УДК 004.946.5.056
DOI: 10.31866/2617-796x.1.2018.147257

Ткаченко Олександр,
кандидат фізико-математичних наук, доцент,
Київський національний університет культури і мистецтв,
Київ, Україна
aatokg@gmail.com
http://orcid.org/0000-0001-6911-2770

Ткаченко Костянтин,
асистент,
Київський національний університет культури і мистецтв,
Київ, Україна
tkachenko.kostyantyn@gmail.com
http://orcid.org/0000-0003-0549-3396

КІБЕРПРОСТІР І КІБЕРБЕЗПЕКА: ПРОБЛЕМИ, ПЕРСПЕКТИВИ, ТЕХНОЛОГІЇ

Метою статті є дослідження та розгляд загальних проблем такої важливої сфери інформаційної діяльності держави, бізнесу, освіти, науки як кібербезпека.

Методами дослідження є методи семантичного аналізу основних понять розглянутої предметної області (кібербезпека). В статті розглянуті підходи до тлумачення понять кіберпростору та кібербезпеки, що пов'язані як з організаційними, так і технічними аспектами. В статті розглянута сутність кіберпростору та кібербезпеки з позицій державного забезпечення цієї сфери інформаційної діяльності. В статті розглянуто основні проблеми кібербезпеки та шляхи їх розв'язання. Вказано, що одним з аспектів кіберзагрози є комп'ютерні віруси. Розглянуто їх види та описано основні шляхи їх усунення та знешкодження.

Новизною проведеного дослідження є запропоновані шляхи забезпечення кібербезпеки інформаційного простору підприємств та комп'ютерних мереж (в тому числі й Інтернет).

Висновком проведеного в статті дослідження є те, що інформатизація та цифровизація в наш час проникають у всі сфери діяльності держави, суспільства, бізнесу, науки, освіти та окремої людини. Тому пошук шляхів забезпечення кібербезпеки (зокрема, розробка відповідних технологій) стали важливим аспектом діяльності ІТ-сфери.

Ключові слова: кібербезпека, кіберпростір, кіберзлочин, комп'ютерний вірус, інформаційна система.

Вступ. В наш час щодня приходять новини про те, що кіберзлочинці (які можуть бути представниками різних країн) захоплюють контроль над чужими комп'ютерами, гаджетами, програмними продуктами, запускаючи відповідні програми проти певних сайтів, інформаційних ресурсів чи певного контенту мобільних додатків. За короткий час припиняється робота банкоматів, компаній, телефонних ліній, промислових підприємств, підприємств, що мають стратегічне значення, чи навіть державних сайтів. З банківських рахунків фізичних та юридичних лиць зникають кошти. Відбувається так званий «злам» інформаційних баз підприємств, установ, організацій.

Тому в різних країнах все більше уваги приділяється забезпеченню кібербезпеки, захищеному керуванню інформаційними ресурсами, розробці спеціальних інформаційних систем (ІС) та інформаційних технологій (ІТ), окремих програмних продуктів, що надають можливість забезпечувати кібербезпечне функціонування як окремих підприємств, організацій, установ, так і країни в цілому (ISO/IEC 27032, 2012).

Інтеграція України у світовий інформаційний простір, розвиток суспільства нашої країни, як суспільства знань призвели до появи нових загроз її національним інтересам, пов'язаних з кібербезпекою. Це спричинило:

- необхідність досліджень не тільки термінології в сфері інформаційної безпеки (ця робота по систематизації і аналізу існуючих визначень понять в сфері кібербезпеки ведеться досить активно (Баранов, 2014; Толубка ред., 2015), а й щодо інформаційно-технологічних аспектів забезпечення інформаційної безпеки (аналітичних досліджень щодо існуючих технологій і систем забезпечення кібербезпеки з визначенням їх переваг і недоліків не так і багато, а робіт щодо напрямків подальшого розвитку сфери кібербезпеки ще менше);
- необхідність переосмислення реального забезпечення кібербезпеки інформаційного простору України в цілому;
- необхідність переосмислення реального забезпечення кібербезпеки інформаційного простору окремих підприємств (організацій, установ, інституцій) чи галузей економіки країни;
- необхідність формування єдиної національної політики щодо забезпечення інформаційної та кібербезпеки як країни в цілому, так і окремих її організаційних структур та інституцій;
- вирішення проблем, пов'язаних із розбудовою національної системи кібербезпеки;
- необхідність формування відповідної нормативно-правової бази забезпечення кібербезпеки країни, її інформаційних ресурсів тощо;
- необхідність проведення досліджень щодо розробки нових методів (інформаційних, математичних), механізмів і заходів (організаційних тощо) вирішення проблем забезпечення кібербезпеки;
- вирішення проблем інформаційно-технологічного забезпечення кібербезпеки.

Тому не викликає сумніву актуальність дослідження проблем розробки відповідних сучасних ІТ і ІС забезпечення кібербезпеки України.

Результати дослідження. Уперше поняття «кіберпростір» було використано в Окінавській хартії глобального інформаційного суспільства (Окінавська хартія глобального інформаційного суспільства) та Конвенції про злочинність у сфері комп'ютерної інформації від 23.11.2001 року (Конвенція про кіберзлочинність).

В наш час існує багато підходів до формалізації визначення поняття «кіберпростір». Серед цих підходів вкажемо, зокрема, наступні:

- під кіберпростором розуміється середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення (ПЗ) і послуг в Інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі;
- під кіберпростором розуміється сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікації та обміну даними через системи, що функціонують в мережі Інтернет, та пов'язану з ними фізичну інфраструктуру;
- під кіберпростором розуміються всі форми мережної та цифрової активності, що включають у себе контент і дії по їхній обробці;
- під кіберпростором розуміється інформаційна інфраструктура, доступна через Інтернет;
- під кіберпростором розуміється комунікаційне середовище, що утворюється системою зв'язків між об'єктами кіберінфраструктури, серед яких слід виділити електронні обчислювальні машини, комп'ютерні мережі, ПЗ, інформаційні ресурси.

Авторами статті під кіберпростором розуміється кіберінформаційне середовище, що відображає семантику (сутність) об'єктів кіберінформаційної інфраструктури та системи відношень і зв'язків між цими об'єктами. До об'єктів кіберінформаційної інфраструктури автори відносять апаратно-технічні складові (сучасні гаджети, персональні комп'ютери тощо), програмно-технологічні складові (комп'ютерні мережі, ПЗ), інформаційні складові (інформаційні бази, веб-контенти, Інтернет-відомості тощо).

В наш час існує багато підходів до формалізації визначення поняття «кібербезпека», зокрема:

- під кібербезпекою розуміється сукупність необхідних відповідних заходів щодо мінімізація ризиків;
- під кібербезпекою розуміється захист киберсистем від шкідливого та неправильного їхнього використання та від інших деструктивних атак;
- під кібербезпекою розуміється засіб захисту від широкого кола кіберзагроз (до яких належать заходи з пошкодження інформаційних ресурсів, вилучення чужих даних тощо);
- під кібербезпекою розуміється захист ІС, що входять до складу кіберпростору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам;

- під кібербезпекою розуміється захист киберсистем від шкідливого неправильного використання та від інших злочинних дій.

Під кібербезпекою авторами розуміється стан захищеності кіберпростору держави та окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, при якому порушується їхня стабільність чи сталий розвиток, своєчасне виявлення, запобігання та відповідна нейтралізація реальних і потенційних викликів (кібервтручань, кіберзагроз, кіберзлочинів) реальним особистим, корпоративним, інституціальним і/або національним інтересам.

Авторами статті під забезпеченням кібербезпеки розуміються заходи щодо зниження ризиків отримання шкоди, яка може бути заподіяна можливими збоями у роботі в кіберпросторі, в цілому, окремих його складових (апаратно-технічних, програмно-технологічних, інформаційних) чи неправильного їх використання, а також з відновлення кіберпростору після отримання цих шкод.

- З вказаних підходів до визначення понять «кіберпростір» та «кібербезпека» випливає розуміння того, що найбільш важливими чинниками кіберпростору є:

- зміна характеру діяльності осіб, які приймають та ухвалюють рішення щодо заходів, забезпечуючих кібербезпеку об'єктів, що входять до зони впливу та відповідальності цих осіб;

- цифровізація економічної, наукової, освітньої та соціально-культурної діяльності держави і соціуму, яка передбачає утворення і інформаційно-технологічну підтримку електронно-цифрових форм створення, обробки, зберігання, захисту та переміщення інформації;

- перехід від паперового документообігу до електронно-цифрового;

- підтримка безпечної, стійкої і надійної роботи електронного операційного/інформаційного середовища, яке підтримує національну безпеку країни, мінімізує наслідки злочинних кібервтручань та максимізує переваги цифрової економіки.

Кіберпростір, як сфера здійснення потенційних злочинних дій (зокрема, несанкціонованого доступу до інформаційно-технологічного забезпечення систем чи мереж, проникнення до інформаційних баз; порушення функціонування конкретних програмних продуктів (наприклад, дезорганізація роботи ІС управління стратегічно важливими сферами діяльності держави, соціуму)), надає можливість:

- сформувати систему відношень між суб'єктами та об'єктами кіберпростору;

- визначити основні характеристики кіберзлочинів, кібервтручань і кіберзагроз, пов'язаних з особливостями існування та передавання інформації в кіберпросторі (зокрема, в мережі Інтернет);

- визначитись з основними учасниками роботи в спільному кіберпросторі;

- розглядати кіберпростір як додатковий вимір простору функціонування ІС та ІТ, розрізняючи при цьому такі рівні: фізичний (апаратне забезпечення, інфраструктура, кабелі, роутери тощо), семантичний (інформація, дані,

типизація відношень між об'єктами кіберпростору, архітектура мереж тощо), синтаксичний (протоколи передавання даних в мережі тощо);

- визначитись з основними заходами, методами, механізмами і процедурами запобігання кіберзлочинів, кібервтручань, кіберзагроз.

Реалізація вказаних вище можливостей у багатьох країнах світу здійснюється спеціальними організаційними структурами, основними функціями яких є безпечне існування в кіберпросторі, боротьба в ньому та запобігання можливим кіберзлочинам, кібервтручанням кіберзагрозам, тобто забезпечення кібербезпеки.

Серед цих структур можна, наприклад, назвати:

- об'єднане Кіберкомандування (U.S.Cyber Command-USCYBERCOM) та спеціалізований кібернетичний розвідувальний центр у США;
- управління мережних операцій у Німеччині;
- оперативний центр забезпечення кібербезпеки (CSOC) і Центр державного зв'язку (GCHQ) у Великобританії;
- центр інформаційних систем Служби безпеки (CISSS) та Національного агентства безпеки інформаційних систем (ANSSI) у Франції;
- центр компетенцій кібербезпеки на базі держкомпанії «Ростелеком» в Росії;
- центр захисту національного кіберпростору Tehila в Ізраїлі;
- департамент кіберполіції Національної поліції в Україні.

У Китаї відсутня єдина організація, що займається проблемами кібербезпеки на державному рівні. Натомість існують центр з кібербезпеки та інформатизації, Центральна військова рада, керуючі організації Копартії та Держради Китаю.

Існуючі проблеми кібербезпеки в Україні можна поділити на організаційні, технічні (апаратні, інструментальні), правові, інформаційно-технологічні (програмні, алгоритмічні, тощо).

Серед *організаційних проблем* кібербезпеки слід, насамперед, виділити:

- відсутність системної роботи з підготовки організацій (підприємств, інституцій, державних установ) до кібератак;
- приділення недостатньої уваги організаційним аспектам забезпечення кібербезпеки напротилежність технічним аспектам;
- недостатність процедур по протидії, протистоянню, реагуванню на кібератаки та мінімізації їх наслідків;
- відсутність ефективних механізмів по видаленню порушників кібербезпеки з локальних мереж організацій та глобальних міждержавних (світових) мереж;
- відсутність ефективного інструментарію забезпечення кібербезпеки, який сприяє визначенню наявності кібератаки на мережі конкретної організації та відповідному реагуванню на ці атаки;
- недостатній рівень державної (нормативно-правової, технічної, організаційної, інформаційної) допомоги організаціям, що піддалися чи

піддаються атаці, щодо вилучення зловмисників з комп'ютерних мереж тих організацій, які зазнали атак;

- відсутність достатньої державної координації дій щодо управління кібербезпекою як на рівні країни, так і на рівнях окремих підприємств (організацій, інституцій тощо);
- відповідність існуючим світовим стандартам щодо кібербезпеки повинні підтверджувати не державні аудитори, а експерти, що володіють міжнародною сертифікацією по ІТ-аудиту та кібербезпеці.

В наш час багато проблем кібербезпеки регулюються галузевими регуляторами. Промислові комп'ютерні мережі ставлять унікальні задачі перед фахівцями в області безпеки, бо вони недуже схожі на традиційні комп'ютерні мережі, особливо ті, що були побудовані ще до виникнення таких обсягів кіберзагроз, кібервтручань та кіберзлочинів. Ці мережі багато років були ізольовані від глобальних мереж. Тому в них не передбачалися заходи щодо забезпечення кібербезпеки. Але в наш час навіть така ізольованність не є запорукою кібербезпеки.

Серед *технічних проблем* кібербезпеки слід виділити, насамперед:

- відсутність точного реєстру апаратно-технічного обладнання (як підприємств, так і мереж);
- відсутність підтримки технічними засобами механізму управління змінами і реалізації політики безпеки;
- недостатні можливості апаратного моніторингу станів підприємства та мереж;
- недостатнє апаратно-технічне забезпечення запобіганню проникнення до мережі (підприємства, установи, інституції тощо) кіберзлочинців.

Для захисту комп'ютерних мереж (незалежно від інформації, яка циркулює в них), слід спочатку зрозуміти, які ІТ вони використовують та на яких принципах працюють. Забезпечення безпеки комп'ютерних мереж вимагає, зокрема, знання ПЗ, яке використовується підприємствами (або окремими користувачами), поточних налаштувань відповідного ПЗ.

Важливою проблемою безпеки комп'ютерних мереж є забезпечення прозорості дій, яка може вплинути на безпеку і надійність критично важливих інформаційних активів. Складність усунення цієї проблеми полягає в тому, що в мережах використовуються кілька різних комунікаційних протоколів.

Ще однією проблемою безпеки комп'ютерних мереж є неможливість забезпечення управління змінами та дотримання політики безпеки. Без системи запобігання неавторизованому доступу чи інформування про нього, можна вільно отримати доступ до активу і змінити його налаштування.

Кібербезпека передбачає вирішення багатьох проблем, в тому числі й боротьба з комп'ютерними вірусами. Термін «комп'ютерний вірус» уперше вжив Ф. Коен у 1984 р. Він поділив віруси на такі групи: 1) ті, що написані для наукових досліджень у галузі інформатики; 2) так звані «дикі» віруси для заподіяння шкоди користувачам.

Сьогодні написання вірусів набуває ознак промислового виробництва, їх кількість вимірюється десятками тисяч, і перед людством виникає проблема усвідомлення небезпечності цієї загрози.

Кібербезпека стикнулася з тим, що групи кіберзлочинців стають все більш «корпоративними», ставлячи своїми мішенями:

- нові технології все частіше моделюють корпоративну ієрархію (у багатьох організаціях застосовуються так звані «шлюзи», що маскують шкідливу активність; це надає можливість кіберзлочинцям захоплювати кіберпростір та уникати виявлення);
- можливості та ризики хмарних технологій (багато хмарних застосунків, ініціаторами застосування яких є співробітники компанії з метою підвищення ефективності та пошуку нових бізнес-перспектив, зараховано до категорії підвищеного ризику);
- звичне рекламне ПЗ, що стає джерелом зараження більше половини мереж підприємств.

Забезпечення кібербезпеки є актуальним для багатьох сфер діяльності, зокрема, сфер науки, техніки та технологій (особливо ІТ), що охоплюють проблеми, пов'язані із захищеністю кіберпростору країни, окремих об’єктів його інфраструктури тощо. Такими об'єктами, зокрема, є:

- ІТ підтримки кіберпростору країни (підприємства, установи тощо);
- інформаційні ресурси країни (підприємства, установи тощо);
- ІС та інтелектуальні системи різних класів;
- технології забезпечення кібербезпеки об'єктів різного рівня (система, об'єкт системи, компонент об'єкту тощо),
- процеси управління кібербезпекою об'єктів різної природи.

Згідно з (Information systems defence and security, 2011; Canada’s Cyber Security Strategy, 2010) більше третини організацій, які піддалися кібератакам у 2016 р., повідомили про істотні втрати доходів, втрачені можливості та відтік замовників. Тому більшість цих організацій після таких атак стали вдосконалювати технології, методи, механізми та процедури захисту.

Фахівці з кібербезпеки, серед основних перешкод інформаційного захисту визначають: брак ресурсів; несумісність ІС та технологій захисту; недостатню кількість відповідних фахівців (National Cyber Security Strategy, 2013).

Для забезпечення кібербезпеки авторами пропонуються наступні шляхи:

- визначення пріоритетів національної політики щодо забезпечення кібербезпеки;
- визначення пріоритетів розвитку державних структур по боротьбі з кіберзлочинністю;
- формування відповідної нормативно-правової бази забезпечення кібербезпеки;
- гармонізація заходів забезпечення кібербезпеки в Україні з поширеними світовими;
- формування механізму входження інформаційного простору України до єдиного світового;

- організація тісної взаємодії із зарубіжними законодавчими та державними органами;
- цифровізація роботи державної влади, яка передбачає розробку і використання сучасних ІТ та ІС;
- підготовка фахівців по боротьбі з кіберзлочинністю;
- централізована координація зусиль щодо ефективної взаємодії усіх учасників процесу забезпечення кібербезпеки;
- вдосконалення операційної дисципліни підприємств за рахунок збільшення уваги інформаційним технологіям захисту (коригування існуючого та розробки нового ПЗ відповідних ІС забезпечення кібербезпеки, точок контролю доступу для мережевих систем, застосунків, функцій, даних, веб-контенту, спільних мережевих інформаційних середовищ тощо);
- моніторинг ефективності захисту шляхом формування та використання чітких метрик оцінки стану кіберпростору та стану кібербезпеки;
- вдосконалення методів, механізмів і процедур кіберзахисту;
- системний підхід до кіберзахисту, який забезпечує контроль, вдосконалює сумісність компонентів складових забезпечення кібербезпеки;
- вдосконалення методів, механізмів і процедур скорочення часу, потрібного для запобігання кібератак (часу, що витрачається на виявлення/припинення кібератак, та часу, що витрачається на знешкодження наслідків кібератак).

Висновки. В наш час кібербезпека через зростаюче поширення ІТ стає одним з головних чинників існування держави та функціонування підприємств будь-якої сфери діяльності, в тому числі й соціокультурної.

Кіберпростір і кібербезпека є головними ознаками сьогодення, важливою рисою якого стає інформатизація та цифровізація всіх сфер діяльності держави, суспільства, бізнесу, науки, освіти та окремої людини.

Розвиток ІТ провокує розростання методів та технологій кібератак, але й надає можливість ефективніше від них захищатися. Ця сфера інформаційної діяльності стає все більш важливою (а інколи й найважливішою, враховуючи відповідні ситуації). Тому пошук шляхів забезпечення кібербезпеки (зокрема, розробка відповідних технологій) наразі є актуальним і важливим аспектом діяльності ІТ-сфери.

СПИСОК ПОСИЛАНЬ

Баранов, О.А., 2014. Про тлумачення та визначення поняття «кібербезпека», *Правова інформатика,* 2 (42), с. 54-62.

Конвенція про кіберзлочинність, 2001. [online] Доступно: <http://zakon.rada.gov.ua/laws/show/994_575/> [Дата звернення 10 травня 2018].

Окінавська хартія глобального інформаційного суспільства, 2000. [online] Доступно: <http://zakon.rada.gov.ua/laws/show/998_163> [Дата звернення 10 травня 2018].

Толубка, В.Б. ред., 2015. *Інформаційна та кібербезпека: соціотехнічний аспект*. Київ: ДУТ.
Фурашев, В.М., 2012. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право,* 2 (5), с. 162-175.
Canada's Cyber Security Strategy, 2010. For a stronger and more prosperous Canada. – Her Majesty the Queen in Right of Canada, [online] p. 14. Available at: <//www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrtstrtgy/cbr-scrt-strtgy-eng.pdf/> [Accessed 11 May 2018].
Cyber Security Strategy for Germany, 2011. Berlin: Federal Ministry of the Interior, p 15. Available at: <//www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische Themen/css_engl_download.pdf?_blob=publicationFile> [Accessed 10 May 2018].
Information systems defence and security: France's strategy, 2011. French Network and Information Security Agency, [online] p. 23. Available at: <//www.gouvernement.fr/sites/default /files/fichiers joints/livreblanc-sur-la-defense-et-la-securite-nationale_2013.pdf/> [Accessed 10 May 2018].
ISO/IEC 27032, 2012. Information technology – Security techniques – Guidelines for cybersecurity.
National Cyber Security Strategies, 2012. Practical Guide on Development and Execution. ENISA, [online]. Available at: <//www.enisa.europa.eu/activities/ Resilience-and-CIIP/nationalcyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementationguide> [Accessed 10 May 2018].
National Cyber Security Strategy and 2013-2014, 2013. Action Plan. – Republic of Turkey. Ministry of Transport, Maritime Affairs and Communications, [online]. p. 47. Available at: <//www.ccdcoe.org/strategies/ TUR_CyberSecurity.pdf> [Accessed 10 May 2018].

REFERENCES

Baranov, O.A., 2014. Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka» [About the perception and understanding of the «kéberbezpeka»]. *Pravova informatyka*, 2 (42), pp. 54-62.
Canada's Cyber Security Strategy, 2010. *For a stronger and more prosperous Canada. – Her Majesty the Queen in Right of Canada*, [online] p. 14. Available at: <//www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrtstrtgy/cbr-scrt-strtgy-eng.pdf/> [Accessed 11 May 2018].
Cyber Security Strategy for Germany, 2011. Berlin: Federal Ministry of the Interior, p. 15. Available at: <//www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische Themen/css_engl_download.pdf?_blob=publicationFile> [Accessed 10 May 2018].
Furashev, V.M., 2012. Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti [Cyberspace and Information Space, Cybersecurity and Information Security: Essence, Definition, Differences]. *Informatsiia i pravo*, 2 (5), pp. 162-175.
Information systems defence and security: France's strategy, 2011. *French Network and Information Security Agency*. [online] p. 23. Available at: <//www.gouvernement.fr/sites/default /files/fichiers joints/livreblanc-sur-la-defense-et-la-securite-nationale_2013.pdf/> [Accessed 10 May 2018].

ISO/IEC 27032, 2012. Information technology – Security techniques – Guidelines for cybersecurity.
National Cyber Security Strategies, 2012. *Practical Guide on Development and Execution*. ENISA, [online]. Available at: <//www.enisa.europa.eu/activities/ Resilience-and-CIIP/nationalcyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementationguide> [Accessed 10 May 2018].
National Cyber Security Strategy and 2013-2014, 2013. Action Plan. – Republic of Turkey. *Ministry of Transport, Maritime Affairs and Communications*, [online]. p. 47. Available at: <//www.ccdcoe.org/strategies/ TUR_CyberSecurity.pdf> [Accessed 10 May 2018].
Okinaiv Charter of Global Information Society, 2000. [online] Available at: <http://zakon.rada.gov.ua/laws/show/998_163> [Accessed 10 May 2018].
The Convention on Consolidation, 2001. [online] Available at: <http://zakon.rada.gov.ua/laws/show/994_575/> [Accessed 10 May 2018].
Tolubka, V.B., ed., 2015. Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt [Information and Security Policy: a sociotechnical aspect]. Kyiv: DUT.

 18.05.2018

UDC 004.946.5.056
DOI: 10.31866/2617-796x.1.2018.147257

Tkachenko Oleksandr,
PhD of physical and mathematical sciences, associate professor,
Kyiv National University of Culture and Arts,
Kyiv, Ukraine
aatokg@gmail.com
http://orcid.org/0000-0001-6911-2770

Tkachenko Kostiantyn,
assistant,
Kyiv National University of Culture and Arts,
Kyiv, Ukraine
tkachenko.kostyantyn@gmail.com
http://orcid.org/0000-0003-0549-3396

CYBERSPACE AND CYBERSECURITY: PROBLEMS, PERSPECTIVES, TECHNOLOGIES

The purpose of the article is to study and consider the general problems of such an important area of information activity of the state, business, education, science as cyber security.

The research methods are the methods of semantic analysis of the basic concepts of the considered domain (cybersecurity). The article is dedicated to the approaches to the interpretation of the concepts of cyberspace and cyber security, related to both organizational and technical aspects. The article considers the essence of cyberspace and cyber security from the standpoint of state support of this area of information activity. The article discusses the main problems of cyber security and their solutions. It is indicated that computer viruses are one of the aspects of cyber threats. Their types and main ways of their elimination and neutralization are considered.

The novelty of the study is the proposed ways to ensure the cybersecurity of the information space of enterprises and computer networks (including the Internet).

The main conclusion of the research carried out in the article is that informatization and digitalization nowadays penetrate all spheres of activity in the state, society, business, science, education, and the individual. Therefore, the search for ways to ensure cybersecurity (in particular, the development of appropriate technologies) has become an important aspect of the IT sector.

Key words: cybersecurity, cyberspace, cybercrime, computer virus, information system.

УДК 004.946.5.056
DOI: 10.31866/2617-796x.1.2018.147257

Ткаченко Александр,
кандидат физико-математических наук, доцент,
Киевский национальный университет культуры и искусств,
Киев, Украина
aatokg@gmail.com
http://orcid.org/0000-0001-6911-2770

Ткаченко Константин,
ассистент,
Киевский национальный университет культуры и искусств,
Киев, Украина
tkachenko.kostyantyn@gmail.com
http://orcid.org/0000-0003-0549-3396

КИБЕРПРОСТРАНСТВО И КИБЕРБЕЗОПАСНОСТЬ: ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ, ТЕХНОЛОГИИ

Целью статьи является исследование и рассмотрение общих проблем такой важной сферы информационной деятельности государства, бизнеса, образования, науки как кибербезопасность.

Методами исследования являются методы семантического анализа основных понятий рассмотренной предметной области (кибербезопасность). В статье рассмотрены подходы к толкованию понятий киберпространство и кибербезопасность, связанные как с организационными, так и техническими аспектами. В статье рассмотрена сущность киберпространства и кибербезопасности с позиций государственного обеспечения этой сферы информационной деятельности. В статье рассмотрены основные проблемы кибербезопасности и пути их решения. Указано, что одним из аспектов киберугрозы являются компьютерные вирусы. Рассмотрены их виды и основных пути их устранения и обезвреживания.

Новизной проведенного исследования являются предложенные пути обеспечения кибербезопасности информационного пространства предприятий и компьютерных сетей (в том числе и Интернет).

Основным выводом проведенного в статье исследования является то, что информатизация и цифровизация в наше время проникают во все сферы деятельности государства, общества, бизнеса, науки, образования и отдельного человека. Поэтому поиск путей обеспечения кибербезопасности (в частности, разработка соответствующих технологий) стали важным аспектом деятельности ИТ-сферы.

Ключевые слова: кибербезопасность, киберпространство, киберпреступления, компьютерный вирус, информационная система.