УДК 342.951

ГРИГОРЕНКО В.А., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-0511-3402.

НАЙКРАЩІ ЗАРУБІЖНІ ПРАКТИКИ РОЗБУДОВИ МЕХАНІЗМІВ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ КІБЕРБЕЗПЕКИ

Анотація. *Визначено роль та місце державно-приватного партнерства у сфері забезпечення кібербезпеки в сучасних умовах. Деталізовано моделі розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки через призму набутого досвіду окремих передових країн світу (Ізраїль, Німеччина, США, Великобританія). Узагальнено позитивні здобутки зарубіжного досвіду державно-приватного партнерства у сфері забезпечення кібербезпеки. Сформульовано проблемні питання врегулювання державно-приватного партнерства як складової національної системи кібербезпеки. Запропоновано шляхи удосконалення державно-приватного партнерства у сфері забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, кіберзахист, кібератака, кіберзагроза, кіберпростір, стартап, державно-приватне партнерство, ІТ-ринок, цивільний сектор безпеки.*

Summary. *The role and place of public-private partnership in the field of cybersecurity in modern conditions are determined. Models of building public-private partnerships in the field of cybersecurity through the prism of the experience of some advanced countries (Israel, Germany, USA, GB) are detailed. The positive achievements of foreign experience of public-private partnership in the field of cybersecurity are summarized. Problematic issues of public-private partnership development as a component of the national cybersecurity system are formulated. The directions of improvement of public-private partnership in the field of cybersecurity are proposed.*

Keywords: *cybersecurity, cyberdefense, cyberattack, cyberthreat, cyberspace, startup, public-private partnership, IT- market, civil security sector.*

Аннотация. *Определены роль и место государственно-частного партнерства в сфере обеспечения кибербезопасности в современных условиях. Детализированы модели развития государственно-частного партнерства в сфере обеспечения кибербезопасности через призму приобретенного опыта отдельных передовых стран мира (Израиль, Германия, США, Великобритания). Обобщены позитивные достижения зарубежного опыта государственно-частного партнерства в сфере обеспечения кибербезопасности. Сформулированы проблемные вопросы государственно-частного партнерства как составляющей национальной системы кибербезопасности. Предложены направления усовершенствования государственно-частного партнерства в сфере обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, киберзащита, кибератака, киберугроза, киберпространство, стартап, государственно-частное партнерство, ИТ-рынок, гражданский сектор безопасности.*

Постановка проблеми. Проблема забезпечення безпеки у кіберпросторі не має кордонів. Кожна держава розробляє та впроваджує механізми забезпечення кібербезпеки, використовуючи досягнення світової практики. Важливою складовою та прерогативою цих процесів є залучення приватних гравців, які також активно використовують кіберпростір та його потенційні можливості. У наш час спостерігається підвищена активність приватного сектору та інституцій громадянського суспільства у заходах, спрямованих на забезпечення кібербезпеки як на національному, так і на міжнародному рівнях.

З метою реалізації сучасних завдань у сфері забезпечення кібербезпеки держава повинна активніше: покладатися на підтримку та допомогу підприємств ІКТ-галузі, волонтерських організацій, наукових установ, закладів освіти та громадських організацій; впроваджувати дієві механізми громадського контролю в питаннях забезпечення кібербезпеки; налагоджувати оперативний обмін у режимі реального часу інформацією між державними органами, приватним сектором і громадянами стосовно кіберзагроз, кібератак та кіберінцидентів; залучати представників експертного середовища наукових установ, професійних об'єднань та громадських організацій до підготовки галузевих індикаторів стану кібербезпеки, проектів відповідних нормативних актів у цій сфері. За таких умов висвітлення кращих практик зарубіжного досвіду у сфері розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки є актуальним та своєчасним, особливо в умовах тенденційного поширення гібридних загроз та агресивної експансіоністської політики РФ проти України, у тому числі й у кіберпросторі.

Результати аналізу наукових публікацій. Питанням державно-приватного партнерства у сфері забезпечення кібербезпеки певним чином приділяли увагу у своїх наукових працях такі вчені, як: М. Гребенюк, Б. Леонов [1], Д. Дубов [2], В. Круглов [3], Р. Прав [4], В. Шеломенцев [5] та інші. Проте висвітлення кращих практик зарубіжного досвіду у сфері розбудови державно-приватного партнерства забезпечення кібербезпеки жоден із вказаних авторів не здійснював, що посилює тематичну актуальність цієї наукової публікації.

Метою статті є деталізація заходів, які вживаються для розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки у провідних зарубіжних країнах світу, та на їх підставі узагальнення і визначення дієвих кроків щодо удосконалення національної системи кібербезпеки з урахуванням спроможності цивільного сектору безпеки.

Виклад основного матеріалу. Важливим компонентом посилення спроможностей держави у сфері забезпечення кібербезпеки є саме побудова конструктивного діалогу у форматі державно-приватного партнерства. Набутий міжнародний досвід переконливо доводить, що без комплексної взаємодії держави та приватного сектору неможливо побудувати ефективний та надійний кіберзахист. Державно-приватне партнерство передбачає таку форму співпраці, за якої досягаються цілі та завдання, що сприятимуть забезпеченню національної безпеки, економічного розвитку та побудові безпечного кіберсередовища для усіх громадян. Тобто модель державно-приватного партнерства можливо охарактеризувати як динамічну взаємодію між державними та приватними інституціями, які здійснюють спільну реалізацію функцій з метою забезпечення безпеки у кіберпросторі.

Держава Ізраїль залишається першою країною у світі з найбільшими інвестиціями у кібербезпеку та рекордною кількістю стартап-компаній. Динамічний розвиток цієї сфери залишається першочерговим пріоритетом держави. Так, наприклад, у Ізраїлі на виконання політики Уряду дедалі активніше залучаються до співпраці у сфері забезпечення кібербезпеки компанії приватного сектору. У цій країні в 2017 році в секторі кібербезпеки було задіяне 420 підприємств, а на кіберіндустрію витрачено понад $815 млн. Невипадково держава Ізраїль зарекомендувала себе як світовий лідер у сфері інноваційних кібертехнологій. На ізраїльські передові підприємства, які співпрацюють із міжнародними корпораціями та стартапами, покладаються завдання щодо розробки сучасних та інноваційних систем захисту від кібератак з метою адекватного реагування на ситуативну динаміку та загрози в кіберпросторі. Приватні компанії з кіберзахисту

активно використовують штучний інтелект для розпізнавання шкідливого програмного забезпечення та виявлення агресивної поведінки в Інтернеті [1, с. 48-49].

Згідно із даними дослідницького центру "Cyber Security Ventures", дев'ять ізраїльських компаній входять у топ – 100 найбільш успішних та прибуткових світових компаній у сфері кібербезпеки. Наприклад, Check Point Software посідає у цьому рейтингу четверте місце з ринковою вартістю $15 млрд. Останнім часом, за Ізраїлем закріпився бренд іміджу під назвою "Startup Nation", оскільки у цій державі за сприяння Уряду активно процвітає стартап-індустрія. Венчурний фонд "Flint Capital" інвестував $3 млн. в ізраїльський стартап "CyberX", який спеціалізується на виробництві програмного забезпечення у сфері кібербезпеки для промислових потреб Інтернету речей. Стартап "Checkmarx", який надає сервісні послуги з метою аналізу вихідного коду програмного забезпечення та виявлення кіберзагроз на ранніх стадіях, залучив $ 84 млн. інвестицій. Стартап "Saferide Technologies" представляє на ринку власно розроблений багаторівневий програмний пакет з метою захисту систем кібербезпеки під назвою "vSentry Core", який дозволяє виявляти та ліквідовувати усі потенційні загрози, захищатися від хакерів та різноманітних шкідливих атак.

Тобто сфера підтримки стартапів за тематикою кібербезпеки не залишається поза увагою великих інвесторів. У сучасних умовах інфраструктура сфери кібербезпеки включає у цій країні понад 150 компаній, серед яких представлені стартапи, венчурні фонди, науково-дослідницькі проекти, які реалізують співпрацю між високотехнологічними компаніями та академічними й науковими колами. Спостерігається тенденція перетворення держави Ізраїль на міжнародний центр високих технологій та світового лідера у сфері кібербезпеки. Ізраїль одним із перших почав налагоджувати співпрацю у сфері кібербезпеки між заінтересованими суб'єктами, науковими установами та організаціями приватного сектора.

Одна із провідних ініціатив Ізраїлю в цій царині – проект "CyberSpark Innovation Initiative143", започаткований 2014 року як спільне підприємство INCB муніципалітету Беершеба, університету Бена Гуріона, та бізнес-партнерів: EMC (RSA), Lockheed Martin, IBM, Deutsche Telekom, JVP Cyber Labs та Elbit.IDF та CERT-IL також беруть участь в ініціативах CyberSpark, серед яких – робота зі спільнотою дипломатів та проведення семінарів для фахівців із кібербезпеки з усього світу. З моменту запуску, CyberSpark створив "екосистему" для багатьох заінтересованих сторін – уряду, наукових кіл, бізнесу, місцевого самоврядування та громадянського суспільства. Уряд потужно підтримує ізраїльську галузь кібербезпеки та відповідний бізнес через декілька джерел. Так, Офіс головного вченого в Міністерстві економіки (зараз Національне агентство з технологічних інновацій) надав різноманітні науково-дослідні та інвестиційні інструменти через свій фонд досліджень і розробок, програми Kidma, Magnetta Meimad з підтримки досліджень у царині кібербезпеки та розробок подвійного призначення.

Крім CyberSpark, близько 20 науково-дослідних центрів у галузі кібербезпеки, що працюють над рішеннями безпеки для світового ринку, створені в Ізраїлі транснаціональними корпораціями, серед яких – PayPal, IBM, VMWare, General Electric, Cisco, CA Technologies, McAfee та Ciscom. Наразі корпорації також створюють в Ізраїлі кіберцентри. Так в Ізраїлі працюють дев'ять науково-дослідних університетів, два з яких 2016 року увійшли до сотні найкращих наукових установ у світі й мають кафедри інформатики (Єврейський університет та "Техніон"). У рамках національних програм у середніх школах Ізраїлю проводяться дослідження й тренінги з кібербезпеки. Загалом на сьогодні серед пріоритетів Ізраїлю в галузі кібербезпеки слід виділити забезпечення прозорості дій у цій царині для громадськості, інституційні інновації та державні

інвестиції як короткострокового (субсидії для компаній, що працюють у галузі кібербезпеки), так і довгострокового характеру. Таким чином, можна констатувати, що протягом останніх десятиліть Ізраїль перебуває у світовому авангарді інновацій та науково-технологічних напрацювань у галузі кібербезпеки, яка безпосередньо залежить від обсягу залучених інвестицій та інновацій. Культура інновацій Ізраїлю, його унікальний людський капітал та зусилля з національної безпеки створюють ідеальне середовище, задовольняючи цю потребу як на місцевому, так і на глобальному рівні.

Німеччина є однією із ключових країн, форми державно-приватного партнерства якої є ефективним інструментом у системі забезпечення кіберзахисту країни в цілому. Сфера державно-приватного партнерства у галузі кібербезпеки між операторами критично важливої інфраструктури та відповідними державними органами регулюється в Німеччині планом реалізації "UP KRITIS", який розроблений і фінансується урядом цієї країни. З одного боку, платформа "UP KRITIS" регулярно інформує національних партнерів про відповідні заходи щодо захисту критичної інфраструктури; з іншого – рішення, прийняті членами "UP KRITIS", представляються на розгляд європейських структур, впливаючи тим самим на європейський порядок денний на ранніх стадіях запобігання кіберзагроз, посилюючи інтереси Німеччини в даному секторі безпеки. Також кожен громадянин має доступ до веб-сайту *//www.bsi-fuer-buerger.de* та телефонної гарячої лінії для передачі та отримання інформації чи рекомендацій щодо дій у випадку скоєння кібератаки. Тобто одним із напрямів державно-приватного партнерства, ініційованих Німеччиною, є заохочення співпраці між державними структурами та приватними організаціями, громадськими структурами на ранніх етапах дослідницького та інноваційного процесу як у країні, так і в ЄС в цілому. Зазначене сприятиме синхронізації доступу до інноваційних та надійних європейських рішень – продуктів, послуг та програмного забезпечення для ІКТ.

Цікавим видається досвід США у цій площині. Позитивним прикладом сучасних моделей паритетної взаємодії державного та приватного секторів у сфері забезпечення кібербезпеки є створення на базі Департаменту внутрішньої безпеки США автоматизованої програми відстеження кіберзагроз, яка надає змогу забезпечити автоматизований обмін інформацією між державним і приватним секторами. Аналогічні приклади існують і в європейських країнах (Великобританія, Нідерланди). Також у США з метою прогнозного супроводження діяльності державних інституцій та приватного сектору у сфері забезпечення кібербезпеки створено некомерційний дослідний центр "TechAmerica Foundation", який об'єднує фахівців та експертів 1200 компаній з метою визначення орієнтовно-планових обсягів щорічного фінансування кібероборони, при цьому акценти діяльності постійно передбачають значне збільшення витрат виходячи із потенційних та реальних кіберзагроз. Також у США успішно функціонує некомерційна організація як приватний інститут "SANS" (SysAdmin, Audit, Network and Security) [6], який займається дослідженнями, тренінгами та сертифікацією в галузі комп'ютерної безпеки. На сьогодні "SANS" являє собою один із найбільших сертифікаційних центрів у цій галузі, де окрім традиційного навчання, здійснюється експериментальна діяльність. З метою збільшення аудиторії слухачів використовуються різноманітні формати – навчання он-лайн, проведення науково-практичних заходів, конференцій тощо. Щорічно по усьому світу 12 тис. осіб проходять курс навчання в "SANS". Періодично ця інституція проводить змагання між своїми інструкторами, а також здійснює пошук нових тренерів.

1 листопада 2016 року була представлена Стратегія кібербезпеки Великобританії на 2016 – 2021 роки [7]. У цьому документі підкреслюється важливість трансформацій, що сприятимуть впровадженню цифрових технологій як публічними, так і приватними

підприємствами, але наголошено на значній ролі бізнесу та приватних організацій у реагуванні на кіберзагрози. При цьому акцентована увага на важливості партнерства між урядом та приватним сектором у розробці стандартів кібербезпеки. Згідно із цим документом у цій країні був створений Інститут досліджень питань кібербезпеки, який об'єднав зусилля дослідників, котрі займаються цією темою в різних університетах по всій країні. Інститут фінансується за рахунок гранту 3,8 млн. фунтів. Він став частиною програми Уряду Великобританії, направленої на розширення можливостей академічної науки у сфері кібербезпеки.

Очікується, що діяльність цієї структури надасть методичну допомогу компаніям, приватним особам та державним організаціям, допоможе схвалювати обґрунтовані рішення щодо використання заходів з метою забезпечення безпеки кіберпростору та кардинально вирішувати складні завдання у державному та приватному секторах, об'єднавши їх зусилля. Структурно ця інституція є віртуальною та об'єднує сім університетів, партнерство семи британських науково-дослідницьких рад, серед яких виділяється "Research Councils UK" (RCUK), Дослідницька Рада інженерних та фізичних наук (EPSRC), Департамент бізнесу та навичок (BIS). Таким чином, діяльність цієї організації сприятиме залученню провідних вчених у сфері кібербезпеки, у тому числі соціологів, математиків, програмістів з усіх куточків Сполученого Королівства. Актуалізовано, що ця країна є однією із найбільших Інтернет-економік світу та має гігантський сектор послуг у сфері кібербезпеки, у зв'язку з чим діяльність інституту зарекомендувала себе на правах досвідченого центру вироблення стратегічних рішень у сфері блокування та ліквідації кіберзагроз та їх масштабів. Слід вказати, що на вітчизняному ринку кібербезпеки Великобританії функціонує достатня кількість авторитетних ІТ-компаній, які мають значний досвід у цій сфері, вдало впроваджують новітні технології та надають послуги щодо виявлення кіберінцидентів, виконують комплексні комп'ютерні експертизи тощо.

Невипадково у стратегічних документах ЄС з кібербезпеки неодноразово наголошується на важливості розбудови державно-приватного партнерства в боротьбі з кібератаками і кіберзлочинністю. Слід зазначити, що при вирішенні завдань у сфері забезпечення кібербезпеки держава та її правоохоронні органи відчувають потребу в залученні кваліфікованих спеціалістів з приватного ІТ-сектору, які мають знання, навички та вміння щодо розробок, впровадження та обслуговування сучасного програмного забезпечення. Також важливим питанням залишається впровадження ефективного проектного менеджменту з питань забезпечення кібербезпеки, у тому числі, у питаннях управління науково-технічними проектами з використанням механізмів державно-приватного партнерства. Організація постійної взаємодії у рамках державно-приватного партнерства також може використовуватися з метою скоординованого управління кіберризиками на національному рівні.

Таким чином, на основі узагальнення здобутків зарубіжного досвіду державно-приватного партнерства у сфері забезпечення кібербезпеки можна виділити такі його складові: основною його метою є побудова конструктивного діалогу та плідної співпраці, реальна довіра між приватним сектором та державними інституціями; заохочення співпраці між державними та приватними організаціями на ранніх етапах дослідницького та інноваційного процесу. Державно-приватні інвестиції активно спрямовуються на дослідницькі програми щодо розробки інструментів та прототипів у сфері посилення кіберзахисту та його складових. Серед перспективних спільних заходів у сфері посилення кібербезпеки виділяються: залучення стартапів та науковців щодо проведення комп'ютерно-технічних експертиз; розробки і впровадження сучасного програмного

забезпечення для виявлення і запобігання кіберзагрозам на ранніх стадіях; постійний моніторинг кіберпростору; підготовка галузевих фахівців, розробка та сприяння реалізації освітніх онлайн-платформ тощо.

Висновки.

Як переконливо засвідчує статистика, станом на 2020 рік 25 % компаній – світових лідерів у сфері розробки програмного забезпечення для мобільних платформ мали свої офіси або представництва в Україні. Також в Україні працює понад чотирьох тисяч IT-компаній і понад 110 R&D центрів всесвітньо відомих міжнародних компаній. У 2019 році частка IT-індустрії в українській економіці становила 4 % ВВП, а у цій сфері було задіяне понад 150 тисяч осіб. У той самий час, важливо розуміти, що на цьому етапі розвитку галузі вітчизняний IT-ринок переважно працює на аутсорсі. Тобто надає послуги іноземним компаніям і не надто поспішає у створенні власних технологічних компаній. Саме через нерозвиненість в Україні компаній, які програмують для власних продуктів, та відсутність технологічних дослідницьких центрів оцінка вітчизняного IT-ринку досить низька, порівнюючи із світовими.

На цьому фоні в рамках розбудови державно-приватного партнерства актуальним завданням залишається консолідація зусиль та посилення спроможностей складових сектору безпеки і оборони України та недержавного сектору, особливо під егідою Національного координаційного центру кібербезпеки при РНБО України, який відіграє провідну роль у питаннях розбудови державно-приватного партнерства.

В Україні на ринку кібербезпеки діє досить багато асоціацій, IT-компаній, структур громадянського суспільства, які мають значний досвід і техніко-технологічні напрацювання в зазначеній сфері, надають послуги з виявлення комп'ютерних атак, розслідування обставин виявлених інцидентів, формування доказів при виконанні обстеження комп'ютерних систем і проведенні комп'ютерних експертиз. Чимало вітчизняних IT-компаній, які посіли міцні позиції в зазначеній сфері, не тільки демонструють високу ефективність, напрацювали багаторічний досвід, мають значний штат компетентних фахівців та експертів необхідної кваліфікації, але й проявляють зацікавленість у розширенні своєї діяльності, опануванні нових сегментів ринку послуг кібербезпеки. Серед них можна виділити такі: Українська міжбанківська асоціація членів платіжних систем "ЄМА", Інтернет Асоціація України, Українська Антипіратська Асоціація, Всеукраїнська асоціація "Інформаційна безпека та інформаційні технології", громадська організація ISACA, Об'єднання підприємств "Український мережевий інформаційний центр", Платформи громадянського суспільства "Україна – ЄС", Центр реагування на комп'ютерні надзвичайні події "CERT", IT-компанія "Linkos Group", IT-компанія "Eset", Експертно-правова консалтингова компанія "ЮрЕкс", Київський експертно-дослідний центр тощо. Тому ще одним перспективним напрямом у зазначеному контексті видається залучення спеціалістів та експертів комерційних IT-структур з метою використання сучасного обладнання та програмного забезпечення щодо збору цифрових доказів і проведення комп'ютерно-технічних експертиз, що дасть змогу спільно з правоохоронними органами створювати потужні спеціалізовані криміналістичні лабораторії з метою виконання експертиз будь-якої складності.

Враховуючи сучасні засади та перспективні тенденції реформування цивільного сектору безпеки, на сьогодні важливим завданням держави є врегулювання питання державно-приватного партнерства у сфері кібербезпеки на законодавчому рівні. Тому актуалізується важливість питань кібербезпеки при розгляді системних дій держави у секторі безпеки за сучасних умов. Тобто доцільно розвивати державно-приватне партнерство у сфері забезпечення кібербезпеки, зміцнювати правову основу такої

співпраці. Необхідно прискорити діяльність за такими напрямами: врегулювати на законодавчому рівні питання щодо: посилення державно-приватного партнерства у сфері кібербезпеки, визначення форми і методи здійснення такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проектів у цій сфері, залучення на регулярній основі представників наукових установ, громадських організацій та незалежних експертів у сфері кібербезпеки до розроблення нормативно-правових актів, нормативних документів та стандартів у цій сфері; стимулювання розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом, що пріоритетно використовуватимуться для обробки та захисту державних інформаційних ресурсів, а також на об'єктах критичної інформаційної інфраструктури; співпраці всіх суб'єктів забезпечення кібербезпеки, зокрема в рамках державно-приватного партнерства, задля досягнення стратегічних цілей, заснування ініціатив, вироблення узгоджених планів та проектів у сфері кібербезпеки.

Розбудова державно-приватного партнерства у сфері забезпечення кібербезпеки має відбуватися за такими перспективними напрямами: укладання та забезпечення виконання партнерських угод за участю держави та провідних вітчизняних ІТ-компаній, у тому числі й зарубіжних; формування відповідного профільного законодавства, що передбачає розробку вітчизняних правових норм, якими повинні регулюватися процедурні питання участі недержавних структур у зборі цифрових даних та доступу до електронних доказів, порядок та умови державної атестації й сертифікацій таких компаній тощо.

Актуальним питанням залишається необхідність узгодження між державою та інституціями громадянського суспільства питань активізації залучення інвестицій у цивільний сектор кібербезпеки, покращення фахової підготовки спеціалістів у цій сфері, спільної діяльності щодо організації дієвого кіберзахисту, сприяння держави розвитку краудсорсингу в Україні, підвищення довіри та досягнення порозуміння у відносинах державно-приватного партнерства. Держава має проводити постійний моніторинг громадської думки в питаннях забезпечення кібербезпеки, зокрема за допомогою прогнозів-опитувань, соціологічних досліджень та технологій контент-аналізу.

Використана література

1. Гребенюк М.В., Леонов Б.Д. Досвід Їзраілю у сфері забезпечення кібербезпеки *Інформація і право*. № 2(25)/2018. С. 45-50.

2. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с.

3. Круглов В.В. Державно-приватне партнерство у сфері кібербезпеки. *Вчені записки ТНУ ім. В.І. Вернадського. Серія: "Державне управління"*. 2018. № 3. Т. 29(68). С. 57-61.

4. Прав Р.Ю. Роль механізму державно-приватного партнерства у розвитку кібербезпеки України на сучасному етапі. *Інвестиції: практика та досвід.* 2019. № 21. С. 143-150.

5. 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

6. The SANS (SysAdmin, Audit, Network and Security). URL: https://www.sans.org/about

7. National Cyber Security 2016 – 2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

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