо А.А., Тимонина Е.Е. Языки в скрытых каналах. // Труды международной конференции «Информационные технологии в науке, образовании, телекоммуникациях, бизнесе». Украина, Крым, Ялта-Гурзуф, 19-29 мая 2003 г.

24. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection : Council Directive

2008/114/ЕС [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu.

25. Lewis, T.G. Critical infrastructure protection in homeland security: defending a networked nation. – New Jersey: John Wiley & Sons, 2006. – 474 p.

26. Про основи національної безпеки : закон України від 19.06.2003 р. № 964-IV // ВВР. – 2003. – № 39. – Ст. 351 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15.

27. Dorothy E. Denning (May 23, 2000). "Cyberterrorism". cs.georgetown.edu. Archived from the original on March 10, 2014. Retrieved June 19, 2016.

28. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України. / Д.В. Дубов, М.А. Ожеван. – К.: НІСД, 2011. – 30 с.