Зінич Л.В.

ІНФОРМАЦІЙНА БЕЗПЕКА ЕСТОНІЇ: ДОСВІД ДЛЯ УКРАЇНИ

УДК: 659.4:327.88 https://doi.org/10.15330/apiclu.50.26-38

Постановка проблеми. Сучасні реалії розвитку інформаційних процесів у світі демонструють, що інформаційна безпека є такою ж важливою складовою національної безпеки як і економічна, військова чи політична. В умовах інтенсивного розширення інформаційного потоку, збільшення засобів інформаційного обміну, ведення інформаційних війн, інформаційна безпека стала найменш захищеним елементом національної безпеки. Вирішення цього питання залишається пріоритетним для всієї міжнародної спільноти. Серед країн Європейського Союзу однією із найбільш передових, яка проводить активну інформаційну політику є Естонська Республіка [1, с.441].

Україна і Естонія як пост-радянські країни підтримують двосторонні дружні відносини з моменту проголошення незалежності у 1991 році. Україна та Естонія мають схожі погляди на актуальні проблеми європейської та глобальної безпеки, спільні прагнення у політичній, економічній, соціальній та інших сферах [2]. Крім того досвід Естонії надзвичайно важливий для України ще й тому, що Естонія успішно протистоїть інформаційній агресії з боку Російської Федерації, однак за територією та кількістю людських і природних ресурсів є значною меншою. Між Україною та Естонією зроблено перші кроки для співпраці щодо взаємодії та обміном досвідом у сфері нейтралізації кібератак. ТакожЕстонська Республіка є членом Північноатлантичного альянсу (далі – НАТО) з 29 березня 2004 року, що є стратегічним курсом України. Протягом багатьох років Естонія перебуває на чолі кібербезпеки на міжнародному рівні. Центр розвитку кіберзахисту НАТО у справах кіберзахисту (CCD CoE) та Агентство ЄС для широкомасштабних ІТ-систем (EU-LISA) знаходяться в Таллінні. Ряд впливових міжнародних угод, які були затверджені тут, у Таллінні [3].

Попри те, що Естонія і Україна має спільні інформаційні загрози варто враховувати, що Естонія пройшла власний шлях до

формування інформаційної безпеки. А її багаторічний досвід демонструє, що захист інформаційного простору вимагає розроблення комплексної державної політики у цій сфері.Тому на нашу думку, необхідне вивчення ефективності діяльності державних органів, аналіз нормативно-правових актів та визначення можливості їх адаптації в Україні. Саме дослідженню цих особливостей інформаційної безпеки присвячена дана стаття.

Сучасний стан інформаційної безпеки України значною мірою не відповідає рівню безпеки інформаційно захищених країн, зокрема Естонії. Критичний стан кібербезпеки, нерозвинута система інформаційної інфраструктури, недосконалий захист персональних даних та ряд інших проблем зумовлюють детальний аналіз правових аспектів забезпечення інформаційної безпеки Естонії і аналіз можливості запозичення цього досвіду для України.

Стан дослідження. Проблематика інформаційної безпеки та її складові у зв'язку із сьогоднішніми викликами та необхідністю, досліджена недостатньо. Сучасний стан напрацювання цієї тематики свідчить, що серед науковців немає єдності думок щодо сутності інформаційної безпеки, підсилює це й те, що у міжнародних актах визначення також досить різноманітні. Підкреслимо, що стан інформаційної безпеки в будь-якій державі є досить нестабільним, адже залежить від багатьох чинників, до яких можна віднести суспільно-політичні події, економічний і соціальний стан суспільства, тому забезпечення інформаційної безпеки є постійним завданням.

Особливу увагу естонські вчені приділяють кібер безпеці, яка стала основним засобом ведення інформаційних війн. У Естонії діють потужні наукові школи з підготовки фахівців у сфері інформаційної безпеки, а численні науково-практичні проекти Естонії спільно із НАТО та Європейським Союзом дозволили розробити концепції протидії кібер атакам.

У сфері персональних даних науковцями напрацьовується бачення, що крім конфіденційності та захищеності є необхідність у створення ринку приватних даних, де компанії можуть надати пропозиції щодо оренди / ліцензування своїх даних для майбутніх фінансових, рекламних та інших послуг, що на сьогодні є достатньо перспективним.

Виклад основного матеріалу.

Законодавство і сучасні погляди на інформаційну безпеку в Естонії.

Інформаційна безпека поняття яке було ведено у науковий обіг вже досить давно проте особливої актуальності набуло із розвитком технологій.Поштовхом для активного впровадження технологій інформаційної безпеки стали кібератаки Російської Федерації на естонські інформаційні ресурси у 2007 році.Естонія як країна з розвинутим «e-sociеty» за декілька років сформувала модель електронного урядування менш уразливу до зовнішнього впливу.

Сьогодні у Естонії правове регулювання інформаційної безпеки здійснюється Конституцією Естонії, Законом «Про публічну інформацію», Законом «Про захист приватних даних», Законом «Про державну таємницю та засекречування зовнішньої інформації», Законом «Про кібербезпеку», Стратегією кібербезпеки на 2019-2022 рр.

Конституція Естонії у § 44передбачає право кожного на інформацію та гарантії захисту цього права [4].

Обмеження доступу до інформації, які встановлені Конституцією Естонії опосередковано спрямовані на забезпечення інформаційної безпеки, оскільки захист приватних даних і державної таємниці розглядаються як складові безпеки інформації.

Обґрунтовуючи обмеження доступу до інформації потрібно зазначити, що міжнародне право визнає, що держава може вилучати з категорії загального надбання певну обмежену інформацію, поширення якої могло б завдати шкоди інтересам, що їх держава може охороняти на законних підставах. До них належать, зокрема, інтереси національної безпеки, що вимагають зберігати певну інформацію «в таємниці» (тобто так, щоб вона була відома кільком представникам уряду або війська) протягом обмеженого часу. Утім, обмеження ці завжди мусять бути такими, без яких демократичне суспільство не обійдеться, і задовольняти критерій суспільного інтересу, а це означає, що вони завжди мають тимчасовий характер (тобто їх запроваджують лише на обмежений термін) і інформація зрештою стане доступною загалові [5,с.151].

У законі Естонії «Про публічну інформацію» не міститься поняття «інформаційна безпека» [6]. Стратегія захисту кібер-про-

стору в Республіці Естонія підкреслює необхідність створення безпечного кібер-простору в цілому і фокусується на інформаційних системах. В основу стратегії покладено заходи цивільного характеру, рекомендовано зосередити зусилля на регулюванні, освіті та співробітництві.

Варто відзначити, що як в українських так і естонських науковців сьогодні немає єдності думок щодо розумінняцього поняття. Виокремлюють декілька підходів до визначення сутності інформаційної безпеки, за якими під останнім розуміють: стан захищеності інформаційного простору; процес управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України; стан захищеності національних інтересів країни в інформаційному середовищі або в інформаційній сфері; захищеність установлених законом правил, за якими відбуваються інформаційні процеси в державі; суспільні відносини пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі; невід'ємну частину політичної, економічної, оборонної та інших складових національної безпеки [7, с.25-30].

Забезпечення інформаційної безпеки стало глобальним завданням, а тому є предметом правового регулювання не тільки у законодавствах окремих держав, а й у міжнародному законодавстві. Щодо міжнародних актів, то враховуючи те, що Естонія є членом НАТО у актах цієї організаціїзастосовується термін «класифікована інформація» під яким розуміють інформацію, чутливу до загроз що виникають у зв'язку із несанкціонованим доступом до неї, а тому потребує захисту або принаймні обмеження доступу до неї [8].

Важливим у контексті інформаційної безпеки держави є розуміння сутності міжнародної інформаційної безпеки. Сьогодні під міжнародною інформаційною безпекою розуміють стан, що забезпечується загальновизнаними і спеціальними принципами та нормами міжнародного права, який включає порушення міжнародного миру і безпеки як окремих держав, так і світового співтовариства в цілому у сфері інформації і комунікації [9, с.30-31].

У законодавствах інших держав часто використовуються два терміни «Безпека інформації» та «інформаційна безпека». Дослідники в сфері інформаційної безпеки розмежовують інформаційну

безпеку та безпеку інформації наступним чином, інформаційна безпека є значно глибшим за сутністю і ширше за змістом. Інформаційну безпеку можна розглядати з позиції захисту не тільки інтересів держави, а й насамперед особистості і суспільства [10, с.56].

Відтак проаналізувавши законодавство та наукові погляди щодо інформаційної безпеки вважаємо, що інформаційна безпека – це стан захищеності інформації в системах і додатках при якому зберігається цілісність та конфіденційність даних, стійкість до зовнішнього впливу.

Безпека інформаційного середовища як базовий принцип діяльності державних структур Естонської Республіки

Забезпечення інформаційної безпеки основне завдання спеціалізованих державних утворень. Основним органом забезпечення інформаційної безпеки є Міністерство у справах економіки та комунікацій Естонської Республіки та Міністерство внутрішніх справ Естонії, які спільно з Лігою оборони кібербезпеки, Міжнародним центром оборонних досліджень, органом Естонської інформаційної системи забезпечують кібербезпеку Естонії.

Серед недержавних організацій особливе місце займає Естонська асоціація інформаційних технологій та телекомунікацій [11].

В Естонії нагляд за виконанням закону «Про публічну інформацію» був покладений на Інспекцію з захисту даних при Міністерстві юстиції Естонії. Правовий статус останньої визначається законом «Про захист персональних даних» та «Публічну інформацію». Більше уваги Інспекція приділяє саме захисту персональних даних, аніж захисту права на доступ до публічної інформації.

До компетенції Інспекції входить: 1) здійснення державного нагляду за розпорядниками інформації з питань виконання ними інформаційних запитів і оприлюднення інформації; 2) порушення наглядового провадження на підставі звернення або з власної ініціативи.

Естонські громадяни підтверджують ефективність діяльності Інспекції, у зв'язку з можливістю оперативно додавати, змінювати чи видаляти персональні дані про фізичну особу, які та бажає розповсюджувати.

Особливе місце у забезпеченні інформаційної безпеки належить Центру реагування на комп'ютерні інциденти (далі - CERT). CERTЕстонія було створено у 2006 році як спеціалізована організація, яка реагує на комп'ютерні інциденти, допомагає користувачам у зменшенні негативних наслідків та вживає безпекові заходи при їх загрозі.

Особливістю роботи CERT є те, що ця організація не працює з користувачами. У разі настання інциденту користувач повинен звернутися до провайдера надання послуг, мережевого адміністратора або служби підтримки споживачів.

Завданнями CERTє: a) виявлення найменш захищених елементів у системах і додатках; b) надання допомоги у разі настання інциденту; c) координація дій та реагування на інцидент.

Результатом роботи CERT-EE стало виявлення у 2018 році загрози збору і відправлення на сервери Російської Федерації персональних даних громадян Естонії при користуванні додатком Yandex Taxi. Як відомо в Росії не діють вимоги Європейського Союзу щодо персональних даних, а це надає можливість використовувати ці дані спецслужбами [12].

Розглядаючи різні моделі управління інформаційною сферою, вартим уваги є досвід країн, де запроваджено посаду Уповноваженого або Комісара з питань інформації.Для прикладу у Канадідіє Комісар з питань інформації Канади, який здійснює контроль за реалізацією закону «Про доступ до інформації». У цілому запроваджена в Канаді модель Комісара з питань інформації вважається досить дієвим інструментом у механізмі захисту права на доступ до інформації. Це виявляється як в ефективності розгляду справ інформаційним уповноваженим, так і в розробці його рекомендацій для державних установ, а також рекомендацій щодо необхідності подальшого реформування інформаційного законодавства [5, с.213-214].

З цього приводу науковцями України відзначається, що запровадження інституту Комісара (Уповноваженого) є дуже складними і маловірогідним, оскільки Конституція не передбачає можливості створення спеціалізованих омбудсменів. Тому, щоб створити цей інститут потрібно внести зміни до Конституції України. Сьогодні Інститут Інформаційного уповноваженого знаходиться лише на етапі свого становлення, тому вбачається за до-

цільне запровадити посаду представника Уповноваженого з прав людини, який буде займатися охороною та захистом інформаційних прав [13, с.181-182].

Ефективність діяльності спеціальних органів контролю за дотриманням права на доступ до публічної інформації в межах виконавчої влади оцінюється фахівцями по-різному. Дискусії ведуться щодо їх реальної незалежності у здійсненні діяльності та ухваленні рішень.Сформована у Естонії модель інформаційної безпеки перевірена критичними ситуаціями показала свою дієвість та ефективність, актуальним є той аспект, що всі державні органи та приватні структури взаємодіють між собою для запобігання та подолання негативних наслідків.

Стан Кібербезпеки в Естонії

За останніми даними «Національного індексу кібербезпеки Європи» поданими Естонською академією електронного управління, Естонія посідає перше місце у Європі в можливостях аналізу та інформації про кіберзагрози, внеску в глобальну кібербезпеку, захист цифрових послуг, захист персональних даних, повідомлення про кібер-інциденти, управління кібер-кризою та військові кібер-операції», - зазначила команда індексу на своєму веб-сайті [14].

Відповідно до стратегії кібербезпеки Європейського Союзу, кібербезпека – це гарантії та дії, що використовуються для захисту кіберпростору як з цивільної, так і з військової точок зору від загроз, що пов'язані із шкідливим впливом чи можуть нанести шкоду його взаємозалежним мережам та інформаційній інфраструктурі. Кібербезпека покликана зберігати цілісність і доступність мереж та інфраструктури, а також конфіденційність інформації, що там містить з метою забезпечення її доступності, цілісності, автентичності, конфіденційності і непідробленості [15, с.58].

У Естонії діє Закон «Про кібербезпеку» (1) Цей Закон передбачає вимоги до обслуговування мереж та інформаційних систем, необхідних для функціонування суспільства та мережевих та інформаційних систем органів державної влади та місцевої влади, відповідальності та нагляду, а також підстав для запобігання та вирішення кіберзахисту. інциденти [16].

Естонія здійснює заходи для підвищення кібер безпеки за такими напрямками як: боротьба із кібер злочинами, розвитком

критичної інфраструктури та електронних послуг та підвищенням рівня національної безпеки.

Загальносвітовою тенденцією є на сьогодні створення у державах підрозділів кібер поліції та Центрів реагування на комп'ютерні інциденти, основним завданням яких є боротьба із кібер злочинами. Вважаємо, що для реалізації заходів із підвищення кібер безпеки необхідно посилити відповідальності як адміністративну так і кримінальну за інформаційні правопорушення.

Поряд із детальним правовим регулюванням важливу роль відіграють створені спільні із НАТО та Європейським Союзом організації координації зусиль, до яких відноситься Центр передового досвіду спільної кібер безпеки НАТО, Європейське агентство по оперативному управлінню великими ІТ системами та інші для запобігання кібер атакам в Естонії. Естонськими фахівцями також здійснюється тестування уразливості на кібер атаки та моделювання процесу злому, а також розробку досконаліших програмно-апартних засобів виявлення кібер атак.

Правова політика Естонії щодо захисту персональних даних

Беззаперечним є успіх Естонії у захисті персональних даних, свідченням цього є розробка концепції відкриття перших у світі Посольств даних у іноземних країнах. Захист персональних даних здійснюється за допомогою Закону Естонської Республіки «Про захист персональних даних» [17], Регламент (ЄС) 2016/679 Європейського Парламенту та Ради, Директива 95/46 / ЄС (Загальний регламент про захист даних) (ОВЛ 119, 04.05.2016, с. 1-88).

Органом до компетенції якого входить захист даних у Естонії є Естонська інспекція захисту даних. В законодавстві детально регламентовано повноваження, права та обов'язки контролера. Важливим є те, що власник персональних даних має правові можливості запобіганню поширенню, перекручуванню інформації про свої персональні дані і це не в останню чергу забезпечується чіткими правами і обов'язками контролера персональних даних. Також у особливих випадках правоохоронні органи мають право призначати спеціаліста із захисту даних на підставі договору про надання послуг, для охорони важливої інформації.

У науковій літературі Jaan Priisalu, Rain Ottis обґрунтовують необхідність створення ринку приватних даних у Естонії. Одне можливе рішення організаційного посередництва фірмового ринку, де компанії та дослідники пропонують представити дату використання та ліцензування / оренду / продаж, пов'язані з пропозиціями, присвоєння моделей цін, де пацієнт може вибирати або ліцензію, оренду, продаж, або вилучення своїх даних із використання [1, с.450]. Вважаємо, що дана пропозиція є перспективною та в майбутньому отримає своє втілення як в Естонії так і в інших країнах Європи.

Уроки для України. Проаналізувавши досвід Естонської Республіки у забезпеченні інформаційної безпеки можна виділити декілька факторів, що стали основою для формування безпечного інформаційного середовища.

По-перше, тільки всеохоплююча інформаційна політика дає змогу забезпечити належний рівень безпеки підприємств, установ, організацій та держави в цілому.При цьому розвинена система «e-society» в Естонії зумовила необхідність участі практично всіх державних органів у забезпеченні інформаційної безпеки через дотримання технічних, правових та організаційних вимог. У рамках інформаційної політики вагому роль відіграє налагоджена широкомасштабна взаємодія держави із приватними структурами, що сприяло залученню новітніх технологій захисту інформації. У підсумкузабезпечення інформаційної безпеки стало справою всього естонського суспільства.

По-друге, Естонія спрямувавши всі зусилля на забезпечення кібер безпеки (як складової інформаційної безпеки), створила сприятливі умови для приходу іноземних IT компаній із значними капіталами та інноваціями. Як наслідок держава отримала нові економічні, технологічні надходження. Надійність кібер безпеки Естонії обумовлена ефективними системами криптографічних та програмно-апаратних засобів.Для підвищення безпеки і запобіганню виникненню кібер атак у Естонії фахівцями застосовується технологія тестування уразливості на кібер атаки та моделювання процесу злому а також створюються безпечні програмні середовища для обміну інформацією.

По-третє, у контексті інформаційної безпеки значна увага в Естонії приділяється охороні та використанню персональних

даних, яке здійснюється максимально прозоро, з використанням цифрового підпису і шифрованих повідомлень. Особа має право в будь-який момент виправити або видалити персональні дані шляхом звернення до Інспекції захисту даних.Естонія йде шляхом створення ринкової моделі приватних даних,за якої власникам персональних даних надається можливість ліцензувати/ орендувати дані.

Саме розвинена інформаційна інфраструктура, детальна Стратегія кібер безпеки, яка приймається на кожних 4 роки, надійна система захисту персональних даних дала можливість Естонії стати передовою інформаційно захищеною країною. Виділений досвід Естонії є корисним для України при подоланні кризових явищ в інформаційній сфері та прийнятті нормативно-правових актів.

Висновки і рекомендації. Підсумовуючи проведене дослідження можемо стверджувати, що досвід Естонії свідчить - розвинена система інформаційної безпеки сприяє добробуту та благополуччю суспільства і підвищує рівень довіри до державних інституцій.

Вважаємо, що підвищити рівень інформаційної безпеки допоможуть ряд таких заходів:

1) Створити робочу групу із залученням міжнародних експертів з напрацювання концепції інформаційної безпеки і нормативно-правове забезпечення її діяльності

2) У концепції інформаційної безпеки передбачити створення єдиного національного електронного інформаційного ресурсу.

3) Впровадити єдиний національний ідентифікатор фізичної особи.

4) Створити єдиний захищений веб-портал електронних послуг з можливістю створення електронних кабінетів фізичних осіб для отримання адміністративних послуг.

1. Jaan Priisalu, Rain Ottis Personal control of privacy and data: Estonian experience. HealthTechnol. (2017) 7:441–451

2. Embassy of Ukraine in the Republic of Estonia. URL: https://estonia.mfa.gov.ua/en/ukraine-ee/diplomacy

3. Cyber Security. Ministry of Foreign Affairs Republic of Estonia. URL:https://vm.ee/en/cyber-security

4. *The Constitution of the Republic of Estonia. Passed 28.06.1992RT 1992, 26, 349Entry into force 03.07.1992. URL: https://www.riigiteataja.ee/en/eli/530102013003/consolide*
5. *Інформація в Україні: право на доступ. Нестеренко О. «Акта», 2012. с.151*
6. *Public Information Act. Passed 15.11.2000. RT I 2000, 92, 597. Entry into force 01.01.2001. URL:https://www.riigiteataja.ee/en/eli/514112013001/consolide*
7. *Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: [навчальний посібник]. К.: КНТ, 2006. 280 с.*
8. *Document C-V(2002)49: SecuritywithintneNorthAtlanticTreatyOrganization (NATO). URL: www.statewatch.org/ news/2006/sep/nato-secclassifications.pdf*
9. *Грицун О.О. Міжнародно-правове забезпечення міжнародної інформаційної безпеки. Дис. на здоб. наук. ступеня к.ю.н., спец. 12.00.11. КНУ імені Тараса Шевченка. Київ, 2016. 233 с.*
10. *Волошина Н.М. Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. Сучасні інформаційні технології у сфері безпеки та оборони. №2(8)/2010. С.53-56.*
11. *ITL Estonia. URL:https://www.itl.ee/index.php?page=181*
12. *Yandex Taxi to introduce app-based ride ordering service in Tallinnhttps://news.err.ee/827618/yandex-taxi-to-introduce-app-based-ride-ordering-service-in-tallinn*
13. *Збирак Т.В. Проблеми адміністративно-правового забезпечення права на свободу слова в Україні та шляхи їх вирішення. Актуальні проблеми вдосконалення чинного законодавства України. Збірник наукових статей. Випуск 48. – Івано-Франківськ: Прикарпатський національний університет імені Василя Стефаника, 2018. С.178-190.*
14. *Estonia ranks first in the world in the national cyber security index. URL: https://estonianworld.com/security/estonia-ranks-first-in-the-world-in-the-national-cyber-security-index/*
15. *DOD Dictionary of Military and Associated Terms [Electronicresource]. – USA : Department of Defense, 2017. – 388 p. – URL : http://www.dtic.mil/ doctrine/new_pubs/jp1_02.pdf.*
16. *Cybersecurity Act. Riigi Teataga. URL: https://www.riigiteataja.ee/en/eli/523052018003/consolide*
17. *PersonalDataProtectionAct. Passed 12.12.2018. URL: https://www.riigiteataja.ee/en/eli/523012019001/consolide*

Зінич Л.В. Інформаційна безпека Естонії: досвід для України

У статті розглянуто особливості забезпечення інформаційної безпеки у Республіці Естонія. Відзначається, що основними чинниками, які дозволили підвищити рівень інформаційної безпеки в Естонії є розвинена інформаційна інфраструктура, ефективна політика у сфері кібер безпеки та надійний захист персональних даних. Встановлено, що кібер безпека залежить від боротьби із кібер злочинністю, покращення критичної інфраструктури і електронних послуг та забезпеченням національної оборони. Надано практичні рекомендації щодо запозичення Україною досвіду Естонії у сфері інформаційної безпеки.

Ключові слова: інформаційна безпека, кібер-безпека, інформаційна інфраструктура, персональні дані.

Зиныч Л.В. Информационная безопасность Эстонии: опыт для Украины

В статье рассмотрены особенности обеспечения информационной безопасности в Республике Эстония. Отмечается, что основными факторами, которые позволили повысить уровень информационной безопасности в Эстонии существует развитая информационная инфраструктура, эффективная политика в сфере кибербезопасности и надежную защиту персональных данных. Установлено, что кибер безопасность зависит от борьбы с кибер преступностью, улучшение критической инфраструктуры и электронных услуг и обеспечением национальной обороны. Даны практические рекомендации по заимствования Украины опыта Эстонии в сфере информационной безопасности.

Ключевые слова: информационная безопасность, кибер-безопасность, информационная инфраструктура, персональные данные.

Zinich LV Information security of Estonia: experience for Ukraine

The article deals with features of information security in the Republic of Estonia. It is noted that the main factors that have helped to increase the level of information security in Estonia are the developed information infrastructure, effective cybersecurity policy and reliable protection of personal data. Cybersecurity depends on a combination of cybercrime, provision of critical infrastructure and e-services, and national defense.

In the area of personal data protection, it is reasonable to create a private data market where companies and researchers propose to submit a date of use and license / lease / sale related to offers or license, lease, sell or withdraw their data from use.

Analyzing the experience of the Republic of Estonia in information security, there are several factors that have become the basis for the creation of a secure information environment. First, only a comprehensive information policy enables the security of enterprises, institutions, organizations and the state as a whole.

Secondly, Estonia has made every effort to ensure cybersecurity (as a component of information security) and has created favorable conditions for the arrival of foreign IT companies with significant capital and innovation.

Third, in the context of information security, considerable attention in Estonia is given to the protection and use of personal data, which is carried out as transparently as possible, using digital signatures and encrypted messages.

Practical recommendations for Ukraine's acquisition of Estonia's information security experience are provided. We believe that raising the level of information security will help a number of the following activities: 1) Create a working group with the involvement of international experts to develop the concept of information security and regulatory support for its activities 2) Ensure the creation of a single national electronic information resource in the concept of information security. 3) Enter a unique national ID for the individual. 4) Create a single secure web portal for electronic services with the possibility of creating electronic offices of individuals for receiving administrative services. Keywords: information security, cybersecurity, information infrastructure, personal data.

Keywords: information security, cyber security, information infrastructure, personal data.

Козич І.В.

МІСЦЕ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ В ПОЛІТИКО-ПРАВОВІЙ СИСТЕМІ

УДК 343.2.01 https://doi.org/10.15330/apiclu.50.38-48

Актуальність теми. Загальновідомою, хоча і сумною істиною є той факт, що як політологи, так і юристи часом схильні забувати, що право і політика — як в теоретичному, так і в практичному плані — тісно пов'язані між собою. Ще у 1882 р. англійський юрист Ф. Поллок писав про те, що «право для політичних інститутів означає те ж, що хребет для тіла» [1, с. 20]. Однак лише останнім часом у вітчизняній юридичній науці почали гостро підніматись питання про державну політику, а особливо про політику в сфері протидії злочинності.

Стан дослідження. З моменту прийняття Кримінального кодексу України до проблем політики в сфері протидії злочинності та кримінально-правової політики в широкому розумінні на дисертаційному та монографічному рівні звертались лише П. Л. Фріс [2] та А. А. Митрофанов [2]. Окремим аспектам кримінально-правової політики присвячені дослідження В.І.Борисова, Ю.А.Поно-