УДК 004.056.5
DOI https://doi.org/10.32782/2524-0374/2024-12/157

КІБЕРБЕЗПЕКА В ЄС: НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ТА ОСНОВНІ СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ

CYBERSECURITY IN THE EU: LEGAL AND REGULATORY FRAMEWORK AND KEY STAKEHOLDERS

Кумейко А.В., к.ю.н.,
докторант відділу аспірантури і докторантури
Національна академія Служби безпеки України

У статті досліджено питання нормативно-правового забезпечення кібербезпеки в ЄС. Вказано, що спочатку пандемічна криза, а згодом й повномасштабне вторгнення та початок бойових дій безперечно показали, наскільки наша економіка та життєдіяльність в цілому залежить від цифрових технологій. Констатовано, що на сучасному етапі розвитку людства, переважна більшість секторів економіки, таких як фінанси, охорона здоров'я, енергетика та транспорт, повністю покладаються на інфраструктуру доступу та безпеки інформаційних та комунікаційних технологій. Отже, зловмисне посягання на критичну інфраструктуру є серйозним глобальним ризиком. Так, останні статистичні дані наочно показують вразливість цифрового ринку Європи, який постійно піддається кіберзагрозам. Крім того підкреслено, що кібербезпека за своєю суттю є глобальною проблемою. Так, за даними Всесвітнього економічного форуму, кібератаки є одним із найбільш ймовірних глобальних ризиків. Кібератаки стали поширеною небезпекою для приватних осіб, а компанії ставлять їх на сьоме місце за ймовірністю та восьме за впливом ризику, а також на друге місце за тривожністю ризику для ведення бізнесу в усьому світі протягом наступних 10 років.

Зроблено висновок, що кібербезпека актуалізується тим, що має прямий вплив на фундаментальні права людини; впровадження заходів кібербезпеки пов'язано з деякими очевидними викликами, як-то: 1) масштабність кіберпростору; 2) кібербезпека за своєю суттю є міждисциплінарним, складним явищем, яке вимагає знань та досвіду у багатьох сферах: інформаційних технологій, політології, інженерії, економіки, права тощо; 3) кібербезпека є глобальною і багатонаціональною проблемою, що швидко розвивається, а кібератаки рідко обмежується виключною юрисдикцією; запровадження стандартів у кібербезпеці є ключовим питанням; Європейський Союз відіграє вирішальну роль у кібербезпеці та розробці єдиної нормативно-правової бази.

Ключові слова: кібербезпека, цифрова епоха, ЄС, нормативно-правова база, кіберзагрози.

The article examines the issues of regulatory and legal support of cybersecurity in the EU. It is indicated that first the pandemic crisis, and then the full-scale invasion and the outbreak of hostilities, undoubtedly showed how much our economy and life in general depend on digital technologies. It is stated that at the present stage of human development, the vast majority of sectors of the economy, such as finance, healthcare, energy and transport, fully rely on the infrastructure of access and security of information and communication technologies. Consequently, malicious encroachment on critical infrastructure is a serious global risk. Thus, the latest statistics clearly show the vulnerability of the European digital market, which is constantly exposed to cyber threats. In addition, it was emphasized that cybersecurity is inherently a global problem. Thus, according to the World Economic Forum, cyberattacks are one of the most likely global risks. Cyberattacks have become a common danger for individuals, with companies ranking them seventh in likelihood and eighth in risk impact, as well as second in risk anxiety for doing business globally over the next 10 years.

It is concluded that cybersecurity is actualized by the fact that it has a direct impact on fundamental human rights; The implementation of cybersecurity measures is associated with some obvious challenges, such as: 1) the scale of cyberspace; 2) cybersecurity is inherently interdisciplinary, complex phenomenon that requires knowledge and experience in many areas: information technology, political science, engineering, economics, law, etc.; 3) cybersecurity is a rapidly evolving global and multinational problem, and cyberattacks are rarely limited to exclusive jurisdiction; Implementing cybersecurity standards is a key issue; The European Union plays a crucial role in cybersecurity and the development of a common regulatory framework.

Key words: cybersecurity, digital age, EU, regulatory framework, cyber threats.

Постановка проблеми. Спочатку пандемічна криза, а згодом й повномасштабне вторгнення та початок бойових дій безперечно показали, наскільки наша економіка та життєдіяльність в цілому залежить від цифрових технологій. Зокрема, під час пандемії 40% працівників ЄС перейшли на дистанційну роботу [1], що, абсолютно вплинуло на повсякденне життя [2]. Утім варто підкреслити, що цифрові технології об'єднують не лише людей, зокрема кількість підключених пристроїв вже перевищує кількість людей на планеті [3], і за прогнозами, до 2025 року їхня кількість зросте до 25 мільярдів [4].

Доцільно вказати, що на сучасному етапі розвитку людства, переважна більшість секторів економіки, таких як фінанси, охорона здоров'я, енергетика та транспорт, повністю покладаються на інфраструктуру доступу та безпеки інформаційних та комунікаційних технологій. Отже, зловмисне посягання на критичну інфраструктуру є серйозним глобальним ризиком. Так, останні статистичні дані наочно показують вразливість цифрового ринку Європи, який постійно піддається кіберзагрозам. Як вказано у звіті Агентства Європейського Союзу з кібербезпеки (ENISA) «Основні інциденти в ЄС та світі» [5], значною загрозою стали кіберризики. Зокрема Міжнародний валютний фонд оцінив щорічні втрати від кібератак у 9% чистого прибутку банків у всьому світі, або близько $100 млрд. [6].

За даними Європейської комісії, вплив на європейський бізнес та організації конкретного типу кіберінциденту, а саме кіберкрадіжки комерційної таємниці, орієнтовна вартість кіберкрадіжки комерційної таємниці становить близько 60 мільярдів євро економічного зростання та до 289 000 робочих місць у ЄС [7].

Крім того, слід підкреслити, що кібербезпека за своєю суттю є глобальною проблемою. Так, за даними Всесвітнього економічного форуму, кібератаки є одним із найбільш ймовірних глобальних ризиків. Кібератаки стали поширеною небезпекою для приватних осіб, а компанії ставлять їх на сьоме місце за ймовірністю та восьме за впливом ризику, а також на друге місце за тривожністю ризику для ведення бізнесу в усьому світі протягом наступних 10 років [6].

Отже, статистичні дані свідчать про зростаючу небезпеку з боку діяльності кіберзлочинців, яка зобов'язує ЄС вживати рішучих і термінових заходів для захисту цифрового ринку, а отже, і всієї нашої економіки з глобальним і системним підходом.

ЄС усвідомлює ці ризики не лише щодо прямих потенційних збитків, але й щодо втрати довіри до цифрового

ринку, що може призвести до більш серйозних наслідків. Без довіри та безпеки неможливо розвиватися або використовувати можливості нової цифрової епохи. Занепокоєння щодо безпеки є основним стримуючим фактором для використання онлайн-сервісів [8]. Варто вказати, що ЄС працює над мережевою та інформаційною безпекою та кіберзлочинністю більше десяти років, зокрема ще у 2013 році було опублікувано перший документ, що стосується широкого спектру кіберзагроз: Стратегію кібербезпеки Європейського Союзу. Важливо зазначити, що документ підкреслює, що в контексті кібербезпеки централізований нагляд ЄС не є панацеєю, і, отже, національні уряди повинні залишатися основними суб'єктами, які організовують запобігання та реагування на кіберінциденти на національному рівні.

Крім того Європейським Союзом були зроблені й інші кроки задля захисту цифрового ринку, а саме, було прийнято Директиву про мережеву та інформаційну безпеку (NISD), Закон ЄС про кібербезпеку, Загальний регламент про захист даних (GDPR), які відображають поточну регуляторну стратегію щодо захисту даних, критичної інфраструктури від ризиків кібербезпеки.

З огляду на вищезазначене, кібербезпека заслуговує на серйозну рефлексію щодо функціонування ЄС і, зокрема, цифрового ринку. Занепокоєння щодо безпеки є основним стримуючим фактором для використання онлайн-сервісів. Ризик втрати довіри до цифрового ринку може спричинити серйозні наслідки для держави, тому кібербезпека є фактором довіри до нових варіантів використання цифрових послуг і, таким чином, може сприяти трансформації суспільства у цифрову епоху.

Аналіз останніх досліджень і публікацій. До вивчення різних аспектів засад забезпечення кібербезпеки присвячено праці: В.Л.Бурячка, Ю.Г.Даника, С.Г.Вдовенка, І.В.Діордіца, Є.О.Живила, В.В.Куцаєва, О.О.Чернонога та ін.

Метою статті є аналіз нормативно-правового забезпечення кібербезпеки в ЄС.

Виклад основного матеріалу. Як зазначено у Стратегії кібербезпеки: «покращення кібербезпеки має важливе значення для того, щоб люди довіряли, використовували та отримували вигоду від інновацій, зв'язку та автоматизації, а також для захисту основних прав та свобод, включаючи право на недоторканність приватного життя та захист персональних даних, а також свободу вираження поглядів та інформації» [9]. Важливо, що Стратегія кібербезпеки ЄС закріплює, що «особливо серйозний кіберінцидент або атака може стати достатньою підставою для того, щоб держава-член посилатися на положення про солідарність ЄС» [10].

Доцільно зазначити, що ЄС вирішує питання кібербезпеки за допомогою трьох складових: мережевої та інформаційної безпеки, правоохоронних органів та оборони. Рада ЄС прийняла Рамки політики кіберзахисту ЄС як додатковий документ для підтримки європейських інституцій у їхній роботі, пов'язаної з кіберзахистом, та надання Стратегії кібербезпеки ЄС інструменту впровадження.

У сфері мережевої та інформаційної безпеки основними учасниками ЄС є Європейська комісія, Європейське агентство мереж та інформаційної безпеки (ENISA) – це агентство ЄС, яке займається кібербезпекою та надає підтримку державам-членам, установам ЄС та підприємствам у ключових сферах, включаючи імплементацію Директиви NIS.

Центри обміну інформацією та аналізу (ISAC) сприяють співпраці між спільнотою кібербезпеки в різних секторах економіки. Подальший розвиток ISAC як на рівні ЄС, так і на національному рівні є пріоритетом для Комісії. У співпраці з ENISA Комісія також сприяє створенню нових ISAC у секторах, які не охоплені. Консорціум ISAC ЄС, що надає повноваження, під наглядом Комісії, надає юридичну, технічну та організаційну підтримку ISAC.

Спільний дослідницький центр (JRC) Комісії активно сприяє кібербезпеці в ЄС. Наприклад, JRC розробила таксономію кібербезпеки, чим узгоджує термінологію, що використовується в кібербезпеці, щоб була можливість мати більш чіткий огляд складових кібербезпеки в ЄС [11]. JRC також опублікував звіт, який дає уявлення про поточний ландшафт кібербезпеки ЄС та його історію, під назвою «Кібербезпека – наш цифровий якор» [12].

Крім того, відповідно до Директиви NIS, державичлени ЄС зобов'язані забезпечити функціонування групи реагування на інциденти комп'ютерної безпеки (CSIRT), також відомі як групи реагування на комп'ютерні надзвичайні ситуації (CERT). Всі типи операторів основних послуг та постачальників цифрових послуг повинні бути охоплені призначеними CSIRT.

В Україні CSIRT – група реагування на інциденти комп'ютерної безпеки ДержНДІ технологій кібербезпеки, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України. Основним функціональним напрямом діяльності CSIRT є забезпечення протидії кіберзагрозам в автоматизованих системах та інформаційно-комунікаційних системах ДержНДІ технологій кібербезпеки та підприємств енергетичної галузі. Це позаштатна структурна одиниця ДержНДІ технологій кібербезпеки, яка взаємодіє із з командами CERT-UA, Системою виявлення вразливостей і реагування на кіберінценденти та кібератаки, зовнішніми організаціями та іншими суб'єктами національної системи кібербезпеки [13].

У сфері правоохоронних органів основними учасниками ЄС є Європейський центр боротьби з кіберзлочинністю (ЕС3) та EUROPOL, CEPOL та Eurojust. На додаток до вже існуючих інструментів боротьби зі кіберзагрозами, була прийнята Директива 2013/40/ЄС про напади на інформаційні системи та Рамкове рішення Ради 2005/222/ JHA, яке спрямовано на боротьбу з масштабними кібератаками, вимагаючи від держав-членів посилення національного законодавства про протидію кіберзлочинності та запровадження жорсткіших санкцій для злочинців.

У сфері оборони основними суб'єктами є Європейська служба зовнішньої діяльності (EEAS), військовий штаб Європейського Союзу (EUMS) та Європейське оборонне агентство (EDA). Крім того у 2016 році була створена Європейська організація з кібербезпеки (ECSO) для того, щоб виступати в якості контрагента Комісії в договірному державно-приватному партнерстві, що охоплює Horizon 2020.

Разом з тим ЄС працює з партнерами для просування спільних інтересів у політиці кібербезпеки. Зокрема 9-й кібердіалог між ЄС та США відбувся в Брюсселі в грудні 2023 року, завдяки чому ЄС та США розвинули співпрацю в таких сферах, як кібердипломія, управління кризовими ситуаціями, нарощування потенціалу, кібербезпека критичної інфраструктури (включаючи звітування про інциденти), кібербезпека апаратних та програмних продуктів (включаючи Спільний план дій щодо кібербезпечних продуктів) та різні аспекти кібербезпеки нових технологій, таких як штучний інтелект.

З 2021 року ЄС та Україна провели два кібердіалоги. У 2023 році Агентство ЄС з кібербезпеки ENISA формалізувало робочу угоду з вітчизняними фахівцями задля сприяння розбудові потенціалу, обміну передовим досвідом та ситуаційної обізнаності. ЄС також запосередкував кібердіалог з Індією, Японією, Республікою Корея та Бразилією. Перший кібердіалог між ЄС та Великобританією відбувся в Брюсселі в грудні 2023 року.

Кібербезпека також обговорюється в контексті двостороннього цифрового партнерства та цифрових діалогів, а також цифрового альянсу ЄС-LAC, регуляторного діалогу ЄС-Західних Балкан, структурованого діалогу ЄС-НАТО щодо стійкості та структурованого діалогу ЄС-НАТО з кібербезпеки та оборони. Зокрема у 2023 році Цільова група ЄС-НАТО з питань стійкості критичної інф-

раструктури опублікувала звіт, який відобрахував важливі наскрізні сектори [14].

Отже, кібербезпека має важливе значення, зокрема, як зазначено в Аналітичній записці «Виклики ефективній політиці ЄС у сфері кібербезпеки»: «Кіберекосистема ЄС є складною та багатошаровою, охоплює низку сфер внутрішньої політики, таких як юстиція та внутрішні справи, єдиний цифровий ринок та політика досліджень. У зовнішній політиці кібербезпека відіграє важливу роль у дипломатії, а також дедалі частіше стає частиною нової оборонної політики ЄС... із залученням багатьох стейкхолдерів. Об'єднати всі його розрізнені частини – це серйозний виклик» [15].

Як було зазначено вище, у 2013 році інституції Європейського Союзу спільно опублікували те, що можна вважати наріжним каменем стратегії кібербезпеки ЄС [16]. Тому кібербезпека має важливе значення «для побудови стійкої, зеленої та цифрової Європи» [17]. Після прогресу, досягнутого в рамках попередніх стратегій, він містить конкретні пропозиції щодо застосування трьох основних інструментів – регуляторних, інвестиційних та політичних – для вирішення таких аспектів, як: стійкість, технологічний суверенітет та лідерство, розбудова оперативного потенціалу для запобігання, стримування та реагування, а також просування глобального та відкритого кіберпростору.

Європейський Союз свого часу усвідомив необхідність сильної та надійної стратегії кібербезпеки, саме тому у 2019 році було опубліковано новий нормативно-правовий акт, а саме Закон про кібербезпеку, метою якого було регулювання та створення схеми сертифікації кібербезпеки продуктів ІКТ, послуг ІКТ та процесів ІКТ для подолання поточної фрагментації внутрішнього ринку. Для досягнення цієї мети було встановлено, що Агентство Європейського Союзу з мережевої та інформаційної безпеки (ENISA) відіграватиме вирішальну роль у процесі такої сертифікації. Насправді, як і в багатьох випадках, на яких наголошували інституції ЄС, відсутність сумісних рішень (технічних стандартів), практики та загальносоюзних механізмів сертифікації є серед інших прогалин, що впливають на єдиний ринок у сфері кібербезпеки. «Це ускладнює для європейського бізнесу конкуренцію на національному, союзному та глобальному рівнях. Це також зменшує вибір життєздатних і придатних для використання технологій кібербезпеки, до яких мають доступ приватні особи та компанії» [15].

Крім того, дуже важливо, щоб Європейська система сертифікації кібербезпеки була встановлена в єдиний спосіб у всіх державах-членах, щоб запобігти незаконним «покупкам сертифікації» в різних державах-членах.

Метою європейських схем сертифікації кібербезпеки було визначено забезпечення того, щоб продукти ІКТ, ІКТ-послуги та процеси ІКТ, сертифіковані за такими схемами, відповідали визначеним вимогам, спрямованим на захист доступності, автентичності, цілісності та конфіденційності даних, що зберігаються, передаються або обробляються, або пов'язаних функцій або послуг, що пропонуються цими продуктами або доступні через них, послуг і процесів протягом усього їх життєвого циклу.

Ще одним важливим документом є Директива (ЄС) 2016/1148 про заходи щодо високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (NIS) [18], яка стала першим нормативно-правовим актом для досягнення стратегічного пріоритету кіберстійкості, закладеного в Стратегії кібербезпеки ЄС.

Як зазначалося вище, перша Стратегія кібербезпеки ЄС включає кілька фундаментальних принципів, що лежать в основі підходу ЄС до кібербезпеки, за якими слідують 5 стратегічних пріоритетів. «Таким чином, пропозиція щодо Директиви NIS була зроблена в рамках першого стратегічного пріоритету «Досягнення кіберстійкості» [19].

Директива NIS підкреслює «відсутність єдиних вимог до операторів основних послуг та постачальників цифрових послуг», заявляючи, що «держави-члени мають дуже різні рівні готовності, що призвело до фрагментації підходів у всьому Союзі. Це призводить до нерівного рівня захисту споживачів та бізнесу та підриває загальний рівень безпеки мережевих та інформаційних систем у межах Союзу». У цьому контексті фрагментації метою директиви є досягнення «високого загального рівня безпеки мереж і систем формування в межах Союзу з метою поліпшення функціонування внутрішнього ринку» та встановлення загального рівня безпеки для мережевих та інформаційних систем, оскільки ці системи є життєво важливим компонентом для усунення ризиків, які можуть виникнути у важливих секторах суспільства. Директива NIS зосереджена на двох типах постачальників послуг: операторах основних послуг (OES) та відповідних постачальниках цифрових послуг (DSP) [20].

З 25 травня 2018 року Загальний регламент про захист даних (ЄС) 679/20161 (GDPR) став основною правовою базою в ЄС із захисту даних, яка безпосередньо застосовуватиметься до всіх держав-членів, скасовуючи чинну Директиву про захист даних 95/46/ЕС2. Відповідно до Регламенту, одним із основних зобов'язань для всіх компаній, які виступають або як контролери даних, або як обробники даних, є безпека обробки персональних даних [21].

Актуальність захисту персональних даних констатується з першого рядка Положення, де закріплено, що: «захист фізичних осіб у зв'язку з обробкою персональних даних є основоположне право. Стаття 8(1) Хартії основних прав Європейського Союзу та стаття 16(1) Договору про функціонування Європейського Союзу передбачають, що кожна людина має право на захист персональних даних, що стосуються її або неї [21].

У регламенті усвідомлюється, що: «Швидкий технологічний розвиток та глобалізація принесли нові виклики для захисту персональних даних. Масштаби збору та обміну персональними даними значно зросли. Технології дозволяють як приватним компаніям, так і державним організаціям використовувати персональні дані в безпрецедентних масштабах для здійснення своєї діяльності. Фізичні особи все частіше роблять особисту інформацію загальнодоступною та глобальною» [21].

Висновки. Отже, підсумовуючи наведене доцільно дійти деяких висновків щодо стратегії кібербезпеки Європейського Союзу, а саме:

1) Кібербезпека актуалізується тим, що має прямий вплив на фундаментальні права людини. Немає жодних сумнівів щодо важливості кібербезпеки, враховуючи потенційний вплив на основоположне право на приватність та захист персональних даних, а також на свободу вираження поглядів та інформації. Як закріплено у Стратегії кібербезпеки ЄС [10]: «покращення кібербезпеки має важливе значення для того, щоб люди довіряли, використовували та отримували вигоду від інновацій, зв'язку та автоматизації, а також для захисту основних прав і свобод, включаючи право на недоторканність приватного життя та захист персональних даних, а також свободу вираження поглядів та інформації» [9].

2) Впровадження заходів кібербезпеки пов'язано з деякими очевидними викликами, як-то: 1) масштабність кіберпростору; 2) кібербезпека за своєю суттю є міждисциплінарним, складним явищем, яке вимагає знань та досвіду у багатьох сферах: інформаційних технологій, політології, інженерії, економіки, права тощо; 3) кібербезпека є глобальною і багатонаціональною проблемою, що швидко розвивається, а кібератаки рідко обмежується виключною юрисдикцією.

3) Запровадження стандартів у кібербезпеці є ключовим питанням. Важливість стандартів та сертифікатів з метою гармонізації впровадження технічних та організа-

ційних заходів кібербезпеки не може піддаватися сумнівам, оскільки впровадження стандартів у сфері кібербезпеки може бути адекватним рішенням для досягнення відповідності нормативним актам, забезпечення гармонізаційного регулювання в ЄС та посилення вимог до безпеки.

Власне кажучи, кібербезпека стикається з тією ж проблемою, яка присутня в багатьох інших сферах політики ЄС, а саме: відсутність гармонізації, що призводить до фрагментарного підходу не тільки в усьому Союзі, а й за його межами, через необхідність вертикальної узгодженості на рівні як ЄС, так і держав-членів.

У цьому контексті, як слушно вказується у спеціальній літературі, держави-члени мають дуже різний рівень захищеності, що призводить до фрагментарних підходів у протидії, а також до нерівного рівня захисту споживачів та бізнесу та підриває загальний рівень безпеки мережевих та інформаційних систем в цілому. [22]. Відсутність єдиних вимог до операторів основних послуг та постачальників цифрових послуг, у свою чергу, унеможливлює створення глобального та ефективного механізму співпраці на рівні Союзу; кібербезпека є «чудовим прикладом сфери, в якій різні сфери політики повинні бути об'єднані (вимога до горизонтальної узгодженості), і де необхідно вживати заходів на рівні як ЄС, так і держав-членів (закликаючи до вертикальної послідовності)» [23].

4) Європейський Союз відіграє вирішальну роль у кібербезпеці та розробці єдиної нормативно-правової бази. Зокрема дії ЄС видаються необхідними і пропорційними, враховуючи наднаціональний характер атак на кібербезпеку, і відповідно до принципу надання захисту не можуть бути оптимально досягнуті державами-членами на регіональному та місцевому рівнях. Проте, як вказують окремі автори, застосування неєвропейських міжнародних стандартів, таких як стандарти NIST або ISO, не може бути найбільш адекватною відповіддю, оскільки ці стандарти не враховують унікальність та інтерес європейського ринку. Власне кажучи, останні зусилля ЄС докладаються у сфері сприяння гармонізації Єдиного ринку кібербезпеки щодо продуктів та послуг з метою впровадження єдиної європейської сертифікації та стандарту кібербезпеки, що є спільним підґрунтям для всіх держав-членів [23].

У цьому сенсі Стратегія кібербезпеки підкреслює важливість ETSI, CENELEC та ENISA, заявляючи: «Комісія підтримуватиме розробку стандартів безпеки»; «Така робота має ґрунтуватися на поточній роботі зі стандартизації Європейських організацій зі стандартизації (CEN, CENELEC та ETSI), Координаційної групи з кібербезпеки (CSCG), а також на досвіді ENISA, Комісії та інших відповідних гравців» [24]. Варто розуміти, що за відсутності ініціатив ЄС та лідерства у цій сфері зростає ризик фактичної стандартизації практик шляхом консолідації ринку, оскільки інноваційні постачальники послуг на базі ЄС можуть поступово консолідуватисяв групи компаній, які не є членами ЄС.

ЛІТЕРАТУРА

1. European Commission. (2020). Telework in the EU before and after the COVID-19: where we were, where we head to. URL: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf
2. Gartner. (14 July 2020). Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to WorkRemotely Some of the Time. URL: https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time
3. Estimated by telecommunications trade association GSMA URL: https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf
4. The International Data Corporation forecast 42.6 billion connected machines, sensors, and cameras URL: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.
5. European Union Agency for Cybersecurity (ENISA). (2020). Main Incidents in the EU and worldwide. ENISA. URL: https://www.enisa.eur
6. World Economic Forum. (2020). Global Risks Report URL: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
7. Special Eurobarometer 499 : Europeans' attitudes towards cyber security (cybercrime) URL: https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en
8. 2020 Digital Economy and Society Index URL: https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG
9. EUROPEAN COMMISSION. (16 december 2020). The EU's Cybersecurity Strategy for the Digital Decade. Brussels. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=g
10. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391
11. JRC Cybersecurity Taxonomy URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC125533
12. Cybersecurity, our digital anchor URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC121051
13. COMPUTER SECURITY AND INCIDENT RESPONSE TEAM URL: https://csirt.csi.cip.gov.ua/uk/pages/about-csirt
14. EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564
15. EUROPEAN COURT OF AUDITORS. Challenges to effective EU cybersecurity policy. 2019 URL: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf
16. EUROPEAN COMMISSION. (07 February 2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN
17. EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (17 April 2019). REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019. on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN
18. EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (06 de july de 2016). DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
19. European Union Agency for Cybersecurity (ENISA). (2017). Incident notification for DSPs in the context of the NIS Directive. ENISA. URL: https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/at_download/fullReport
20. Cyberwatching Consortium. (2019) URL: https://cyberwatching.eu/sites/default/files/D3.4%20EU%20Cybersecurity%20legal%20and%20policy%20aspects_preliminary%20recommendations%20and%20road%20ahead_0.pdf.
21. EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (27 April 2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
22. Dominik Herrmann and Pridöhl Henning. Basic Concepts and Models of Cybersecurity. En M. C. Loi (Ed.), The Ethics of Cybersecurity, 2020 P. 11-44. doi:10.1007/978-3-030-29053-5_2
23. Wessel R. A Towards EU cybersecurity law: regulating a new policy field. En M. C. Loi (Ed.), The Ethics of Cybersecurity, 2015. P. 98. doi:10.1007/978-3-030-29053-5_2
24. European Union Agency for Cybersecurity (ENISA). (2019). Guidance and gaps analysis for European standardisation. URL: https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation/at_download/fullReport