TECHNICAL SCIENCES AND TECHNOLOGIES
УДК 004.056.5
DOI: 10.25140/2411-5363-2019-1(15)-145-151

Ярослав Усов

ПРОБЛЕМИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Актуальність теми дослідження. *У статті висвітлено проблеми захищеності інформаційного середовища, запропоновано аналіз низки звітів провідних організацій у сфері захисту інформації щодо загроз кібербезпеці за останній рік, сформульовано означення захищеного інформаційного середовища (ІС) та виділено його складові.*

Постановка проблеми. *Забезпечення захисту інтересів особи, суспільства та держави від зовнішніх і внутрішніх загроз, які стосуються питань кібербезпеки.*

Аналіз останніх досліджень і публікацій. *Значний внесок у розвиток систем захисту інформації та забезпечення кібербезпеки загалом зробили провідні вітчизняні та закордонні науковці.*

Виділення недосліджених частин загальної проблеми. *Значний обсяг накопичених у цій галузі знань, недостатньо дослідженою залишились проблеми захищеності інформаційного середовища.*

Постановка завдання. *Стратегія кібербезпеки України має за мету створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства й держави.*

Виклад основного матеріалу. *Кіберпростір є інформаційним середовищем, яке функціонує за допомогою інформаційно-телекомунікаційних систем, тобто сукупності інформаційних та телекомунікаційних систем, які в процесі обробки інформації діють як єдине ціле.*

Висновки відповідно до статті. *Враховуючи існуючу останню аналітику щодо ризиків та загроз кібербезпеці, можна зробити висновок, що для забезпечення захисту інформації: за напрямками (технічний, інженерний, криптографічний та організаційний) та забезпечення захисту властивостей інформації (цілісність, конфіденційність, доступність), інструментальними оболонками ІС мають стати: апаратні, програмні, правові та апаратно-програмні засоби захисту інформації.*

Ключові слова: *захищене інформаційне середовище; кібербезпека; захист інформації.*
Бібл.: 14.

Актуальність теми дослідження. У статті висвітлено проблеми захищеності інформаційного середовища, запропоновано аналіз низки звітів провідних організацій у сфері захисту інформації щодо загроз кібербезпеці за останній рік, сформульовано визначення захищеного інформаційного середовища (ІС) та виділено його складові, а саме інструментальними оболонками ІС мають стати: апаратні, програмні, правові та апаратно-програмні засоби захисту інформації, при цьому захист інформації буде здійснюватись за технічним, інженерним, криптографічним та організаційним напрямками.

Постановка проблеми. Розвиток глобального інформаційного суспільства, швидкий темп розвитку сучасних ІТ-технологій у всіх сферах діяльності (як у державному, так і в приватному секторі), а також їх стрімке поширення серед широких мас населення обумовлюють необхідність забезпечення кібернетичного захисту інформації. Тобто забезпечення захисту інтересів особи, суспільства та держави від зовнішніх і внутрішніх загроз, які стосуються питань кібербезпеки.

Таким чином, питання захищеності інформаційного середовища виступають на перший план.

Аналіз останніх досліджень і публікацій. Значний внесок у розвиток систем захисту інформації та забезпечення кібербезпеки загалом зробили такі провідні вітчизняні та закордонні науковці, як О. Є. Архіпов, В. Л. Бурячок, Ю. О. Дрейс, С. В. Казмірчук, В. В. Козловський, О. Г. Корченко, В. А. Лахно, В. О. Хорошко, К. Шеннон, В. Гібсон, Брюс Шнайєр, Чарльз Г. Беннет, G. Bertoni, C. Chapman, B. Chor, J. Daemen, J. Dawkins, M. Endler, M. Hellman, G. Kaiser, A. Keromytis, V. Misra, J. Nieh, R. Rivest, A. Shamir, F. Silva, S. Stolfo та ін.

Разом з тим проблема забезпечення кібербезпеки залишається актуальною як для України, так і для всього світу.

Виділення недосліджених частин загальної проблеми. Проте, незважаючи на значний обсяг накопичених у цій галузі знань, недостатньо дослідженою залишились проблеми захищеності інформаційного середовища. Захисту інформаційного середовища, яке оточує сучасне суспільство в усіх сферах життєдіяльності людини, не приділено належної уваги.

Мета статті. Висвітлити проблеми захищеності інформаційного середовища.

Виклад основного матеріалу. Сьогодні наука та законодавча база щодо проблеми кібербезпеки перебувають на етапі свого активного розвитку, коли відбувається формування понятійно-категоріального апарату теорії права й держави як на законодавчому рівні, де приймаються закони, постанови, стратегії тощо, так і на рівні наукового середовища.

Так, протягом останніх кількох років було прийнято багато нормативних актів.

Наприклад, правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки висвітлені в Законі України «Про основні засади забезпечення кібербезпеки України» (№ 2469-VIII від 21.06.2018). Значна увага в Законі приділена означенню таких понять, як «кібератака», «кібербезпека», «кіберзагроза», «кіберзахист», «кіберзлочин» (комп'ютерний злочин), «кібероборона», «кіберпростір», «кіберрозвідка», «кібертероризм», «кібершпигунство» та ін. Закон визначає Національну систему кібербезпеки, яка «є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури» [4].

Законом України «Про основи національної безпеки України» (№ 2469-VIII від 21.06.2018) визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз у всіх сферах життєдіяльності. У ньому тлумачаться терміни «національна безпека», «національні інтереси», «загрози національній безпеці» [5].

Стратегія кібербезпеки України (затверджена Указом президента України від 15 березня 2016 року № 96/2016) має за мету створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Для досягнення цієї мети визначені завдання:

- створення національної системи кібербезпеки;
- посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва в цій сфері;
- *забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом*, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки й оборони України (критична інформаційна інфраструктура) [9].

Таким чином, сьогодні питання забезпечення кібербезпеки є надзвичайно актуальним, що підтверджується тенденцією до збільшення уваги держави до цього питання через зростання кількості прийнятих щодо цієї проблеми нормативно-правових актів. Є і певні досягнення в напрямку організації заходів із протидії сучасним викликам у сфері інформаційних технологій та кіберзагрозам. Зокрема, Законом України «Про основні засади забезпечення кібербезпеки України» передбачено створення Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Проте ці заходи перебувають на етапі становлення та не мають комплексного (системного) характеру. Зауважимо, що захисту інформаційного середовища, яке оточує сучасне суспільство в усіх сферах життєдіяльності людини, не приділено належної уваги.

Отже, актуальність подальшого встановлення сутності поняття «захищене інформаційне середовище» не викликає сумніву, адже розуміння цього поняття сприятиме вибудовуванню правильної стратегії щодо її захисту.

Проаналізувавши основні нормативно-правові акти щодо інформаційного середовища та його захисту ми дійшли висновку, що *на законодавчому рівні це поняття оминули.*

Зупинимось на висвітленні проблеми побудови захищеного інформаційного середовища в науковій сфері.

Спроби визначитись із дефініціями понятійних конструктів «інформаційне середовище» стали вже традиційними для значної частини дисертаційних досліджень. Але науковці так і не дійшли до одностайної думки щодо цього поняття.

Оскільки «інформаційне середовище» є змістовим ядром понятійного конструкта «захищене інформаційне середовище», то розглянемо спочатку його.

Аналіз сучасної науково-практичної літератури засвідчив, що понятійний конструкт «*інформаційне середовище*» (ІС) тлумачать таким чином:

- це частина інформаційного простору, що характеризується мінімальною територією поширення та обмеженою кількістю суб'єктів інформаційної діяльності, а також обумовлюється своєрідним інформаційним мікрокліматом, що включає сукупність способів, прийомів, заходів та умов безпосереднього здійснення інформаційної діяльності; при цьому *інформаційний простір* – це частина інформаційної сфери, обмеженої матеріальною та нематеріальною територією поширення, центром якої є сукупність суб'єктів, що здійснюють інформаційну діяльність, а її складовими – інформація та інформаційні відносини, інформаційна наука та інформаційна культура, інформаційна діяльність та інформаційна інфраструктура, інформаційне право та інформаційне законодавство [8];
- це сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, а також політичні, економічні й культурні умови реалізації процесів інформатизації [6];
- це сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням, споживанням інформації [1];
- це середовище, що постійно і дедалі більш агресивно збільшує мотивацію підростаючого покоління до споживання контенту, що циркулює в ньому; надає доступ до ресурсів у будь-який зручний час; володіє зручним, гнучким, дружнім, інтелектуальним сервісом, що допомагає людині знайти необхідні інформаційні ресурси, дані або знання; не є емоційним, воно працює відповідно запитам людини стільки, скільки їй необхідно; наповнює інформацією, даними, знаннями з величезною, постійно наростаючою швидкістю; дозволяє організувати практично безкоштовні, зручні у часі контакти між будь-якою кількістю людей, забезпечити зручні у часі контакти між будь-якою кількістю людей, забезпечити зручний і гнучкий обмін інформацією (причому в будь-якому вигляді) між ними; крок за кроком, стандартизує, а потім інтегрує в собі функціональність усіх попередніх, нині, так званих, традиційних засобів отримання,збереження, обробки і представлення необхідної людству інформації, даних та знань; бере на себе все більш рутинних операцій, пов'язаних з операційною діяльністю людини (це, до речі, одна з найбільших проблем, яку людство очікує в майбутньому – «чим більше доручень – тим більше відповідальності – тим більше небезпеки залишитися без ресурсів»); одержує дедалі більше контролю над даними та операційною діяльністю людства [7].

Таким чином, *інформаційне середовище обмежується територією та в часі. Воно характеризується певним мікрокліматом та організаційними умовами. Це може бути як окремий колектив, так і підприємство, держава і т. ін. Інформаційне середовище може включати безліч інформаційних об'єктів і зв'язків між ними, містити цілу низку засобів і технологій для обробки, накопичення, передавання та продукування інформації.*

Оскільки згідно із Законом України «Про основні засади забезпечення кібербезпеки України» кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [4], то в цьому контексті *інформаційне середовище* – це не лише суб'єкти і об'єкти (засоби, прийоми та методи захисту, тобто «*інструментальні оболонки середовища*»), а і їх змістове наповнення – сама «інформація». При цьому сам кіберпростір і є інформаційним середовищем, яке функціонує за допомогою інформаційно-телекомунікаційних систем, тобто сукупності інформаційних та телекомунікаційних систем, які в процесі обробки інформації діють як єдине ціле [3].

Згідно з ДСТУ 3396.2-97 [2] інформацію як таку захищати неможливо, тому що вона не існує сама по собі, а фіксується (відображається) в певних матеріальних об'єктах або пам'яті людей, які виступають у ролі суб'єктів (носіїв) і являють собою базовий об'єкт захисту, а оскільки інформаційне середовище являє собою сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, то його (інформаційне середовище) можна захистити.

Отже, *захищене інформаційне середовище* (ЗІС) – це сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, до якої застосовні взаємопов'язані організаційні, інженерно-технічні та *криптографічні* заходи, засоби та методи захисту, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру.

Загроза (threat) – це можлива причина небажаного інциденту, який може завдати шкоди системі або організації [12].

Ми поділили загрози ІС на загрози природного та штучного характеру. Під *природними (об'єктивними)* ми розуміємо загрози викликані дією будь-яких стихійних явищ або фізичних процесів, які не залежать від людини; під *штучними* (суб'єктивними) – що виникають унаслідок впливу людини. Також штучні загрози можуть бути як навмисними (умисні дії людини), так і ненавмисними (збої, відмови тощо).

Загалом перш ніж загроза кібербезпеки стає реальною, є ризик реалізації тієї чи іншої вразливості.

Ризик інформаційної безпеки пов'язаний із ймовірністю того, що загрози будуть реалізовуватись через використання вразливостей інформаційних активів або груп інформаційних активів і, тим самим, завдає збитків організації [12].

Сьогодні США створено Національну базу даних вразливостей (National Vulnerability Database, скорочення NVD), яка містить інформаційну базу даних національного органу стандартизації США, Національного інституту стандартів і технології. У своїй базі вони перелічують відомі вразливості та баги програмного забезпечення. Призначення бази – допомога в уникненні несанкціонованого доступу (НСД) до інформації.

У звіті, наведеному лабораторією кібератак *Varonis Global Data Risk* [14], зазначено, що:

- 21 % всіх папок відкрито для всіх;
- 58 % мають більше 100 000 відкритих папок для кожного;
- 54 % даних є застарілими;
- 41 % компаній мають понад 1000 конфіденційних файлів відкриті для всіх.

Дані, наведені у звіті CSO from IDG [11], говорить про те, що 11 найкращих статистичних даних із кібербезпеки – це:

- 90 % атак віддаленого виконання коду пов'язані з криптомінуванням;
- 92 % шкідливих програм доставляються електронною поштою;

– 56 % тих, хто приймає рішення щодо IT, вважають, що цільові атаки фішингу є їхньою загрозою безпеки;
– 77 % компрометованих атак у 2017 році були безладними;
– середня атака на вимогах компанії коштує компанії 5 мільйонів доларів;
– організація потребує в середньому 191 день для виявлення порушень даних;
– 69 % компаній бачать, що мандати на виконання вимог регулюють витрати;
– 88 % компаній витратили понад 1 мільйон доларів на підготовку до ВВП;
– 25 % організацій мають окремий відділ безпеки;
– 54 % компаній пережили інцидент безпеки системи промислового контролю;
– 61% організацій пережили інцидент безпеки IoT.

PREY Nation охарактеризував такі факти кібербезпеки [13]:

1. 70 % організацій кажуть, що вони вважають , що їх ризик безпеки значно збільшився в 2017 році (Ponemon Institute).
2. До 2020 року кількість паролів, що використовуються людьми та машинами в усьому світі, зросте до 300 мільярдів (SC Media).
3. 43 % кібератак націлені на малий бізнес (Тенденції малого бізнесу).
4. Щодня виробляється 230 000 нових зразків шкідливого програмного забезпечення - і це передбачає лише зростання (Panda Security).
5. 90% хакерів покривають свої треки за допомогою шифрування (Вансон Борн).
6. Більшість компаній займають більше шести місяців, або близько 197 днів для виявлення порушення даних (ZD Net).
7. Windows є найбільш цільовою платформою для хакерів; Android – це номер два (Комп'ютерний світ).
8. Були більш 3 мільйони відповідей крипто домкрата в період із січня по травень 2018 роки (Quick Heal).
9. Кількість варіантів зловмисного програмного забезпечення для мобільних криптозахисних пристроїв зросла з 8 варіантів у 2017 році до 25 варіантів до травня 2018 року – збільшившись утричі.

Ландшафт атак згідно зі звітом Cisco 2018 [10] такий:

- розвиток шкідливих програм;
- зашифрований зловмисний веб-трафік;
- загрози з боку електронної пошти;
- тактика ухилення від «пісочниці»;
- злочинне використання хмарних сервісів та інших легітимних ресурсів;
- Інтернет речей та DDoS-атаки;
- уразливості та використання патчів.

Висновки відповідно до статті. Таким чином, ми бачимо, що у зв'язку зі стрімким розвитком IT технологій, нові загрози виникають мало не щодня, про що свідчить наведена вище статистика. Отже, враховуючи існуючу останню аналітику щодо ризиків та загроз кібербезпеці, можна зробити висновок, що для забезпечення захисту інформації: за напрямками (технічний, інженерний, криптографічний та організаційний) та забезпечення захисту властивостей інформації (цілісність, конфіденційність, доступність), *інструментальними оболонками ІС мають стати:* апаратні, програмні, правові та апаратно-програмні засоби захисту інформації.

Список використаних джерел

1. Арский Ю. М., Гиляревский Р. С., Туров И. С., Черный А. И. Инфосфера: Информационные структуры, системы и процессы в науке и обществе. Москва: ВИНИТИ, 1996. 489 с.
2. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. [Чинний від 01.01.1998 р.]. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38934&cat_id=38836.

3. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

4. Про основні засади забезпечення кібербезпеки України: Закон України від 21.06.2018 № 2469-VIII. URL: https://uteka.ua/ua/publication/news-14-novosti-zakonodatelstva-1-osnovnye-principy-obespecheniya-kiberbezopasnosti-ukrainy-prinyat-zakon.

5. Про основи національної безпеки України: Закон України від 21.06.2018_№ 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

6. Інформаційне середовище. 2018. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5_%D1%81%D0%B5%D1%80%D0%B5%D0%B4%D0%BE%D0%B2%D0%B8%D1%89%D0%B5.

7. Петухова Л. Є., Співаковський О. В. До питання про трисуб'єктну дидактику. *Комп'ютер у школі та сім'ї*. 2007. № 5 (61). С. 7–9.

8. Селезньова О. М. Теоретико-методологічне трактування окремих засадничих категорій інформаційного права. 2019. URL: http://aphd.ua/publication-164.

9. Стратегія кібербезпеки України: затверджена Указом Президента України від 15 березня 2016 року № 96/2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016.

10. Cisco 2018. URL: https://www.cisco.com/c/uk_ua/products/security/security-reports.html.

11. CSO from IDG. 2018. URL: https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html.

12. ISO/IEC 27000. Серия стандартов. 2018. URL: https://intercert.com.ua/articles/regulatory-documents/210-iso-27000.

13. PREY Nation. 2018. URL: https://preyproject.com/blog/en/24-cybersecurity-statistics-that-matter-in-2019.

14. Varonis Global Data Risk. 2018. URL: https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf.

References

1. Arskyi, Yu. M., Giliarevskyi, R. S., Turov I. S., Chornyi, A. I. (1996). *Infosfera: Informatsionnye struktury, sistemy i protsessy v nauke i obshchestve [Infosphere: Information Structures, Systems and Processes in Science and Society]*. Moscow: VINITI [in Ukrainian].

2. DSTU 3396.2-97. Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Terminy ta vyznachennia [Information protection. Technical protection of information. Terms and definitions]. Effective as of 01.01.1998. Retrieved from http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38934&cat_id=38836.

3. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh [On Information Protection in Information and Telecommunication Systems]. № 80/94-BP (on April 19, 2014). Retrieved from https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

4. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the Basic Principles of Cybersecurity of Ukraine]. № 2469-VIII (on June 21, 2018). Retrieved from https://uteka.ua/ua/publication/news-14-novosti-zakonodatelstva-1-osnovnye-principy-obespecheniya-kiberbezopasnosti-ukrainy-prinyat-zakon.

5. Pro osnovy natsionalnoi bezpeky Ukrainy [On National Security of Ukraine]. № 2469-VIII (on 21.06.2018). Retrieved from https://zakon.rada.gov.ua/laws/show/ 2469-19.

6. Informatsiine seredovyshche [Information environment] (2018). Retrieved from https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1% 86% D1% 96% D0% B9% D0% BD% D0% B5_% D1% 81% D0% B5% D1% 80% D0% B5% D0% B4% D0% BE% D0% B2% D0% B8% D1% 89% D0% B5.

7. Petukhova, L. Ye., Spivakovskyi, O. V. (2007). Do pytannia pro trysubiektnu dydaktyku [On the issue of three-subject didactics]. *Kompiuter u shkoli ta simi – Computer at school and family, 5* (61). 7-9 [in Ukrainian].

8. Seleznev O. M. (2019). Teoretyko-metodolohichne traktuvannia okremykh zasadnychykh katehorii informatsiinoho prava [Theoretical and methodological treatment of certain basic categories of information law]. Retrieved from http://aphd.ua/publication-164.

9. Stratehiia kiberbezpeky Ukrainy [Strategy of cyber security of Ukraine]. № 96/2016 (on March 15, 2016). Retrieved from https://zakon5.rada.gov.ua/laws/show/96/2016.

10. Cisco 2018 (2018). Retrieved from https://www.cisco.com/c/en_products/security/security-reports.html.

11. CSO from IDG (2018). Retrieved from https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html.

12. ISO / IEC 27000. Standard series (2018). Retrieved from https://intercert.com.ua/articles/regulatory-documents/210-iso-27000.

13. PREY Nation (2018). Retrieved from https://preyproject.com/blog/en/24-cybersecurity-statistics-that-matter-in-2019/.

14. Herat Global Data Risk (2018). Retrieved from https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf.

UDC 004.056.5

Yaroslav Usov

PROBLEMS OF THE INFORMATIONAL ENVIRONMENT PROTECTION

Urgency of the research. *In the article the problem of security information environment presents an analysis of a number of reports leading organizations in the field of information security threats of cybersecurity last year, formulated the definition of secure information environment (IE) and highlighted its components.*

Target setting. *Ensuring the protection of the interests of the individual, society and the state from external and internal threats related to cybersecurity.*

Actual scientific researches and issues analysis. *The leading Ukrainian and foreign scientists made a significant contribution to the development of information security and cybersecurity systems in general.*

Uninvestigated parts of general matters defining. *Significant amount of accumulated knowledge in this area, insufficiently researched remained problems of the security of the information environment.*

The research objective. *Ukraine cybersecurity strategy aims to create conditions for the safe functioning of cyberspace, its use for the benefit of individuals, society and the state.*

The statement of basic materials. *Cyberspace is an information environment that operates using information and telecommunication systems that aggregate information and telecommunication systems in the information processing function as a unit.*

Conclusions. *Considering the latest analytics about the risks and threats cybersecurity, we can conclude that for the protection of information, in areas (technical, engineering, cryptography and organizational) and protection properties of information (integrity, confidentiality, availability) tool shells IC should be: hardware, software, legal and hardware-software information security.*

Keywords: *protected information environment; cybersecurity; information protection.*

References: 14.

Усов Ярослав Юрійович – викладач, Чернігівський національний технологічний університет (вул. Шевченка 95, м. Чернігів, 14035, Україна).

Usov Yaroslav – Senior Lecturer, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).

E-mail: usov75@gmail.com

ORCID: https://orcid.org/0000-0002-7771-0524

ResearcherID: G-2406-2019

Scopus Author ID: 57205630823