УДК 342.951

МАНУІЛОВ Я.С., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-8149-2745.

ЩОДО КОНЦЕПЦІЇ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОЇ МОДЕЛІ КІБЕРЗАХИСТУ

Анотація. *Визначено актуальні загрози кібербезпеці в сучасних умовах. Регламентовано складові функціонування національної системи кібербезпеки. Окреслено повноваження Держспецзв'язку у сфері побудови ефективного кіберзахисту на вітчизняних теренах. Деталізовано напрямки розбудови організаційно-технічної моделі національної системи кіберзахисту. Узагальнено компоненти організаційно-технічної моделі кіберзахисту. Актуалізовано доцільність прискорення схвалення на державному рівні Концепції організаційно-технічної моделі кіберзахисту.*

Ключові слова: *гібридна загроза, сектор безпеки і оборони, кібербезпека, кіберзагроза, кібератака, кіберзахист, кіберпростір, організаційно-технічна модель кіберзахисту, національна система кібербезпеки, цифровізація.*

Summary. *The current threats to cyber security in modern conditions have been identified. The components of the functioning of the national cyber security system are regulated. The powers of the State Special Communications Service in the field of building effective cyber defense in the domestic territory are outlined. The directions of development of organizational and technical model of the national cyber defense system are detailed. The components of the organizational and technical model of cyber defense are generalized. The expediency of accelerating the approval at the state level of the Concept of the organizational and technical model of cyber defense has been updated.*

Keywords: *hybrid threat, security and defense sector, cyber security, cyber threat, cyber attack, cyber defense, cyberspace, organizational and technical model of cyber defense, national cyber security system, digitalization.*

Аннотация. *Определены актуальные угрозы кибербезопасности в современных условиях. Регламентированы составляющие функционирования национальной системы кибербезопасности. Определены полномочия Госспецсвязи в сфере построения эффективной киберзащиты на отечественных просторах. Детализировано направления развития организационно-технической модели национальной системы киберзащиты. Обобщены компоненты организационно-технической модели киберзащиты. Актуализировано целесообразность ускорения принятия на государственном уровне Концепции организационно-технической модели киберзащиты.*

Ключевые слова: *гибридная угроза, сектор безопасности и обороны, кибербезопасность, киберугроза, кибератака, киберзащита, киберпространство, организационно-техническая модель киберзащиты, национальная система кибербезопасности, цифровизация.*

Постановка проблеми. В сучасному світі поширення кіберзагроз вражає своїми масштабами та наслідками. Адже загрози кібербезпеці останнім часом актуалізуються через дію таких негативних чинників, як: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів від потужних кіберзагроз; безсистемність заходів кіберзахисту критичної інформаційної інфраструктури; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів тощо.

За таких умов є потреба активізації зусиль з боку держави щодо кіберзахисту державних електронних інформаційних ресурсів та інформаційної інфраструктури з метою забезпечення безперебійного функціонування національної телекомунікаційної мережі та прискорення упровадження організаційно-технічної моделі національної системи кіберзахисту, вироблення єдиного підходу до питань оперативного реагування на кібератаки та кіберінциденти. У зв'язку із викладеним класичні моделі політичного, соціально-економічного та державного управління потребують перегляду в умовах суттєвої зміни кіберсередовища, особливо в умовах здійснення тотальної цифровізації усіх сфер життєдіяльності держави та суспільства. Викладене потребує активізацію діяльності владних структур держави у контексті забезпечення стану кібербезпеки, у першу чергу, прискорення створення та запровадження організаційно-технічної моделі кіберзахисту, висвітлення отриманих здобутків у цьому сегменті, відстеження динаміки відповідних процесів.

Результати аналізу наукових публікацій. Питання правового забезпечення розбудови організаційно-технічної моделі кіберзахисту досліджували у своїх працях: О. Бакалінська [1], О. Довгань [2], П. Рогов [3], В. Шеломенцев [4] та інші. Проте аналіз та узагальнення здобутків у сфері впровадження організаційно-технічної моделі кіберзахисту недостатньо висвітлено вказаними авторами, особливо в умовах масштабного поширення гібридних загроз, агресивної поведінки РФ у кіберпросторі, що посилює актуальність тематичного напрямку цього дослідження.

Метою статті є визначення подальших кроків з метою прискорення схвалення та впровадження у практичну площину Концепції організаційно-технічної моделі кіберзахисту як важливої складової менеджменту кібербезпеки в сучасних умовах масштабного поширення гібридних загроз у кіберпросторі.

Виклад основного матеріалу. Забезпечення кібербезпеки неможливе без прийняття виважених та послідовних управлінських рішень на планових засадах, що передбачає розробку та вжиття необхідних заходів, визначення алгоритму спільних дій з боку державних органів та інших суб'єктів забезпечення кібербезпеки, встановлення конкретних строків та відповідальних за їх виконання структур. Національна система кібербезпеки – органічна системна сукупність загальних і спеціальних суб'єктів її забезпечення та взаємопов'язаних і взаємоузгоджених між ними заходів організаційно-технічного, навчально-виховного, нормативно-правового, соціально-економічного, правоохоронного, оборонного, інформаційного характеру. Її основою є державні органи, правоохоронні структури, які відповідно до покладених завдань та в рамках взаємодії виконують функції із забезпечення безпеки кіберпростору України, громадські об`єднання, підприємства, установи, організації незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Першочерговими заходами щодо розбудови національної системи кібербезпеки є: вдосконалення державного управління у цій сфері; створення нормативно-правової бази для забезпечення такої діяльності; запровадження протоколів спільних дій суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів; підвищення спроможностей суб'єктів забезпечення кібербезпеки з виявлення, попередження та припинення правопорушень, пов'язаних із несанкціонованими доступом та діями, порушенням приватності, конфіденційності, цілісності та автентичності, поширенням та продажем даних і інформації, насамперед з обмеженим доступом; профілактика, виявлення та усунення умов і факторів загроз кібербезпеці держави; запровадження активних дієвих заходів у сфері боротьби з кібертероризмом, зокрема терористичними

актами та диверсіями у кіберпросторі, кібератаками на державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури.

В умовах нарощування російської агресії, найвищим національним пріоритетом є подальше зміцнення складових сектору безпеки і оборони. Тільки успішна і послідовна державна політика, що виходить із максимально ефективного використання власних людських, фінансових, матеріально-технічних та інформаційних ресурсів, неухильне просування у напрямі європейської і євроатлантичної інтеграції, а також всебічний розвиток взаємодії зі стратегічними союзниками, у тому числі з НАТО, надасть змогу захистити інтереси України і створити синергетичний ефект національної єдності та міжнародної співпраці. За таких умов модель сектору безпеки і оборони України має бути суттєво змінена, що передбачає передусім уточнення повноважень, взаємоузгодження функцій та завдань суб'єктів сектору безпеки і оборони з метою унеможливлення виконання ними дублюючих або невластивих їм функцій, розпорошення сил та засобів. Має запрацювати чіткий механізм керівництва сектором безпеки і оборони як функціональним об'єднанням з визначенням особливостей його функціонування в мирний час, у кризових ситуаціях та в особливий період, що неможливо без формування відповідної нормативно-правової бази.

Важливою складовою нормального та безперебійного функціонування національної системи кібербезпеки є прискорення впровадження організаційно-технічної моделі кіберзахисту з метою оперативного (кризового) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості усіх комунікаційних систем. На цьому фоні актуальним та своєчасним питанням є визначення та узагальнення шляхів удосконалення вітчизняної організаційно-технічної моделі кіберзахисту, яка є важливою складовою менеджменту кібербезпеки у сучасному світі.

Згідно із чинним законодавством саме на Держспецзв'язку покладено обов'язок розробки, впровадження і поширення організаційно-технічної моделі кіберзахисту. Тобто у рамках компетенції та відповідно до функціональності саме Держспецзв'язку є регулятором з кібербезпеки для органів державної влади, а для інших галузей має виконувати роль координатора – сприяє розслідуванню та відновленню нормального стану після кібератак, сповіщає бізнес-структури (приватний сектор) про нові реальні та потенційні кіберзагрози. Запорукою ефективної діяльності складових національної системи кібербезпеки оптимальним є ініціювання, розробка та запровадження під егідою Держспецзв'язку на підставі спільних нормативно-правових актів механізму оперативної комплексної взаємодії в межах компетенції та згідно із функціональністю її суб'єктів з метою виявлення і нейтралізації кібератак та кіберзагроз із протидії їм, боротьби з кібертероризмом та кіберзлочинністю, забезпечення дієвого кіберзахисту, інформаційного обміну в режимі реального часу між суб'єктами забезпечення кібербезпеки та Національним координаційним центром кібербезпеки при РНБО України. Так, організаційно-технічна модель національної системи кіберзахисту, передбачає, передусім, забезпечення безперебійного функціонування автоматизованих систем органів військового та державного управління, оскільки в сучасних умовах з метою ефективного відбиття кібератак та гарантування надійного кіберзахисту вказані системи повинні вдосконалюватися в напрямі підвищення ступеня їх автоматизації та комп'ютеризації.

Ураховуючи викладене, актуальною та сучасною вимогою сьогодення є перегляд принципів побудови автоматизованих систем органів військового та державного управління кібербезпекою як у мирний, так і у воєнний час. Також у контексті

розбудови національної системи кібербезпеки важливим напрямком залишається перспективне використання її інтелектуальної підсистеми. Саме інтелектуальна підсистема кібербезпеки надасть можливість не тільки оперативно виявляти нові, невідомі та нетипові кібератаки в процесі моніторингу кіберпростору, але й системно аналізувати виявлені кіберзагрози й автоматично обирати параметри функціонування автоматизованих систем в умовах деструктивних впливів без погіршення їх основних характеристик.

Крім вдосконалення складових функціонування автоматизованих систем органів військового та державного управління, у рамках розбудови організаційно-технічної моделі національної системи кіберзахисту мають бути реалізовані можливості щодо: автоматичної зміни властивостей та параметрів підсистем і засобів забезпечення кібербезпеки залежно від зміни стану кіберпростору (виявлення активності потенційних джерел кіберзагроз, виявлення кібератак) та результатів проведених кібератак; автоматичної оцінки змін захищеності автоматизованих систем органів військового та державного управління від кіберзагроз при диференційованих умовах функціонування; автоматизованої підтримки прийняття рішень щодо протидії кібератакам та автоматичного впливу на джерело кібератаки; автоматизованої підтримки прийняття рішень щодо перерозподілу ресурсів систем та засобів забезпечення кібербезпеки на випадок їх функціонального ураження в результаті кібератак; обліку у процесі посилення кібербезпеки всіх взаємопов'язаних та взаємодіючих факторів, які можуть впливати на рівень її забезпечення; контролю та зниження нецільового навантаження на комплекси засобів автоматизації систем кібербезпеки; прогнозування на підставі отриманих у процесі експлуатації програмно-апаратних комплексів знань та факторів, що можуть впливати на рівень захищеності автоматичних систем управління від усіх видів кіберзагроз.

Також важливими елементами організаційно-технічної моделі кіберзахисту є розробка та використання сучасних засобів і методів, відповідних алгоритмів, завдяки яким в системі слід передбачити можливості реалізації запобіжних апаратно-програмних впливів та завдання ударів на виявлені джерела кібератак або на відповідні інформаційні системи і ресурси. Отже, важливою умовою створення організаційно-технічної моделі кіберзахисту є застосування апаратної та програмної платформ у складі довіреного програмно-апаратного середовища як сукупності технічних і програмних засобів, організаційних заходів, які забезпечують створення, застосування та розбудову систем спеціального призначення, що відповідають за умови забезпечення кібербезпеки.

Для забезпечення безпеки інформаційних ресурсів можуть використовуватися такі програмно-технічні рішення, як: обладнання комп'ютерів антивірусними програмами та засобами, які гарантують надійний захист від шкідливого програмного забезпечення, що може міститися в Інтернет-ресурсах та в додатках електронної пошти; міжмережеве екранування з метою обмеження несанкціонованого доступу до комп'ютерів через мережу; використання системи DLP, яка забезпечує захист інформації від копіювання на змінні носії, незареєстровані ресурси в зовнішній мережі; застосування програмно-технічних рішень для забезпечення контролю фізичного доступу до інформаційних та інформаційно-комунікаційних систем.

Як слушно зазначають А.В. Чунарьова та А.В. Чунарьов, роль організаційних заходів щодо захисту інформації в системі заходів кібербезпеки визначається своєчасністю, адекватністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації. Проведення організаційно-технічних та організаційно-правових заходів здійснюються завдяки таким принципам захисту інформації: науковий

підхід до організації захисту інформації; планування захисту; керування системою захисту; безперервність процесу захисту інформації; мінімальна достатність організації захисту; системний підхід до організації та проектування систем і методів захисту інформації; комплексний підхід до організації захисту інформації; відповідність рівня захисту інформації; гнучкість захисту; багатозональність захисту, що передбачає розміщення джерел інформації в зонах із контрольованим рівнем її безпеки; обмеження кількості осіб, які допускаються до захищеної інформації; особиста відповідальність персоналу за збереження довіреної інформації [5].

Таким чином, основою організаційно-технічної моделі кіберзахисту є система функціонування автоматизованих систем органів військового та державного управління, яка включає такі складові: постійний моніторинг кіберпростору, комплексний захист інформації, оперативне оповіщення про кібератаки або кіберзагрози та протидія їм; впровадження стандартів управління кібербезпекою. Загальноприйнятим є розуміння постійного моніторингу кіберпростору як сукупності апаратно-програмних систем і засобів, що дають змогу здійснювати оцінку ситуації (обстановки) в кіберпросторі, систематично збирати, обробляти та аналізувати інформацію про можливі кіберзагрози, наявні кіберінциденти завдяки цифровому проникненню в зовнішні мережі та комп'ютери, що потребує розробки передових розвідувальних кібертехнологій.

Комплексний захист інформації в інформаційних та інформаційно-телекомунікаційних системах має базуватися на таких підсистемах: попередження та виявлення комп'ютерних атак, криптографічний захист інформації, контроль стану й функціональної стабільності автоматизованих систем. Оперативне оповіщення про кібератаки або кіберзагрози передбачає вибір оптимальної стратегії запобігання та протидії кібератакам за допомогою програмно-апаратних і телекомунікаційних засобів, які призначені для своєчасного доведення до відповідних суб'єктів забезпечення кібербезпеки оперативної інформації в режимі реального часу про можливі або виявлені кіберзагрози або кібератаки, їхні параметри та зміст, а також вибору дієвих та доступних заходів кіберзахисту.

Впровадження організаційно-технічної моделі кіберзахисту неможливе без запровадження на підприємствах, в установах та організаціях, що належать до об'єктів критичної інфраструктури, ефективних систем менеджменту кібербезпеки, вжиття відповідних заходів щодо їх сертифікації згідно з міжнародними стандартами, наприклад, ISO/IEC 27032:2012 "Information technology – Security techniques – Guidelines for cybersecurity" – підвищення рівня кібербезпеки в глобальній мережі Інтернет. Тому для установ, організацій, підприємств, які провадять діяльність на міжнародному рівні, важливою умовою підвищення ефективності цієї діяльності є наявність сертифікату відповідності міжнародним стандартам серії ISO/IEC 27001 (оцінки й управління інформаційною безпекою) "Інформаційні технології – засоби забезпечення безпеки", що ґрунтуються на авторитетних британських стандартах BS 17799 (з 2000 року визнаних міжнародними у форматі "International Standart ISO/IEC 17799. Information technology – Code of practice for information security management".

У рамках вказаного стандарту тезаурус кібербезпеки повинен бути узгоджений із понятійним апаратом базових термінів у сфері інформаційної безпеки, при цьому стандарт являє собою керівні принципи у вигляді рекомендацій за такими напрямами: оцінка потенційних ризиків; дотримання вимог безпеки користувачами Інтернету; забезпечення кібербезпеки організаціями – провайдерами. Уважається, що завдяки використанню рекомендацій ISO/IEC 27032:2012 провайдери Інтернет-послуг зможуть підвищити загальний рівень кібербезпеки, забезпечити кіберзахист ресурсів

комп'ютерних мереж загального користування. Упровадження сучасної організаційно-технічної моделі кіберзахисту надасть змогу посилити координацію діяльності складових сектору безпеки і оборони України, їх техніко-технологічні можливості в рамках цілісної управлінської системи для боротьби з кіберзагрозами незалежно від способу, мети та суб'єкта їх реалізації, надасть можливість векторно спрямувати науковий та людський потенціал державних органів на забезпечення безпеки кіберпростору.

Виходячи із вищевикладеного, пріоритетними завданнями держави у цій площині залишаються: створення сучасної гнучкої національної системи кібербезпеки з метою ефективної взаємодії уповноважених органів під час реалізації заходів, спрямованих на її забезпечення; створення сприятливих умов для співпраці між державним і приватним секторами з питань протидії кіберзагрозам; активізація міжнародного співробітництва у сфері забезпечення кібербезпеки; формування передумов для забезпечення кіберзахисту інформаційної інфраструктури держави, передусім – об'єктів критичної інформаційної інфраструктури; прискорення розробки та практичного впровадження сучасної організаційно-технічної моделі забезпечення кіберзахисту.

Задля забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту щорічно проводяться планові заходи аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість, тобто оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законодавства України, установ і організацій незалежно від форм власності.

Водночас, в нашій країні здійснюються поступальні кроки у напрямку розбудови вітчизняної організаційно-технічної моделі кіберзахисту. Протягом останніх років реалізовано низку практичних рішень, спрямованих на розробку організаційно-технічної моделі кіберзахисту. Так, окреслено державний контур кіберзахисту, активно та динамічно розвивається Національна телекомунікаційна мережа, працює Центр реагування на кіберзагрози, проведено масштабну модернізацію системи захищеного доступу до Інтернету. Також на виконання положень Закону України "Про основні засади забезпечення кібербезпеки в Україні" [6] Держспецзв'язку було офіційно презентовано Концепцію організаційно-технічної моделі кіберзахисту як важливої складової національної системи кібербезпеки [7]. У підготовці проекту "Організаційно-технічної моделі кіберзахисту" взяли участь фахівці і науковці Національного інституту стратегічних досліджень, Держспецзв'язку, Національної академії державного управління при Президентові України, фахівці приватних компаній та незалежні експерти.

За задумом "Організаційно-технічна модель кіберзахисту" складатиметься з трьох вертикально та горизонтально інтегрованих інфраструктур.

Перший рівень – це організаційно-керуюча інфраструктура кіберзахисту, її складовими елементами є суб'єкти національної системи кібербезпеки.

Другий рівень являє собою технологічну інфраструктуру кіберзахисту, яка складається з сукупності сил та засобів кіберзахисту. Це відповідні технологічні підрозділи суб'єктів кіберзахисту різних секторів (військовий та цивільний). На цьому рівні забезпечується відповідна комплексна взаємодія технологічних підрозділів, тобто обмін інформацією, моніторинг, забезпечення сталої безпеки кіберпростору тощо. Технологічна інфраструктура має три горизонти – національний, галузевий (регіональний) та об'єктовий.

Третій рівень – це базисна інфраструктура кіберзахисту, що забезпечує основні спроможності кіберзахисту. Базисна інфраструктура складається з двох шарів: захищена інформаційна інфраструктура та обізнане суспільство (громади та громадяни). Важливими питаннями впровадження цієї моделі залишаються її ресурсне забезпечення та механізми її імплементації.

Аналіз положень вказаної моделі дозволив визначити, що кіберзахист – це цілеспрямована діяльність із забезпечення безпеки кіберпростору та важлива складова національної системи кібербезпеки.

Також акцентовано увагу розробників на посиленні ризиків глобальної цифровізації, у зв'язку з чим існує вірогідність збільшення кількості кібератак та кіберзагроз, що потребує схвалення адекватних системних заходів реагування і відповідно, додаткових ресурсних витрат за напрямком посилення спроможностей відповідальних суб'єктів у сфері забезпечення кібербезпеки.

Висновки.

З метою розвитку технологічної платформи для розгортання національної системи кібербезпеки сьогодні вживаються заходи з розвитку її організаційно-технічної моделі як сукупності систем, комплексів і заходів, призначених для забезпечення кібербезпеки об'єктів критичної інфраструктури та кіберзахисту державних електронних інформаційних ресурсів, а також її телекомунікаційної платформи — Національної телекомунікаційної мережі. Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки відповідно до ч. 5 ст. 8 Закону України "Про основні засади забезпечення кібербезпеки в Україні" здійснює Державний центр кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

У контексті посилення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки ключовим елементом оргтехмоделі є виконання відповідних завдань Центром реагування на кіберзагрози Держспецзв'язку, який було відкрито на початку 2018 року. З метою забезпечення ефективного обміну інформацією про кіберінциденти, аналізу загрозливих тенденцій, виявлення основних джерел кіберінцидентів, організації навчання щодо протидії кіберзагрозам, а також забезпечення належного рівня функціонування Центру реагування на кіберзагрози Держспецзв'язку, сьогодні розгортається єдина інтерактивна база даних про кіберінциденти для потреб основних суб'єктів забезпечення кібербезпеки як складових її національної системи.

На жаль, в Україні все ще спостерігаються повільні темпи, незавершеність заходів, спрямованих на повноцінне та повноформатне впровадження організаційно-технічної моделі кіберзахисту, яка має відповідати та адекватно реагувати на сучасні гібридні загрози, попереджувати їх негативні наслідки, нівелювати виклики у кіберпросторі та сприяти впровадженню глобальних тенденцій у розвиток індустрії кібербезпеки. У зв'язку із викладеним, в сучасних умовах, доцільно прискорити схвалення на державному рівні Концепції організаційно-технічної моделі кіберзахисту як фундаментального документа у цій площині.

Використана література

1. Бакалінська О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* 2019. № 9. С. 100-108.

2. Довгань О.Д., Тарасюк А.В. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право.* № 3(26)/2018. С. 94-103. URL: http://nbuv.gov.ua/ UJRN/Infpr_2018_3_11

3. Рогов П.Д., Воровичб Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері: зб. наук. праць Центру воєнно-стратегічних досліджень Національного університету оборони України ім. Івана Черняховського. 2017. № 1. С. 64-72. URL: http://nbuv.gov.ua/UJRN/Znpcvsd_2017_1_13

4. Шеломенцев В.П. Основні проблеми побудови системи кібернетичної безпеки України *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2. С. 183-186. URL: http://nbuv.gov.ua/UJRN/ boz_2014_2_44

5. Чунарьова А.В., Чунарьов А.В. Принципи організації захисту інформації в сучасних інформаційно-комунікаційних системах і мережах. URL: http://www.rusnauka.com/16_ADEN_2010/Informatica/68642.doc.htm

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

7. В Україні презентовано Організаційно-технічну модель кіберзахисту. URL: https://cip.gov.ua/ua/news/klyuchovi-predstavniki-sub-yektiv-nacionalnoyi-sistemi-kiberbezpeki-ukrayini-obgovorili-organizaciino-tekhnichnu-model

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