ПРЯМУЄМО РАЗОМ

ВЕРХОВНА РАДА УКРАЇНИ

UNDP

Проєкт ЄС-ПРООН з парламентської реформи

Комітет з питань цифрової трансформації

КРАЩІ ПРАКТИКИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

Оглядовий звіт

Публікація підготовлена Офісом парламентської реформи в рамках проєкту ЄС-ПРООН з парламентської реформи. Зміст публікації є виключно відповідальністю автора і необов'язково відображає позицію Європейського Союзу або Програми розвитку ООН.

Авторка – **Лілія Олексюк**, кандидат наук з державного управління, юрист, позаштатний консультант Комітету Верховної Ради України з питань цифрової трансформації.

ЗМІСТ

СКОРОЧЕННЯ

GCI	Глобальний індекс кібербезпеки
DDOS	Distributed Denial-of-service attack, атака на відмову в обслуговуванні
IBM	International Business Machines Corporation
CERT	Computer Emergency Response Team
CERT-IL	Israel National Cyber Event Readiness Team
CSIRT	Computer security incident response team
GDP	Gross Domestic Product
GSS	General Security Service
ICT	Information and Communications Technology
IDF	Israel Defense Forces
IIX	Israel Internet eXchange
INCB	Israeli National Cyber Bureau
ISP	Internet Service Provider
ITU	International Telecommunication Union
NCSA	National Cyber Security Authority
NIS	Israeli New Sheqel

NISA	National Information Security Agency
OECD	Organisation for Economic Co-operation and Development
R&D	Research and Development
UK	United Kingdom (of Great Britain and Northern Ireland)
UN	United Nations
US	United States (of America)
USD	US Dollar
NCSI	Національний індекс кібербезпеки
ЄС	Європейський Союз
ЄК	Європейська Комісія
МСЕ	Міжнародний союз електрозв'язку
МЗІ	Міністерство зв'язку та інформатики

ВСТУП

Національний індекс кібербезпеки (NCSI)[1] — це глобальний індекс, який вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами. NCSI — це також база даних із загальнодоступними матеріалами та інструментарієм для розбудови потенціалу національної кібербезпеки. За даними 2019 року, країни, представлені в огляді, посідають такі місця за індексом NCSI: Естонія — 3 місце, Литва — 4 місце, Іспанія — 5 місце, Нідерланди — 10 місце, Сполучені Штати Америки — 14 місце, Велика Британія — 15 місце (тобто всі країни входять до першої тридцятки). Україна наразі посідає за рейтингом NCSI 28 місце.

NCSI розроблений і реалізується Фондом академії електронного врядування Естонії, натомість Глобальний індекс кібербезпеки (GCI)[2] укладає Міжнародний союз електрозв'язку (МСЕ), він є ініціативою для заінтересованих сторін, спрямованою на підвищення обізнаності щодо кібербезпеки та вимірювання прихильності країн до кібербезпеки та її широкого застосування в різних галузях і секторах. Рівень розвитку кожної країни аналізується за п'ятьма категоріями: правові заходи, технічні заходи, організаційні заходи, розбудова потенціалу та співробітництво.

Відповідно до останнього GCI 2018 року, однакові бали за всіма п'ятьма категоріями набрали три країни: Велика Британія, Франція та Литва. За правовими та організаційними показниками всі набирають максимальний бал (0.200). Усі країни показують найнижчі (але все одно доволі високі) бали в категорії співробітництва, при цьому високі, але не максимальні бали — в категоріях технічних заходів та розбудови потенціалу.

Велика Британія посідає перше місце з найвищими балами у двох категоріях — правові та організаційні заходи.

1 https://ncsi.ega.ee/ncsi-index/

2 https://www.itu.int/pub/D-STR-GCI.01-2018

Велика Британія має низку правових інструментів, що дають змогу боротися з кіберзлочинністю, зокрема Закон про зловживання комп'ютером[3].

Національне агентство з питань злочинності успішно провело міжнародну операцію із закриття вебсайту, пов'язаного з 4 млн DDOS-атак у всьому світі.

Франція вдруге посіла друге місце в Європі, при цьому набрала 100 відсотків за категоріями правових та організаційних заходів. Франція активно співпрацює з інституційними партнерами (міністерствами, національними органами влади, приватним сектором та неприбутковими організаціями), а під час Європейського місяця кібербезпеки використовує різні засоби для підвищення в суспільстві обізнаності з цих питань.

Литва має найвищий бал як у правовій, так і в організаційній категорії. Закон Литви про кібербезпеку містить положення, що дозволяють компетентним органам вживати заходів проти загальнодоступної інфраструктури електронного зв'язку, яка бере участь у шкідливій онлайн-діяльності (наприклад, у ботнеті). Державна інспекція захисту даних може публікувати інформацію про випадки, пов'язані з порушеннями персональних даних.

Високі бали також набрали США (2 місце), Литва (4 місце), Естонія (5 місце), Іспанія (7 місце) Нідерланди (12 місце), Ізраїль (39 місце). Для порівняння, Україна посіла у рейтингу GCI 2018 року 54 місце.

Саме ці сім провідних країн були обрані для огляду організаційних заходів, а також аналізу управління колективною кібербезпекою в ЄС.

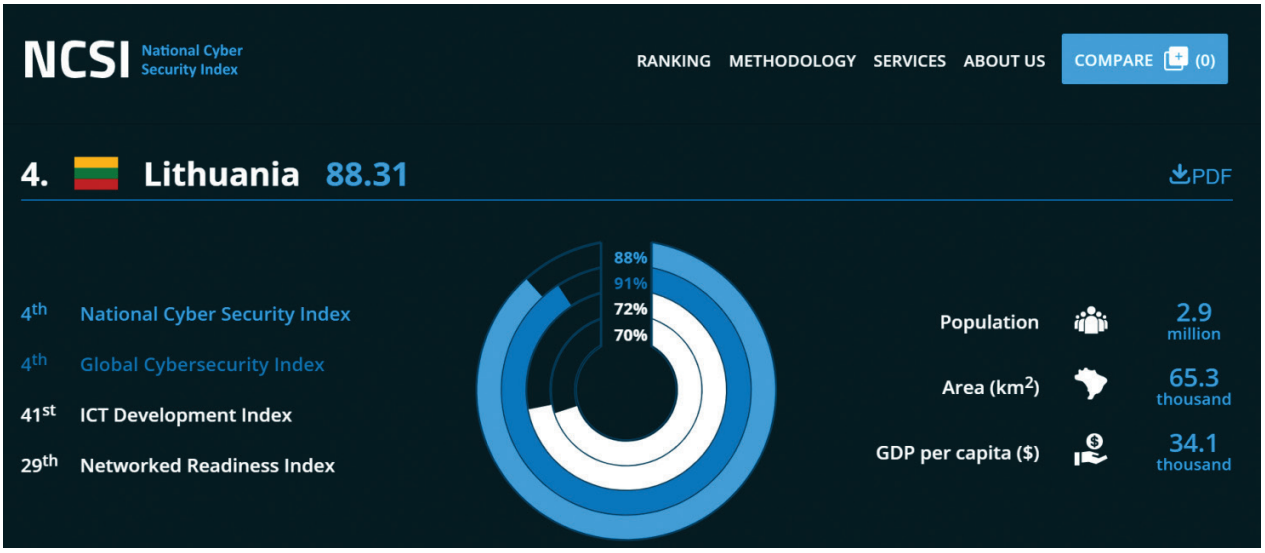
У дослідженні розглянуті законодавчі акти досліджуваних країн та інформація з офіційних сайтів органів, відповідальних за забезпечення кібербезпеки.

Документ містить аналіз кращих практик управління кібербезпекою в країнах, що входять до десятки найуспішніших у сфері кібербезпеки і кіберзахисту в світі. Звіт складається з таких структурних компонентів: показники Національного індексу кібербезпеки (NCSI); огляд законодавчого забезпечення кібербезпеки, організаційна та інституційна складова, координація політики кібербезпеки, військова кібербезпека, запобігання критичним загрозам та кризам, державно-приватне партнерство та огляд суб'єктів, викликів і загроз у рамках національних стратегій.

Документи Стратегій англійською мовою для аналізу було взято з сайту ENISA за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

3 http://www.legislation.gov.uk/ukpga/1990/18/contents

ЛИТВА



Литва розбудовує свої інститути в галузі кібербезпеки та управління на основі багаторічної традиції роботи в галузі інформаційних технологій та телекомунікацій, започаткованої ще в минулому столітті. Литва створила індустрію, яка охопила розробку та виготовлення обладнання й програмного забезпечення для різних сфер — радіо, звукозапис, вимірювальні прилади тощо. Для її підтримки було започатковано успішне партнерство між урядом, галуззю та навчальними закладами.

Наприкінці 1980-х виробнича група Sigma складалася з семи заводів, на яких працювали понад 18000 людей у виробництві та менеджменті, а 2000 — у науково-дослідній царині. Було налагоджено виробництво комп'ютерів — від клонованих версій мейнфреймів DEC VAX 730 до першого персонального клону комп'ютерів IBM. Однак ця унікальна промислова база IT невдовзі після відновлення незалежності Литви у 1990 році занепала.

Новий незалежний уряд Литовської Республіки незабаром здійснив перші кроки до формування інформаційного суспільства, створивши Міністерство зв'язку та інформатики (MCI). У 1993 році уряд затвердив Державну програму розвитку комунікацій та інформатики MCI для модернізації комунікацій та інфраструктури. Так було започатковано розробку відповідних правових актів і стандартів, необхідних для створення основних елементів інформаційної інфраструктури.

Прагнучи досягнути національних цілей у галузі кібербезпеки, Литва застосовувала різні підходи. Подальші зусилля були спрямовані на створення інститутів кібербезпеки без закону, який чітко визначає обов'язки та сферу діяльності організацій кібербезпеки.

Згодом, у 1996 році, було ухвалено Закон про основи національної безпеки. У документі перераховано сектори національної економіки, які мають значення для національної безпеки, — це енергетика, транспорт, інформаційні технології та телекомунікації, інші високотехнологічні сектори, фінанси та кредитування.

Надалі у 1999 році було створено Державну інспекцію захисту даних, у 2006 році уряд уповноважив Національний орган регулювання зв'язку створити Національну команду реагування на комп'ютерні надзвичайні ситуації (CERT-LT), а також 29 червня 2011 року затвердив Постанову №766 «Про затвердження Програми розвитку електронної інформаційної безпеки (кібербезпеки) на 2011–2019 рр.»[4].

Програма забезпечення інформаційної безпеки (кібербезпеки) Литви має три основні цілі: (1) забезпечити безпеку державних інформаційних ресурсів; (2) забезпечити ефективне функціонування критичної інформаційної інфраструктури; (3) забезпечити кібербезпеку мешканців Литви та осіб, які перебувають у Литві. Згодом ці цілі були зазначені та доопрацьовані у Законі про кібербезпеку, ухваленому 2014 року.

2008 року Указом Прем'єр-міністра Литовської Республіки №225 було створено міжвідомчу робочу групу з питань кібербезпеки під головуванням Міністерства національної оборони, яка мала здійснити аналіз та надати рекомендації щодо напрямків та заходів зміцнення кібербезпеки.

Однією з рекомендацій група визначила підготовку Національної стратегії кібербезпеки.

Сейм (Парламент) Литви згодом затвердив Стратегію національної безпеки, яка оголосила кібербезпеку одним із пріоритетних національних інтересів. Серед загроз національній безпеці зазначені кібератаки, які загрожують інформаційно-комунікаційним системам, що використовуються в економічному секторі, функціонуванню життєво важливих державних установ, безпеці секретної інформації, та інші дії, що загрожують життєво важливим функціям держави та добробуту громадян.

4 https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.403385

Організаційна структура системи кібербезпеки Литви визначена Законом про кібербезпеку, що набрав чинності 11 грудня 2014 року (останні зміни внесено 27 червня 2018 року, №XIII-1299) (далі — Закон)[5].

Відповідно до Закону, стратегічні цілі та пріоритети політики кібербезпеки, а також заходи, необхідні для їх досягнення, визначаються урядом Литовської Республіки.

ОРГАНИ, ЩО КОНТРОЛЮЮТЬ ПОЛІТИКУ КІБЕРБЕЗПЕКИ

Розробку політики кібербезпеки, її реалізацію організовує, контролює та координує Міністерство національної оборони Литовської Республіки. Національний центр кібербезпеки бере участь у розробці політики кібербезпеки тією мірою, якою має бути встановлено правове регулювання діяльності суб'єктів кібербезпеки для виконання функцій, передбачених цим законом.

Політика кібербезпеки реалізується Національним центром кібербезпеки, Державною інспекцією захисту даних, Литовською поліцією та іншими органами влади, функції яких пов'язані з кібербезпекою.

Уряд Литви має такі повноваження:

- затверджує Національну стратегію кібербезпеки;
- затверджує інституційний склад Ради з питань кібербезпеки;
- затверджує методику ідентифікації критичної інформаційної інфраструктури та перелік критичної інформаційної інфраструктури і її керівників;
- затверджує організаційні та технічні вимоги до кібербезпеки, що висуваються до суб'єктів кібербезпеки;
- затверджує Національний план управління кібербезпекою;
- здійснює контроль за управлінням кризами кібербезпеки.

Міністерство національної оборони координує підготовку Національної стратегії кібербезпеки та подає її на затвердження уряду; подає на затвердження уряду організаційні та технічні вимоги до кібербезпеки, що висуваються до суб'єктів кібербезпеки; подає на затвердження уряду Національний план управління кіберінцидентами; подає на затвердження уряду методику ідентифікації критичної інформаційної інфраструктури; подає на затвердження уряду перелік критичної інформаційної інфраструктури та її керівників; затверджує типовий план управління кіберінцидентами в критичних інформаційних інфраструктурах; затверджує план кіберзахисту для критичних інформаційних інфраструктур; встановлює порядок реагування національних центрів кібербезпеки на кіберінциденти, що трапляються в системах зв'язку та інформації суб'єктів кібербезпеки; затверджує план імплементації заходів технічної кібер-

5 https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee?positionInSearchResults=2&searchModelUUID=b372d7f3-b750-486c-900b-7329b9ad349f

безпеки, встановлює порядок їх впровадження та управління інформаційними ресурсами й критичною інформаційною інфраструктурою; бере участь у управлінні безпекою в кризових ситуаціях; створює інформаційну мережу кібербезпеки та затверджує її положення; затверджує положення Ради з питань кібербезпеки та її склад.

Міністерство національної оборони несе відповідальність за формулювання та координування реалізації політики кібербезпеки в Литві. Ця нова функція покладена на новостворений відділ з питань кібербезпеки та інформаційних технологій.

Також Законом передбачено створення Ради з питань кібербезпеки.

Рада з питань кібербезпеки є постійним колегіальним незалежним дорадчим органом, який аналізує ситуацію із забезпеченням кібербезпеки в Литовській Республіці та вносить пропозиції до установ, які розробляють і впроваджують політику кібербезпеки, суб'єктів кібербезпеки, науково-дослідних і освітніх установ та суб'єктів господарювання, які беруть участь у діяльності в галузі інформаційних технологій (далі — «Актори кібербезпеки»), щодо покращення ситуації із забезпеченням кібербезпеки.

Раду з кібербезпеки очолює представник Міністерства національної оборони. Забезпечення Ради кібербезпеки покладене на Міністерство національної оборони або уповноважену ним установу.

Основними завданнями Ради з питань кібербезпеки є: подання суб'єктам кібербезпеки пропозицій щодо пріоритетів кібербезпеки, напрямів розвитку, цільових результатів та способів досягнення цілей; подання суб'єктам кібербезпеки пропозицій щодо можливостей співпраці між державним сектором, бізнесом та дослідженнями у сфері забезпечення кібербезпеки; аналіз тенденції вдосконалення забезпечення кібербезпеки, надання акторам кібербезпеки висновків та пропозицій щодо управління кіберінцидентами ; надання суб'єктам кібербезпеки рекомендацій щодо підвищення кібербезпеки.

Найбільше завдань із реалізації політики кібербезпеки Закон покладає на Національний центр кібербезпеки. Ця підпорядкована Міністерству національної оборони установа:

- здійснює нагляд за дотриманням суб'єктами кібербезпеки та керованими ними системами зв'язку та інформації інформаційних, організаційних і технічних вимог щодо кібербезпеки, які висуваються до суб'єктів кібербезпеки, а також здійснює опитування щодо ситуації з кібербезпекою;
- наказує суб'єктам кібербезпеки надавати інформацію, необхідну для відповідності суб'єктів кібербезпеки й керованих ними комунікаційних та інформаційних систем організаційним і технічним вимогам кібербезпеки, що висуваються до суб'єктів кібербезпеки, та здійснювати оцінку ситуації з кібербезпекою;
- застосовує технічні заходи для вимірювання опірності державних інформаційних ресурсів та критичних інформаційних інфраструктур кіберінцидентам;

- видає накази щодо забезпечення кібербезпеки та усунення виявлених дефектів кібербезпеки, встановлює граничний строк виконання замовлень суб'єктами, які контролюють інформаційні ресурси держави, керівниками критичної інформаційної інфраструктури, провайдерами мережі загальнодоступних комунікацій та / або загальнодоступних електронних послуг зв'язку та постачальниками послуг з розміщення цифрової інформації;
- дає вказівки суб'єктам кібербезпеки, за винятком постачальників цифрових послуг, проводити незалежні аудити комунікаційних та інформаційних систем чи послуг, що надаються за допомогою таких систем, за власний рахунок та надавати результати таких аудитів, якщо вони не надають технічну інформацію, необхідну для оцінки ситуації з кібербезпекою щодо комунікаційних та інформаційних систем або послуг, які надаються з використанням таких систем та викладені в описі організації та технічних вимог щодо кібербезпеки, що висуваються до суб'єктів кібербезпеки;
- після отримання доказів від суб'єкта кібербезпеки, користувача цифрової послуги або будь-якої іншої держави — члена ЄС, в якій надаються цифрові послуги, від компетентного органу, який здійснює нагляд за діяльністю постачальників цифрових послуг у сфері кібербезпеки, який заявляє, що провайдери цифрових послуг не відповідають вимогам, встановленим цим законом, дає вказівки постачальникам цифрових послуг надавати інформацію, необхідну для оцінки кібербезпеки керованих ними комунікаційних та інформаційних систем та усунення недоліків у дотриманні вимог щодо кібербезпеки;
- здійснює моніторинг кіберінцидентів на національному рівні та їх аналіз;
- відповідно до плану заходів з кібербезпеки, погоджених із суб'єктами, які здійснюють контроль та / або управління державними ресурсами, або з керівниками критично важливої інформаційної інфраструктури, у порядку, встановленому Міністром національної оборони, здійснює та контролює технічні заходи кібербезпеки в державних інформаційних ресурсах та критичній інформаційній інфраструктурі. Заходи, що здійснюються за рахунок коштів Національного центру кібербезпеки, мають використовуватися виключно для забезпечення кібербезпеки. Технічні засоби, що використовуються за рахунок коштів Національного центру кібербезпеки, мають підтримуватися, а їх ремонт має здійснюватися за кошти Національного центру кібербезпеки;
- здійснює організаційне управління кіберінцидентами в комунікаційних та інформаційних системах суб'єктів кібербезпеки на національному рівні;
- застосовує заходи кібербезпеки у випадку кіберінциденту;
- припиняє розповсюдження наслідків кіберінцидентів на кібербезпеку державних інформаційних ресурсів або критичної інформаційної інфраструктури, наказує постачальникам загальнодоступних комунікаційних мереж та / або постачальникам послуг електронного зв'язку обмежувати надання послуги загальнодоступних мереж зв'язку та / або публічні послуги електронного зв'язку не більше ніж на 48 годин для одержувача послуг. Національний центр кібербезпеки повідомляє Регуляторному органу комуніка-

ції Литовської Республіки про розпорядження, надані постачальникам загальнодоступних комунікаційних мереж та / або постачальникам послуг публічного електронного зв'язку відповідно до цього пункту, не пізніше ніж наступного робочого дня;

- бере участь в управлінні кризами кібербезпеки;
- за необхідності інформує громадськість з метою уникнення кіберінциденту або припинення кіберінциденту в процесі;
- співпрацює з компетентними органами міжнародних організацій, зі створеними ними групами співробітництва, а також з іноземними компетентними органами та службами; має право звертатися до них з метою виконання функцій, передбачених цим законом та іншим законодавством у сфері кібербезпеки;
- обробляє персональні дані, необхідні для виконання функцій Національного центру кібербезпеки у сфері забезпечення кібербезпеки. Національний центр кібербезпеки обробляє персональні дані у порядку, встановленому Законом про правовий захист персональних даних;
- у співпраці з суб'єктами господарювання, науково-дослідними та освітніми установами й суб'єктами кібербезпеки розробляє проєкти, що зміцнюють національну кібербезпеку;
- виконує інші функції, визначені законодавчими актами Литовської Республіки у сфері забезпечення кібербезпеки.

До сфери кібербезпеки Законом також віднесено Державну інспекцію захисту даних, яка здійснює функції регулятора у сфері захисту персональних даних. Державна інспекція захисту даних здійснює політику кібербезпеки у сфері захисту персональних даних та виконує завдання, встановлені наглядовим органом відповідно до Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та щодо вільного переміщення таких даних, а також скасування Директиви 95/46/ЄС (Загальне положення про захист даних).

Окремі повноваження у сфері кібербезпеки надано поліції, але тільки в рамках запобігання кіберінцидентам, які, можливо, є складом кримінальних правопорушень, та їх розслідування.

Поліція у порядку, встановленому нормативно-правовими актами, здійснює попередження та розслідування кіберінцидентів, які можуть мати ознаки кримінального порушення:

- збирати, аналізувати та узагальнювати інформацію про кіберінциденти, які можуть мати ознаки кримінального правопорушення;
- визначити інформацію, необхідну для суб'єктів державного управління, що здійснюють управління та / або управління державними інформаційними ресурсами, операторів критичної інформаційної інфраструктури, провайдерів мереж загальнодоступного зв'язку та / або послуг електронного зв'язку загального користування, провайдерів послуг розміщення електронної інформації для кіберінцидентів, які можуть спричинити злочин порядок подання ознак акта для запобігання та розслідування;

- має право видавати вмотивовані вказівки максимум на 48 годин без санкції суду, протягом більш тривалого періоду з санкцією районного суду, обмежувати надання мереж загального користування та / або послуг публічного електронного зв'язку та послуг електронного хостингу інформації одержувачу, коли одержувач або його обладнання інформаційно-комунікаційних технологій може бути залученим до злочинної діяльності та / або доручити провайдеру мереж загального зв'язку та / або публічним послугам електронного зв'язку або провайдеру послуг електронного хостингу інформації вжити заходів щодо усунення причин кіберзлочинності. У таких випадках подання для підтвердження законності або обґрунтування дій мотивованим розпорядженням подається голові районного суду або уповноваженому ним судді. Якщо термін закінчується у вихідний день або державне свято, подання подається не пізніше наступного робочого дня після дня відпочинку чи свят. Якщо суддя не підтвердить законність або виправдання зазначених дій мотивованим наказом, наказ негайно зупиняється;
- мають право давати обґрунтовані вказівки провайдеру мереж загального зв'язку та / або послуг електронного зв'язку загального користування та послуг електронного хостингу інформації щодо збереження інформації, пов'язаної з послугами, що ними надаються, з яких можна визначити тип послуги зв'язку, використовувані технічні засоби та час використання; посвідчення особи, поштову, географічну адресу, телефон та будь-який інший номер доступу, платіжну інформацію та інформацію про оплату на підставі договору про надання послуг або угоди та інших відповідно до встановленого порядку, коли рішення суду мотивоване, отримувати дані про трафік користувача послуги та контролювати зміст переданої інформації.

СУБ'ЄКТИ КІБЕРБЕЗПЕКИ

Окремі обов'язки встановлено для суб'єктів кібербезпеки (але вони не поширюються на визначені в Законі про розвиток малого та середнього бізнесу малі та дуже малі підприємства, які надають цифрові послуги в Литовській Республіці та / або будь-якій іншій державі — члені ЄС). Такими суб'єктами кібербезпеки в Литві є:

1) суб'єкт господарювання, який контролює інформаційні ресурси держави та / або керує ними;
2) менеджер критичної інформаційної інфраструктури;
3) постачальник послуг загальнодоступних комунікаційних мереж та / або публічних цифрових послуг зв'язку;
4) постачальник послуг розміщення цифрової інформації;
5) постачальники цифрових послуг.

Суб'єкти кібербезпеки:

- відповідають за кібербезпеку послуг зв'язку та інформації, якими вони керують, та послуг, які вони надають, забезпечують їх відповідність організаційним та технічним вимогам кібербезпеки, що висуваються до суб'єктів кібербезпеки;
- проводять оцінку ризиків у порядку, встановленому в описі організаційних та технічних вимог кібербезпеки, що висуваються до суб'єктів кібербезпеки, а також здійснюють інші технічні та організаційні заходи з кібербезпеки на основі новітніх розробок технологій відповідно до визначеного ризику;
- повідомляють Національному центру кібербезпеки про кіберінциденти, що трапляються в системах зв'язку та інформації, які вони контролюють та / або якими керують, а також про вжиті заходи з управління кіберінцидентами відповідно до строків та умов, а також у порядку, визначеному Національним планом управління кіберінцидентами;
- надавати поліції інформацію, необхідну для запобігання та розслідування порушень закону, які є складовими кримінальних правопорушень у кіберпросторі, у порядку, встановленому Генеральним комісаром поліції, а також виконувати інші доручення поліції, видані на основі цього закону. Накази поліції щодо обмеження надання послуг їх одержувачам повинні виконуватися не пізніше ніж за 8 годин з моменту отримання наказу;
- призначити компетентну особу чи відділ, відповідальний за організацію й забезпечення кібербезпеки, та надати Національному центру кібербезпеки контактні дані такої особи чи відомства;
- виконувати накази Національного центру кібербезпеки, викладені у статті 8 цього Закону.

ОКРЕМІ СПЕЦІАЛЬНІ ОБОВ'ЯЗКИ

Окремі спеціальні обов'язки визначені для: операторів критичної інформаційної інфраструктури; суб'єктів, які контролюють інформаційні ресурси держави та / або керують ними; постачальників загальнодоступних комунікаційних послуг та / або публічних послуг цифрового зв'язку; постачальників послуг цифрового розміщення інформації та постачальників цифрових послуг.

Оператори критичної інформаційної інфраструктури:

- відповідно до типового плану управління кіберінцидентами в критичних інформаційних інфраструктурах затверджують плани управління кіберінцидентами в критичних інформаційних інфраструктурах та подають їх до Національного центру кібербезпеки;
- інформують провайдерів цифрових послуг про негативний вплив на роботу критичної інформаційної інфраструктури, що стався внаслідок несправності комунікаційних та інформаційних систем постачальників цифрових послуг, у порядку, встановленому Національним планом управління кіберінцидентами;

- не рідше ніж один раз протягом календарного року перевіряють функціонування засобів, призначених для управління кіберінцидентами в критичних інформаційних інфраструктурах, та подають результати тестування до Національної системи кібербезпеки у порядку, встановленому в описі організаційно-технічних вимог до кібербезпеки, що висуваються до суб'єктів кібербезпеки;
- забезпечують умови, щоб Національний центр кібербезпеки здійснював та контролював технічні заходи кібербезпеки в критичній інформаційній інфраструктурі та застосовував технічні засоби з метою вимірювання стійкості критичної інформаційної інфраструктури до кіберінцидентів.

Суб'єкти, які контролюють інформаційні ресурси держави та / або керують ними : забезпечують Національному центру кібербезпеки умови для здійснення та контролю технічних заходів з кібербезпеки в інформаційних ресурсах держави та застосування технічних засобів з метою вимірювання опірності інформаційних ресурсів держави до кіберінцидентів.

Постачальники загальнодоступних комунікаційних послуг та / або публічних послуг цифрового зв'язку публічно оприлюднюють рекомендації щодо заходів, спрямованих на забезпечення кібербезпеки під час використання послуг, що надаються мережами зв'язку загального користування, та / або публічних електронних послуг зв'язку, на своїх веб-сайтах або в інших засобах масової інформації .

Постачальники послуг цифрового розміщення інформації публічно оголошують на своїх веб-сайтах або публікують у будь-яких інших засобах масової інформації рекомендації постачальникам послуг цифрового розміщення інформації щодо заходів із забезпечення кібербезпеки за допомогою використання послуг цифрового хостингу інформації.

Постачальники цифрових послуг:

- публічно оголошують на своїх веб-сайтах або публікують у будь-яких інших засобах масової інформації рекомендації постачальникам послуг щодо заходів, спрямованих на забезпечення кібербезпеки шляхом використання послуг, що надаються постачальниками цифрових послуг;
- призначають представника для здійснення діяльності від імені постачальника цифрових послуг у Європейському Союзі. Таким представником є фізична чи юридична особа, яка має офіс в одній із тих держав — членів ЄС, у яких надаються цифрові послуги. Органи з реалізації політики в галузі кібербезпеки мають право звертатися до представника постачальника цифрових послуг щодо виконання обов'язків постачальника цифрових послуг, визначених цим законом. Якщо постачальник цифрових послуг призначає свого представника для здійснення діяльності в Литовській Республіці, вважається, що постачальник цифрових послуг підпорядковується юрисдикції Литовської Республіки.

Законом визначено створення інформаційної мережі кібербезпеки, метою якої є обмін інформацією про потенційні або минулі кіберінциденти, а також рекомендації, розпорядження, технічні рішення та інші заходи, що сприяють забезпеченню кібербезпеки та співпраці між членами мережі у сфері кібербезпеки. Інформаційна мережа кібербезпеки призначена виключно для тих суб'єктів кібербезпеки, які відповідають вимогам, викладеним у Правилах інформаційної мережі кібербезпеки. Інформаційна мережа кібербезпеки слугує для оприлюднення відповідної контактної інформації осіб або відомств, призначених суб'єктами кібербезпеки, відповідальними за організацію кібербезпеки та управління кіберінцидентами.

Між Національним центром кібербезпеки та поліцією здійснюється міжвідомча співпраця в управлінні кіберінцидентами та їх розслідуванні. Ці органи мають мають консультуватись одне з одним, співпрацювати у розслідуванні, обмінюватися інформацією щодо розслідування кіберінцидентів, необхідною цим інституціям для виконання передбачених їхньою компетенцією функцій. У разі необхідності про розслідування кіберінцидентів можна інформувати інші органи кримінальної розвідки та / або розвідувальні органи. Також передбачена міжвідомча співпраця Національного центру кібербезпеки та Державної інспекції захисту даних — з метою розслідування кібер-інцидентів, пов'язаних із порушеннями захисту персональних даних та / або конфіденційності, обміну інформацією, необхідною для виконання функцій, встановлених законодавчими актами, щодо розслідування кібер-інцидентів, які порушують захист особистих даних та / або конфіденційність.

Порядок міжінституційної співпраці в управлінні та розслідуванні кіберінцидентів встановлюється Національним планом управління кіберінцидентами.

Органи, які імплементували Політику кібербезпеки, мають право обмінюватися інформацією, наданою суб'єктами кібербезпеки, зокрема конфіденційною інформацією, тією мірою, якою це необхідно для виконання функцій таких органів, що належать до їх компетенції, і повинні забезпечувати захист отриманих даних.

Окремо Закон доповнений додатком, у якому зазначено, які акти ЄС були імплементовані в Законі: це Директива 2002/21/ЄС[6] та Директива (ЄС) 2016/1148[7].

Огляд[8] Cybersecurity Capacity Review. Republic of Lithuania, опублікований2017 році, містить аналіз та ґрунтовну оцінку інших факторів, що впливають на кібербезпеку. До них віднесено акти законодавства, що регулюють питання електронних комунікацій, захисту персональних даних, загальне кримінальне законодавство та міжнародні конвенції, до яких Литва приєдналась і успішно виконує.

Права та обов'язки постачальників послуг загальнодоступних комунікаційних мереж також регулюються Положенням про затвердження Правил забезпечення безпеки та доброчесності мереж загальнодоступних комунікацій та служб громадського електронного зв'язку.

6 https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0021

7 https://eur-lex.europa.eu/eli/dir/2016/1148/oj

8 https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf

Крім того, Закон про електронні комунікації Литовської Республіки встановлює зобов'язання постачальників послуг виконувати відповідні технічні та організаційні заходи для забезпечення безпеки та цілісності їхніх послуг.

Важливі правові положення про кіберзлочинність містяться в загальному кримінальному законодавстві. Країна ратифікувала регіональні та міжнародні документи щодо кіберзлочинності й послідовно прагне впровадити ці заходи у внутрішнє законодавство.

Кримінальний кодекс Литви містить положення щодо злочинів, скоєних за допомогою електронних пристроїв, однак він не передбачає жодних санкцій за крадіжку даних особи в електронному та неелектронному просторі. Кримінально-процесуальний кодекс гармонізований із законодавством Європейського Союзу і включає положення про розслідування злочинів та доказові вимоги.

Литва ратифікувала або приєдналася до міжнародних угод про права людини і визнала їх захист у всіх нових кодексах. Внутрішнє законодавство визначає гарантії захисту права особи на приватне життя під час збору, використання та розголошення особистих даних, а всеохопний захист даних забезпечують ухвалені Закон про правовий захист персональних даних Литовської Республіки та Закон про захист персональних даних.

Ухвалено та застосовується комплексне законодавство про захист дітей, яке встановлює правила захисту даних та конфіденційності для неповнолітніх. Литва є учасницею Конвенції ООН про права дитини та інших відповідних міжнародних конвенцій. Наразі розробляється законодавство про інтелектуальну власність в Інтернеті , тривають консультації з ключовими заінтересованими сторонами.

Передові можливості розслідування дають змогу розслідувати складні випадки кіберзлочинності. Правоохоронні органи мають достатній потенціал для запобігання кіберзлочинності й боротьби з нею та проходять спеціалізовану підготовку. На центральному та місцевому рівнях діють спеціалізовані прокурори та судді. Однак не існує механізму, який забезпечував би обмін інформацією та передовою практикою між прокурорами та суддями, тим самим сприяючи ефективному розслідуванню справ щодо кіберзлочинності.

Для запобігання кіберзлочинності та боротьби з нею були сформовані офіційні механізми міжнародного співробітництва. Литва уклала угоди з Інтерполом та Європолом, а також двосторонні угоди із сусідніми країнами щодо транскордонного обміну інформацією.

Крім того, встановлені неформальні зв'язки між урядом та органами кримінального правосуддя, а також між інтернет-провайдерами та правоохоронними органами, що забезпечує регулярний обмін інформацією про випадки кіберзлочинності.

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ЛИТВИ

Литва запровадила свою Стратегію 13.08.2018 р.[9]

Основна мета Стратегії — надати литовському суспільству можливість досліджувати потенціал інформаційно-комунікаційних технологій (ІКТ) шляхом своєчасного та ефективного виявлення кіберінцидентів, запобігання виникненню кіберінцидентів, а також управління наслідками порушення кібербезпеки. Національна стратегія кібербезпеки Литви визначає найважливіші стовпи політики національної кібербезпеки. Стратегія спрямована на посилення розвитку можливостей кібербезпеки та кіберзахисту, запобігання кіберзлочинам та їх розслідування, сприяння культурі кібербезпеки та розвитку інновацій, зміцнення тісного державно-приватного партнерства (PPP) та міжнародного співробітництва, забезпечення виконання міжнародних зобов'язань щодо кібербезпеки всередині країни до 2023 року.

Стратегія розроблена з урахуванням екологічного аналізу, досліджень даних та пропозицій від представників державного й приватного секторів. Це відповідає положенням Програми сімнадцятого уряду Литовської Республіки, ухваленої постановою №XIII-82 сейму Литовської Республіки від 13 грудня 2016 р. «Про програму Уряду Литовської Республіки» (далі — програма Уряду Литовської Республіки), Стратегії національної безпеки, затвердженої резолюцією №IX-907 Сейму Литовської Республіки від 28 травня 2002 р. «Про затвердження стратегії національної безпеки», Закону Литовської Республіки «Про кібербезпеку», Рекомендації Європейського Парламенту, Ради та Європейської Комісії у галузі кібербезпеки, а також «Стратегії єдиного цифрового ринку Європи» від 6 травня 2015 року.

Програма розвитку на 2014–2020 рр. «Цифровий порядок денний Республіки Литва», затверджена постановою №244 Уряду Литовської Республіки від 12 березня 2014 року, та рекомендації OECD щодо управління ризиками цифрової безпеки для економічного та соціального процвітання також відображені в Стратегії.

ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

Як і інші країни світу з розвиненою широкосмуговою інфраструктурою, де активно розвивається потенціал ІКТ, Литва як об'єкт атак приваблива не лише для окремих осіб, груп осіб чи організованих груп, а й для країн, зазначених у **Звітах про загрози національній безпеці**, які щороку публікуються Департаментом безпеки Литовської Республіки та Міністерством національної оборони Литовської Республіки (далі — SSD та SID відповідно)[10].

9 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

10 https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-EN.pdf

Ці країни загрожують національній безпеці Литви та проводять ворожі дії в глобальному й литовському кіберпросторі. Дані, зібрані Національним центром кібербезпеки Міністерства національної оборони (NCSC), SSD та SID, свідчать, що Литва постійно стикається з різними типами кіберінцидентів, які зазіхають на інформаційні ресурси та об'єкти критичної інформаційної інфраструктури.

За прогнозами, очікується збільшення кількості та масштабів кіберінцидентів згідно з даними звіту про стан національної кібербезпеки за 2017 рік.

Литовська команда реагування на комп'ютерні надзвичайні ситуації, або CERT-LT, у 2017 р. обробила 54 414 кіберінцидентів. 2017 р. кількість зареєстрованих кіберінцидентів на 10% перевищила відповідний показник 2016 року. Напади на кіберспільноти в основному стосуються литовських публічних інформаційних ресурсів, однак приватна критична інформаційна інфраструктура та інші об'єкти стратегічного або важливого для національної безпеки значення також опинилися в зоні ризику. Застосувавши технічні засоби кібербезпеки, NCSC визначив, що найбільшу кількість шкідливих програм виявлено у таких секторах: енергетика (27%), громадська безпека та правовий порядок (22%), зовнішні справи та політики безпеки (21%). Порівняно з 2016 роком зловмисне програмне забезпечення переважно поширювалося у сферах громадської безпеки та правового порядку, закордонних справ та політики безпеки й енергетики. Стан захисту веб-сайтів громадського сектору погіршився відповідно до національного звіту про стан кібербезпеки за 2017 рік, що також впливає на стан кібербезпеки країни.

Зростання кількості кіберінцидентів, зазначене у щорічних звітах NCSC, SSD та SID, свідчить, що кожен суб'єкт кібербезпеки повинен виділити чітко визначену кількість часу, грошей та інших ресурсів на захист своїх комунікаційних та інформаційних систем і надаваних послуг.

Суб'єкти кібербезпеки виконують оцінки ризиків кібербезпеки, але часто ці процедури формальні й проводяться задля відповідності законодавчим вимогам або міжнародно визнаним стандартам. Посібник з аналізу ризиків, опублікований Міністерством внутрішніх справ Литовської Республіки 12 років тому, свідчить про прогрес в оцінці ризиків, якщо врахувати сучасні умови досліджень та інновацій. З часом методологія оцінювання ризиків для кібербезпеки змінилася, як трансформувалося й **розуміння ефективності оцінки ризиків управління системою безпеки середовища в цілісний підхід оцінювання ризиків діяльності організацій.**

Окремі процеси оцінки ризику безпеки у Литві вже сягнули високого ступеня розвитку, однак **на національному рівні культура оцінювання ризиків кібербезпеки та процеси оцінювання кібербезпеки залишаються фрагментарними**. Загрози щодо кібербезпеки та прогалини в безпеці не були належним чином проаналізовані та цілісно інтегровані в процес оцінювання ризику. Крім того, швидкий розвиток ІКТ становить виклик для фахівців з кібербезпеки, які повинні мати належні знання, навички й практику.

Законодавство

З метою підвищення ефективності розробки та реалізації політики кібербезпеки й покращення оцінки ризиків кібербезпеки та інших вимог у 2018 році розроблені і впроваджені такі зміни до законодавства Литви:

- переглянуті положення Закону «Про кібербезпеку» — з метою покращення організації, управління та контролю системи кібербезпеки;
- визначено компетенцію, функції, права та обов'язки державних установ, відповідальних за розробку та реалізацію політики кібербезпеки;
- детальніше визначені обов'язки та відповідальність суб'єктів кібербезпеки, встановлено додаткові заходи забезпечення кібербезпеки;
- об'єднані регуляторні функції захисту державної інформації, роботи загальнодоступних комунікаційних мереж, загальнодоступних послуг цифрового зв'язку та постачальників послуг цифрового розміщення інформації, що дало змогу здійснювати систематичний моніторинг та управляти кіберпростором; переглянуто систему управління інцидентами.

У 2017 році в національному навчанні з кібербезпеки Cyber Security 2017 взяли участь близько 200 представників від понад 50 організацій приватного та державного сектору.

Відповідно до статей 8 та 26 Закону Литовської Республіки «Про розвідку» громадськості представлено Оцінку загроз національній безпеці[11]. Документ містить консолідовану, некласифіковану оцінку загроз та ризиків для національної безпеки Литовської Республіки.

В документу оцінено події, процеси та тенденції, які зумовлюють найбільший вплив на ситуацію з національною безпекою в Литовській Республіці. З урахуванням цих чинників та довгострокових тенденцій, що впливають на національну безпеку, в документі наведено оцінку основних викликів, які постануть перед сферою національної безпеки Литви найближчим часом (у 2019–2020 рр.). Прогноз щодо довгострокових тенденцій наведено на перспективу до 10 років. Оцінка базується на інформації, доступній до 1 грудня 2018 року, тож окреслює такі ризики й виклики.

Зовнішні загрози

У 2018 році міжнародна спільнота стала свідком імперських амбіцій Росії.

Західні країни відзначили та визначили агресивні заходи, застосовані Росією: спроби втручання у внутрішні процеси західних країн, використання хімічної зброї проти колишнього російського офіцера розвідки, проведення агресивних кібероперацій як з Росії, так і в європейському просторі.

11 https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-LT.pdf

Агресивна зовнішня політика Росії стала ключовим інструментом виправдання правлячого режиму. Прагнучи завоювати «належне» місце у світовій системі, Росія поєднує дипломатію та операції проти «слабкого» Заходу, шукаючи способів зменшити вплив США та Європи в інших регіонах. Однак Росія ще не знайшла надійних союзників для втілення своїх глобальних амбіцій, тоді як Захід дедалі чіткіше усвідомлює російські загрози і вдається до спільної реакції. Російський правлячий режим визнає проблеми, пов'язані з міжнародною ізоляцією та економічним спадом, проте його кроки свідчать, що нинішня політична система не вирішує фундаментальних проблем. У Росії не спостерігається реформ і політичних змін, і вони навряд відбудуться. Кремль надалі розширює свій набір інструментів контролю над суспільством і успішно маніпулює атрибутами передової демократії — фальшивими виборами, контрольованою опозицією, толерантністю до соціальних, але не політично орієнтованих протестів.

У 2018 році у Росії тривав розвиток військових потужностей, зокрема на територіях, що межують із Литвою, а саме в Калінінградській області. Невдовзі Росія має намір розмістити там додаткові наступальні елементи, а також засоби протиповітряної оборони та авіації. Росія посилює свої можливості з виконання військових операцій за 24–48 годин. Значення військової сили як одного з основних інструментів російської зовнішньої політики та політики безпеки зростає. Однак зростаючі оборонні можливості країн Балтії та військових контингентів НАТО, що розгортаються в регіоні, значно зменшують шанси використання Росією військових засобів проти країн Балтії. Найбільш вразливою до російського впливу країною поруч із Литвою є Білорусь. Тим часом Мінськ неспроможний здійснювати повністю незалежну політику через фінансову залежність від Росії, невирішені двосторонні питання та відсутність економічних реформ у державному секторі.

Російські служби розвідки та безпеки намагаються адаптуватися до зовнішніх (зокрема й литовських) оборонних заходів: використовувати ділове, туристичне та інше недипломатичне прикриття, розширити географію своїх операцій, перенести розвідувальні операції в Росію чи треті країни, вербувати довірених осіб (особливо в Білорусі), маніпулюючи спільним радянським минулим, шукаючи людей, ідеологічно близьких до Росії (так, відбувається активне вербування литовських та іноземних громадян, які подорожують до Росії та Білорусі).

Росія розвиває кіберможливості, що стають одним із головних інструментів проведення операцій з розвідки та впливу закордоном. Здійснюючи ці дії, Росія не відчуває «червоних ліній» щодо географії та важливості цілі і сподівається уникнути відповідальності. Поки Росія, ймовірно, вважає, що вигода від кібероперацій перевищує потенційну шкоду, якої може завдати реакція західних країн.

Прагнучи зневажити державність Литви, Росія реалізує цілеспрямовані проєкти з просування історичної політики на основі російської інтерпретації минулого, заперечення радянської окупації та пропагування позитивного радянського впливу на розвиток Литви. Особливо Росія прагне залучити до цих проєктів молодь. У 2018 році однією з головних цілей російської історичної політики був литовський післявоєнний збройний опір.

Росія виробляє постійний потік пропаганди проти Литви, який особливо посилюється, коли Литва ініціює заходи реагування проти агресивної зовнішньої політики РФ.

Намагаючись впливати на внутрішні процеси у Литві, Росія використовує для своєї підривної діяльності демократичні свободи та права. Під гаслами турботи про свою діаспору РФ намагається роздробити литовське суспільство. Крім того, удаючи розвиток культурних відносин, Росія фактично просуває свою агресивну зовнішню політику. Вона прагне впливати на політичні процеси в Литві, але наразі немає беззаперечних свідчень, що бажаного впливу досягнуто.

У міру зростання економічних та політичних амбіцій Китаю діяльність спецслужб і служб безпеки цієї країни в Литві та інших країнах НАТО і ЄС стає дедалі агресивнішою. Прагнучи зібрати відповідну інформацію, китайська розвідка намагається вербувати литовських громадян.

Російські служби розвідки та безпеки приділяють особливу увагу збиранню інформації про стратегічну інфраструктуру Литви: промислові компанії, інфраструктуру Збройних сил Литви, системи зв'язку, морські порти та аеропорти, залізничні й дорожні мережі. Останнім часом російська розвідка зацікавилася об'єктами винятково енергетичного сектору Литви. Росія постійно експлуатує місії Організації з безпеки та співробітництва в Європі (OSCE), спрямовані на формування взаємної впевненості та прозорості між державами-учасницями шляхом обміну інформацією щодо військових можливостей. Представники Росії збирали розвідувальні дані щодо критичної інфраструктури Литви під час оглядових польотів у межах Договору про відкрите небо та інспекції з контролю над озброєнням згідно з Віденським документом.

У 2018 році ворожу діяльність, яка може бути пов'язана як із державою, так і з недержавними суб'єктами РФ, спостерігали в литовській доменній зоні.

У світовій кіберсфері серйозне занепокоєння викликають китайське промислове шпигунство, дії Північної Кореї та Ірану, але досі таку діяльність у литовських інформаційних системах оцінювали як фрагментарну та випадкову.

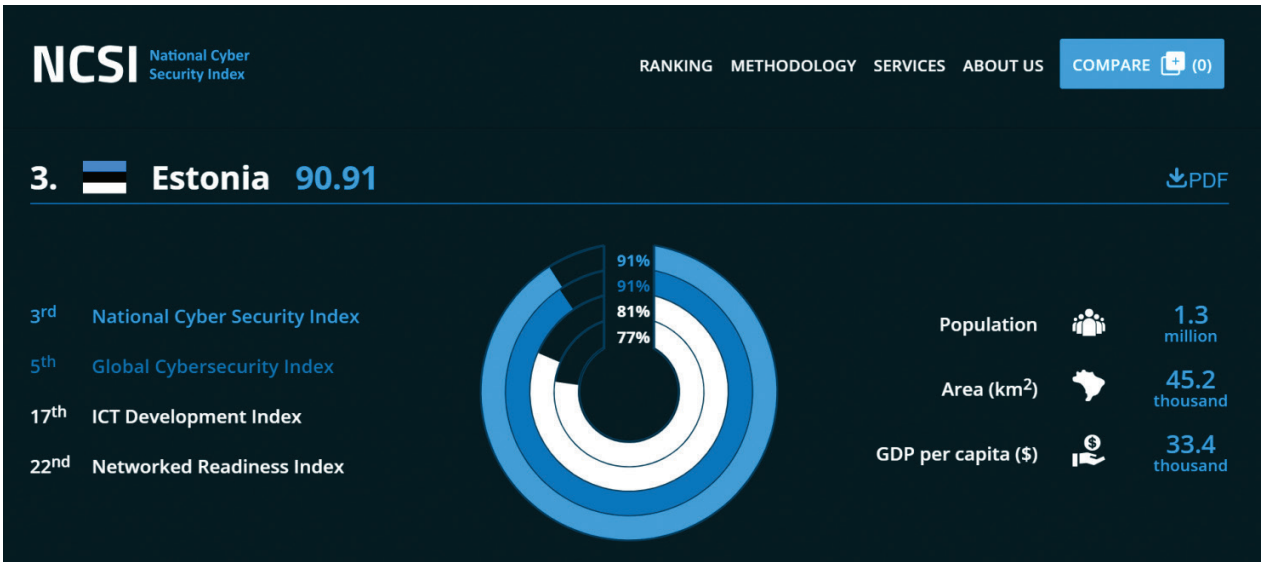
Тим часом російські спецслужби та служби безпеки посідають важливе місце серед загрозах для литовського кібердомену: вони проводять збір розвідданих, порушують роботу IT-систем і сприяють операціям впливу.

Активність російських кібершпигунських груп виявлена майже у всіх країнах світу, але головна увага приділяється країнам НАТО і іншим регіонам, що мають геополітичне значення для Росії. Кібердіяльність стає для Росії одним із основних інструментів досягнення геополітичних цілей не лише під час конфліктів, а й у мирний час. Російська кібердіяльність також використовувалася як елемент стримування конфліктних держав. Займаючись ворожою діяльністю в кіберсфері, Росія не обмежує себе ні географічно, ні з точки зору цілей, сподіваючись уникнути відповідальності. Дотепер користь від кібероперацій для Росії оцінювалася як важливіша, ніж потенційна реакція західних держав.

Постійно спостерігалася активність хакерів, що належать до RISS (російський інститут стратегічних досліджень) щодо збору розвідданих в литовських інформаційних системах. В операціях з кібершпигунства проти Литви застосовуються просунуті кіберінструменти. Їх не можна ідентифікувати за допомогою звичайних програм системної безпеки, тому вони здатні протягом тривалого періоду часу непомітно проводити ворожу активність у заражених мережах. Найактивнішими у кібершпигунстві в Литві були GRu Group Sofacy / APT28 та кібергрупа FsB Agent.btz / Snake. Їхні основні напрямки збору інформації — політика, військова сфера та економіка.

Проводячи розвідувальну діяльність, групи проникають не лише в інформаційні системи державних установ, а й у власність приватних організацій або окремих осіб. Отримані дані зазвичай використовуються для проведення операцій впливу та проникнення до інших систем, наприклад більш захищених мереж, призначені для обробки чутливої інформації або систем, пов'язаних із критичною державною інфраструктурою.

ЕСТОНІЯ



Естонія є одним із беззаперечних лідерів у ЄС у частині впровадження цифрових сервісів, електронного урядування і демократії[12].

Сотні електронних послуг надаються та просуваються державою через портал електронних сервісів[13]. Серед громадян дуже високою популярністю користуються такі державні послуги, як сплата податків та податкова звітність[14]: ще у 2012 році понад 94% декларацій з податку на прибуток надходили в електронному вигляді.

Естонія у 2008 році однією з перших країн світу ухвалила національну стратегію кібербезпеки. Документ розроблений Міністерством оборони на 2008–2013 роки та супроводжувався планом впровадження.

12 https://e-estonia.com/

13 https://www.eesti.ee/

14 https://e-estonia.com/enter-e-governance/

У Стратегії 2008 року запропоновано всебічний погляд на кібербезпеку та окреслено такі основні напрями:

- застосування в Естонії послідовних заходів із розбудови системи кібербезпеки;
- розвиток Естонії в галузі інформаційної безпеки та підвищення обізнаності громадян із цими питаннями;
- розробка відповідної регуляторної та правової бази для підтримки безпечної та безперебійної роботи інформаційних систем;
- просування міжнародного співробітництва, спрямованого на зміцнення глобальної кібербезпеки[15].

У 2019 році Стратегію кібербезпеки було оновлено; тепер вона охоплює 2019–2022 роки[16].

З метою реалізації стратегії наприкінці минулого року було створено міжвідомчу координаційну робочу групу, завданням якої є моніторинг та координація виконання цілей, узгоджених у стратегії, та створення звіту для Ради кібербезпеки.

Стратегія кібербезпеки спрямована на підтримку та розвиток сталого цифрового суспільства з високою технологічною стійкістю та готовністю до криз, сприяння підприємництву та дослідженням і розробкам у галузі кібербезпеки, підвищення рівня фахівців у цій галузі та перетворення Естонії на поважного партнера на міжнародній арені.

Основні міністерства, відповідальні за реалізацію стратегії (Міністерство освіти і досліджень, Міністерство юстиції, Міноборони, Міністерство економіки та комунікацій, Міністерство внутрішніх справ та Міністерство закордонних справ), призначили службовця з кібербезпеки для участі в діяльності координаційної робочої групи. Стратегія на 2019–22 роки була затверджена урядом Естонії у листопаді 2018 року, і це третій стратегічний документ у сфері кібербезпеки, який визначає довгострокове бачення, цілі та пріоритетні напрями, повноваження та завдання, необхідні для досягнення цілей. Міністерство економіки та комунікацій здійснює управління реалізацією стратегії та створеною робочою групою[17].

ЦІЛІ КІБЕРЗАХИСТУ

Нова стратегія кібербезпеки визначає чотири важливі цілі[18]:

1. Естонія — це стале цифрове суспільство, яке спирається на високу технологічну стійкість і готовність до надзвичайних ситуацій.
2. Естонська галузь кібербезпеки є сильною, інноваційною, орієнтованою на дослідження, глобальною та конкурентоспроможною і охоплює всі ключові компетенції Естонії.

15 https://www.kaitseministeerium.ee//et/uudised/valitsus-kinnitas-kuberjulgeoleku-strateegia

16 https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf

17 https://www.ituudised.ee/uudised/2019/07/23/kingo-moodustas-kuberturvalisuse-strateegia-tooruhma

18 https://www.mkm.ee/en/objectives-activities/cyber-security

3 Естонія є надійним та професійним партнером на міжнародній арені.

4 Естонія є кіберграмотним суспільством і забезпечує на перспективу достатню кількість талановитих фахівців.

Питання кіберзлочинності висвітлені й у Цілях кримінальної політики до 2018 року: *«Боротьба з кіберзлочинністю має зосереджуватися на боротьбі із сексуальним насильством над неповнолітніми, запобіганні великим комп'ютерним аферам та поширенню комп'ютерних вірусів і зломів. Для запобігання кіберзлочинності необхідно підвищувати рівень обізнаності уразливих цільових груп (наприклад, неповнолітніх, людей похилого віку). Для покращення боротьби з кіберзлочинністю потрібно забезпечити у правоохоронних органах достатню кількість IT-фахівців»*[19].

Відповідальність за загальну координацію політики у сфері кібербезпеки наразі покладено на Міністерство економіки та комунікації Естонії, хоча до 2011 року цим питанням опікувалося Міністерство оборони.

НАГЛЯД ТА АНАЛІЗ ВИКОНАННЯ

У 2009 році при Комітеті з безпеки уряду Естонії була створена Рада з питань кібербезпеки. Завдання Ради — сприяти безперебійній співпраці між різними установами та здійснювати нагляд за виконанням цілей Стратегії кібербезпеки. Головує у Раді генеральний секретар Міністерства економіки та зв'язку[20]. Крім того, на Раду покладається функція контролю за виконанням стратегії, для цього урядом щороку подається звіт про хід виконання стратегії, в якому окреслюється поточна реалізація поставлених цілей.

Утім, аналіз виконання Стратегії виявив певні проблеми: «Слід визнати, що всі цілі стратегії не були досягнуті належним чином брак ресурсів, слабке керівництво та адміністративні перешкоди, що ускладнювали виконання, а також інші причини»[21].

Естонське управління інформаційних систем (Riigi Infosüsteemi Amet, RIA) було створене в 2011 році як Естонський центр компетенції та координації кібербезпеки в межах сфери управління Міністерства економіки та зв'язку. RIA відповідає за розвиток державних інформаційних систем та управління ними, а також розробку відповідних політик та стратегій, координуючи забезпечення кібербезпеки, стандартів безпеки, заходів, пов'язаних із кібербезпекою, та подолання інцидентів, що фіксуються в естонських мережах[22].

Один із основних сегментів відповідальності RIA — нагляд за постійним застосуванням заходів безпеки, використовуваних тими інформаційними системами, які підтримують життєво важливі для держави послуги та пов'язані з ними інформаційні активи. RIA також здійснює діяльність,

19 https://www.riigiteataja.ee/akt/13329831

20 https://www.mkm.ee/en/objectives-activities/cyber-security

21 https://icds.ee/wp-content/uploads/2013/Piret%20Pernik%20-%20Cyber%20Space%20in%20Estonia.pdf

22 https://www.ria.ee/et/riigi-infosusteem/riigi-infosusteemi-haldussusteem-riha.html

пов'язану із захистом критичної інформаційної інфраструктури, наприклад аналіз ризиків та підготовку відповідних заходів безпеки. У випадку порушення вимог безпеки під час надання життєво важливих послуг RIA також може здійснювати позасудові провадження, наприклад накладати штрафи.

Ще одна основна сфера відповідальності окреслена Законом про публічну інформацію, який визначає Інспекцію із захисту даних та Департамент інформаційної системи Естонії відповідальними за нагляд за дотриманням Закону:

«Департамент інформаційної системи Естонії здійснює адміністративний та державний нагляд за дотриманням запровадження, ведення та обслуговування баз даних та відповідністю взаємодії інформаційної системи з рівнем обміну даними між інформаційними системами вимогам, передбаченим цим Законом та законодавством, прийнятому на його виконання»[23].

Відповідно до оновленого у 2019 році Закону про захист персональних даних Інспекція із захисту даних також має широкі повноваження, числі зокрема: «контролювати відповідні розробки, ступінь їх впливу на захист персональних даних, зокрема розвиток інформаційних та комунікаційних технологій» [24] та накладати адміністративні й кримінальні санкції.

В Законі про кібербезпеку[25] імплементовано Директиву (ЄС) 2016/1148 Європейського парламенту та Ради від 6 липня 2016 року.

Закон про правоохоронні органи також визначає спеціальні заходи «для встановлення серйозної загрози чи протидії їй»[26], наприклад допит осіб, які потребують виготовлення документів чи в'їзду у країну, обстеження приміщень, управління рухомим майном. Такі законодавчі положення були ухвалені у 2014 році .

Крім того, RIA координує розробку та адміністрування системи управління інформаційною системою держави, а також впровадження інших систем, що забезпечують її функціонування.

Команда реагування на комп'ютерні надзвичайні ситуації (CERT-EE)

В межах RIA Естонська команда реагування на комп'ютерні надзвичайні ситуації (CERT-EE) забезпечує запобігання кіберінцидентам в естонських комп'ютерних мережах, опікується питаннями поінформованості користувачів про безпеку, здійснює управління X-Road та адміністрування державного порталу eesti.ee, готує звіти про поширення шкідливих програм та інцидентів, зафіксованих в естонських комп'ютерних мережах.

CERT-EE виявляє, відстежує та долає кіберінциденти в естонських комп'ютерних мережах, інформує про загрози та організовує профілактичні заходи. Департамент із боротьби з інцидентами RIA працює в Естонії як національний CERT і виступає міжнародною контактною точкою.

23 https://www.riigiteataja.ee/en/eli/522122014002/consolide

24 https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523012019001/consolide

25 https://www.riigiteataja.ee/akt/122052018001

26 https://www.riigiteataja.ee/en/eli/528012015003/consolide

З літа 2015 року CERT-EE цілодобово стежить за тим, що відбувається в кіберпросторі Естонії. В результаті було виявлено та попереджено набагато більше кіберінцидентів, ніж у попередні роки.

Цілі CERT-EE:

- контролювати ситуацію з інформаційною безпекою в Естонії, використовуючи отримані звіти та збираючи інформацію про кіберінциденти;
- допомагати запобігти кіберінцидентам та зменшити ризики для безпеки, зокрема забезпечуючи обізнаність та інформування щодо безпеки,
- допомагати та консультувати органи влади щодо кіберінцидентів, якщо вони дають розпорядження правоохоронним органам розпочати розслідування інциденту.
- CERT-EE є членом мережі CSIRT Європейського агентства з інформаційної та мережевої безпеки (ENISA).

Інструменти та послуги CERT-EE:

Середовище передачі файлів paste.cert.ee	Інструмент дає змогу надсилати CERT-EE підозрілі файли для аналізу. Підходить для передачі фішингових листів та вкладених додатків, зразків зловмисного програмного забезпечення тощо.
«Пісочниця» CERT-EE cuckoo.cert.ee	Інструмент аналізу файлів для IT-фахівців. Дає змогу в безпечному середовищі стежити за тим, як поводяться операційні системи, що працюють на різних віртуальних та фізичних платформах, коли виконується підозрілий файл.
Вебінструмент для сканування вірусів IRMA, irma.cert.ee	Інструмент для користувачів мережі передачі даних державних агентств та партнерів з приватного сектора, призначений для перевірки підозрілих вкладень та інших файлів невизначеного походження, отриманих електронною поштою. Перевага інструмента в тому, що надані файли не залишаються в невідомих місцях на копіюванні, а перебувають на файловому сервері естонського державного агентства та регулярно видаляються.
Попередження та повідомлення CERT-EE – twitter.com/cert_ee	Найбільш оперативний спосіб дізнаватися про сповіщення та попередження від CERT-EE.
Автоматизоване рішення для моніторингу Suricata4All (S4A)	Рішення складається з центральної системи, керованої CERT-EE, та датчиків, які власники мережі можуть встановити у своїй компанії чи установі. Центральна система розподіляє правила на датчики, на основі яких виявляються атаки. Датчики, своєю чергою, в разі виявлення шкідливого трафіку надсилають повідомлення до центральної системи. Система також дає змогу зберігати, індексувати та аналізувати мережевий трафік.
Кібербюлетень CERT-EE	Щоденний інформаційний бюлетень із резюме новин зі сфери кібербезпеки та інформації з відкритих джерел.

З 2013 року державні органи, згідно із законом, зобов'язані негайно повідомляти CERT-EE про всі значні кіберінциденти, спрямовані проти їхніх систем, а також подавати щоквартальні звіти про кібербезпеку на підставі затвердженої урядом Естонії «Системи управління інформаційною безпекою»[27].

RIA також бере участь у розробці національних стратегій та політики в галузі кібербезпеки, здійснюючи координацію навчання користувачів та розробників тих інформаційних систем, які належать до мережі інформаційних систем держави, та організацію досліджень і перевірок державної інформаційної системи[28].

Закон Естонії про національну оборону встановлює правову базу для ефективного реагування на загрози країні за потреби. Закон є основою для впровадження національної оборонної системи, що випливає з «Національної оборонної стратегії», згідно з якою у мирний та воєнний час застосовуються подібні системи управління, а також впровадження принципу «широкого розуміння» національної оборони. Згідно з ним, національна оборона охоплює військову оборону, сфери управління всіх міністерств, участь суспільства в національній обороні, а також захист населення[29].

Концепція національної безпеки визначає кіберзагрози як такі, що можуть спричинити значні наслідки та збитки для суспільства[30].

Концепція національної безпеки Естонії встановлює мету, принципи та напрями політики безпеки. Подана урядом Концепція національної безпеки підлягає затвердженню Рійгікогу. Концепція національної безпеки є рамковим документом, який слугує основою для підготовки конкретних планів розвитку та дій.

Національний план розвитку оборони

Національний план розвитку оборони Естонії на 2017–2026 роки[31] визначає пріоритети підвищення обороноздатності та вимоги до неї, виходячи з Національної військової стратегії, а також довгострокових програм розвитку у військово-оборонній сфері та загальних обмежень у ресурсах для розвитку сил оборони та ліги оборони.

Національний план розвитку оборони включає питання інвестицій у модернізацію оборонної інфраструктури. Загальний запланований обсяг інвестицій на період планування — понад 250 млн євро. Заплановані значні інвестиції в інфраструктуру та польові навчання за підтримки союзників. Крім модернізації казарм і забезпечення сучасних умов для навчання призовників, основні інвестиції будуть спрямовані на **розвиток Кіберкомандування**, військової поліції, флоту, підтримку та розбудову Центру медицини катастроф.

---

27 https://www.riigiteataja.ee/akt/119032012004

28 https://www.riigiteataja.ee/akt/13147268?leiaKehtiv

29 https://www.riigiteataja.ee/en/eli/ee/513072016005/consolide/current

30 https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf

31 https://www.kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/rkak2026-a6-spreads_eng-v6.pdf

Національний план розвитку оборони розробляється урядом республіки на підставі пропозиції міністра оборони на десять років і переглядається на підставі пропозиції міністра оборони кожні чотири роки. Перед поданням Національного плану розвитку оборони на розгляд уряду міністр оборони повинен розглянути думку Комітету національної оборони Рійгікогу (естонського парламенту).

План дій військової оборони[32] визначає заходи на виконання Національного плану розвитку оборони, причому це мають бути кроки, засновані на організаційній доцільності та забезпечені ресурсами, що відповідають вимогам до планів розвитку, встановленим Законом про державний бюджет.

План дій військової оборони встановлюється міністром оборони на чотири роки й переглядається щороку. Національний план розвитку оборони описує виконання військових функцій національної оборони з використанням наявних військових можливостей, відповідно до цілей, встановлених Національною військовою стратегією.

Національний план розвитку оборони встановлюється Командувачем сил оборони строком на один рік за погодженням міністра оборони.

Міністерство оборони є координаційним органом з питань кіберзахисту у сфері національної оборони. Загальна функція Міністерства оборони полягає у формуванні пропозицій щодо планування національної оборонної політики, її впровадження, здійснення запланованих заходів та організації національної оборони. Основна зона відповідальності Міністерство оборони — оснащення сил оборони та управління ними, управління Агенцією оборонних ресурсів, військовими навчальними закладами та іншими суб'єктами.

У лютому 2014 року було засновано окремий відділ, що займається кібербезпекою безпосередньо[33]. Відділ у складі технічних експертів з питань забезпечення кібербезпеки та експертів з питань політики координує розвиток інформаційних систем та інформаційних технологій у сфері компетенції Міністерства оборони, займається плануванням політики в межах юрисдикції Міністерства оборони та контролює виконання політики.

Окрім Міністерства оборони, національний кіберзахист підтримує Відділ кіберзахисту Естонської ліги оборони — підрозділ, до складу якого входять фахівці з кібербезпеки як державних, так і приватних інституцій[34].

Естонська ліга оборони (Kaitseliit) — це добровольча воєнізована озброєна національна організація оборони, яка діє в межах завдань Міністерства оборони і включає підрозділ з кіберзахисту. Діяльність Ліги оборони Естонії регулюється окремим Законом про Лігу оборони Естонії[35].

---

32 https://www.kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/rkak_2017_2026_avalik_osa.pdf

33 https://www.kaitseministeerium.ee/et/ministeerium-kontaktid/tutvustus-ja-struktuur

34 https://www.kaitseliit.ee/en/cyber-unit

35 https://www.riigiteataja.ee/en/eli/512092014008/consolide

В частині управління об'єктами критичної інфраструктури та забезпечення їх захисту Естонія ухвалила три основні закони, які слугують регуляторною базою в цій сфері.

Закон про надзвичайний стан[36] та Закон про надзвичайні ситуації[37] окреслюють комплексний підхід і не зосереджені конкретно на кіберкризах. За виконання обох актів відповідає Національний комітет з управління кризовими ситуаціями на чолі з міністром внутрішніх справ. Закон про надзвичайні ситуації забезпечує правову основу для управління кризовими ситуаціями, зокрема підготовки до надзвичайних ситуацій та реагування на них, а також забезпечення безперервної роботи життєво важливих служб. У його положеннях не передбачено державних кроків на випадок військової загрози. Закон стосується широкого спектру надзвичайних ситуацій, визначає організаційну структуру управління надзвичайними ситуаціями та процедурні рамки реагування на них.

Закон про надзвичайні ситуації також регулює захист критичної інфраструктури. Головними обов'язками операторів основних послуг є підготовка сучасної «постійної оцінки ризику експлуатації»[38] та план безперервної роботи для життєво важливих сервісів, що перебувають під контролем цих операторів чи належать їм. Також, за Законом, оператори мають негайно повідомляти національній організації, до сфери компетенції якої належить ця життєво важлива послуга, якщо подія може вплинути на функціонування життєво важливого сервісу або становить небезпеку для нього; надавати інформацію органам, які звертаються із запитом; та виконувати всі інші обов'язки відповідно до Закону про надзвичайні ситуації.

Надзвичайний стан оголошується у випадку виникнення загрози, яка підриває конституційний лад Естонії, наприклад терористичної діяльності, масштабного конфлікту, насильницької ізоляції чи масових заворушень, за умови, що усунути таку загрозу неможливо, не застосовуючи заходів, передбачених державою у Законі про надзвичайний стан. Цей Закон визначає основи, умови та порядок оголошення в державі стану надзвичайної ситуації, окреслює компетенцію органів управління надзвичайними ситуаціями, заходи, що підлягають виконанню, а також права, вимоги та обов'язки під час надзвичайного стану.

Головним органом влади під час надзвичайного стану є прем'єр-міністр. При цьому Закон про надзвичайний стан вимагає оголошувати такий стан за пропозицією президента або уряду. Після оголошення можливе обмеження прав та свобод в інтересах національної безпеки та громадського порядку.

Головним учасником процедур виявлення та попередження кіберзагроз, спричинених кіберрозвідкою, екстремізмом, тероризмом та спробами диверсій, є Служба внутрішньої безпеки Естонії (Kaitsepolitseiamet, KAPO). Основними функціями є розвідка та кримінальні розслідування у співпраці з національними та міжнародними партнерами[39].

---

36 https://www.riigiteataja.ee/en/eli/517122014004/consolide

37 https://www.riigiteataja.ee/akt/116122014014 https://www.riigiteataja.ee/akt/116122014014

38

39 https://www.kapo.ee/et.html

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ЕСТОНІЇ

Стратегія кібербезпеки 2008 року[40] — перший національний стратегічний документ Естонії, в якому визнано міждисциплінарну природу кібербезпеки та потребу в координації дій. Це була також одна з перших горизонтальних стратегій кібербезпеки у світі — лише після кібератак проти Естонії 2007 року кібербезпеку почали сприймати як важливу частину національної безпеки. Стратегія була розроблена Міністерством оборони на 2008–2013 роки та супроводжувалася планом впровадження.

У 2019 році Стратегію кібербезпеки було оновлено, тепер вона охоплює 2019–2022 роки[41].

Це вже третя національна стратегія кібербезпеки в Естонії, яка визначає довгострокове бачення, цілі, пріоритетні напрями дій, ролі та завдання для цієї сфери, будучи основою для планування діяльності та розподілу ресурсів.

Стратегія базується на досвіді, отриманому протягом двох попередніх періодів — реалізації стратегій на 2008–2013 та 2014–2017 рр. Як горизонтальна стратегія вона охоплює всі заінтересовані сторони в Естонії: державний сектор (як цивільний, так і оборонний), постачальників основних послуг, підприємців різних галузей та наукових працівників. Метою цього документу є узгодження та створення умов для здійснення всебічної, систематичної та всеосяжної галузевої політики.

Стратегія кібербезпеки Європейського Союзу (ЄС) 2013 року[42] визначає національну систему кібербезпеки (призначення національних компетентних органів, створення національних груп реагування на інциденти, розробку національної стратегії кібербезпеки); Директива ЄС про безпеку мереж та інформаційних систем 2016 року[43] встановлює ці заходи як юридичне зобов'язання.

Сьогодні кібербезпека повсюдно визнана невіддільним складником функціонування держави, економіки, сфери внутрішньої та зовнішньої безпеки. Основними викликами в царині ідентифікації та управління ризиками є прискорення, диверсифікація та значною мірою непередбачувана цифровізація. Крім того, естонське суспільство сьогодні недостатньо готове до боротьби з наявними кіберзагрозами — приватний і державний сектор в основному не знають про ризики та потреби, зокрема на рівні керівництва.

---

40 https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf

41 https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf

42 http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

43 http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Цифрові технології зараз відіграють настільки засадничу роль в естонському суспільстві, що неможливо подолати всі ризики за допомогою єдиного документа планування. Принципи кібербезпеки вже частково інтегровані в процеси галузевого планування. Однак задля підтримки й розвитку сталого цифрового середовища також потрібна цілеспрямована міжсекторальна співпраця. Це можна забезпечити тільки за допомогою потужної та узгодженої стратегії. Крім того, стратегія кібербезпеки відіграє роль інструмента комунікації та підвищення обізнаності на рівні ухвалення політичних рішень, посилення державно-приватного партнерства та посилення участі Естонії в міжнародній взаємодії.

Стратегія кібербезпеки підготовлена в рамках послідовного процесу взаємодії з Естонською цифровою програмою 2020 року. Досвід Естонії показує, що в успішному цифровому суспільстві та забезпечення кібербезпеки мають бути стратегічним цілим. Роль кібербезпеки в інформаційному суспільстві — забезпечити умови для ефективного та безпечного використання можливостей, пропонованих ІКТ.

Цілі та ключові показники стратегії кібербезпеки заплановані на чотири роки, проміжний перегляд має відбутися із завершенням поточної цифрової програми у 2020 році.

НАПРЯМИ ДІЙ У СФЕРІ КІБЕРБЕЗПЕКИ

Естонська стратегія виділяє три напрями активностей у сфері кібербезпеки — запобігання, захист і розвиток.

На наступні три роки заплановано такі заходи:

- розробка нових сервісів та баз даних за принципами безпеки та конфіденційності. Декларується відмова від застарілих платформ та розвиток спроможності централізованих консультацій щодо архітектури безпеки;
- орієнтація на ризик-орієнтований підхід до організації інформаційної та мережевої безпеки Естонії та дотримання і широке застосування найкращих міжнародних стандартів і практик;
- збільшення охоплення автоматизованого моніторингу вторгнень у мережу, розширення моніторингу для приватних мереж та, в результаті, отримання вичерпної картини ситуації у співпраці з усіма зацікавленими сторонами;
- забезпечення безпеки основних послуг, тестування безпеки інформаційних систем, що лежать в основі найважливіших баз даних, та постійне управління цифровими взаємозалежностями й транскордонними залежностями систем;
- визнання кібербезпеки спільною відповідальністю всіх суб'єктів, що беруть участь у кіберпросторі;

- посилення інституційної складової з метою забезпечення для держави можливості зробити більше з наявними ресурсами після проведення аудиту можливостей у сфері кібербезпеки та розробки відповідної організаційної структури;
- перетворення кібербезпеки на один із компонентів комплексного підходу до національної оборони. Для цього передбачено інтеграцію кібербезпеки в документи планування у сфері національної безпеки (національний план розвитку оборони та план діяльності національної оборони) та регулярні спільні навчання з постачальниками життєво важливих послуг, вищим політичним керівництвом та національними організаціями оборони;
- підтримка активної та згуртованої спільноти кібербезпеки. Для цього пропонуються інформаційні заходи, організацію спільних навчань та залучення приватного сектора й академічної спільноти до розробки законодавчих процесів та стратегічного планування;
- розвиток потенціалу для кібероперацій, подальший розвиток кіберкомандування сил оборони, можливостей відвернення кібератак. Просування ідеї «кіберпризову», в рамках якого місцем проходження служби можна обрати IT-сектор, а не збройні сили;
- запровадження заходів із боротьби з кіберзлочинністю. Для цього буде створено основу для ефективного міжвідомчого співробітництва та обміну інформацією, навчання операторів даних, сприяння прямим контактам між операторами даних та міжнародними експертами, підвищення спроможності правоохоронних органів;
- забезпечення безпеки критичних баз даних та передачі даних про їх стан. Для цього буде втілено концепцію державної комунікації та забезпечено резервне копіювання («відзеркалення») критичних баз даних у «посольствах даних», розташованих за межами Естонії. Визначення терміну «посольство даних» можна знайти в угоді між Естонією та Люксембургом про розміщення даних та інформаційних систем44;
- посилення практичної щоденної співпраці з міжнародними стратегічними партнерами та союзниками;
- розвиток експорту IT-фахівців, на підтримку якого кібербезпека розглядатиметься як складник розширених IT-досліджень, а до університетів висуватимуться очікування щодо підготовки фахівців;
- підтримка ефективної співпраці між державними, академічними інституціями та ключовими партнерами з приватного сектору. З цією метою планується запуск кластера, який сприятиме як внутрішньому, так і міжнародному співробітництву;
- забезпечення зростання сфери кібербезпеки як економічного сектора шляхом підтримання інновацій та розвитку продуктів, посилення дипломатичної підтримки маркетингової діяльності;

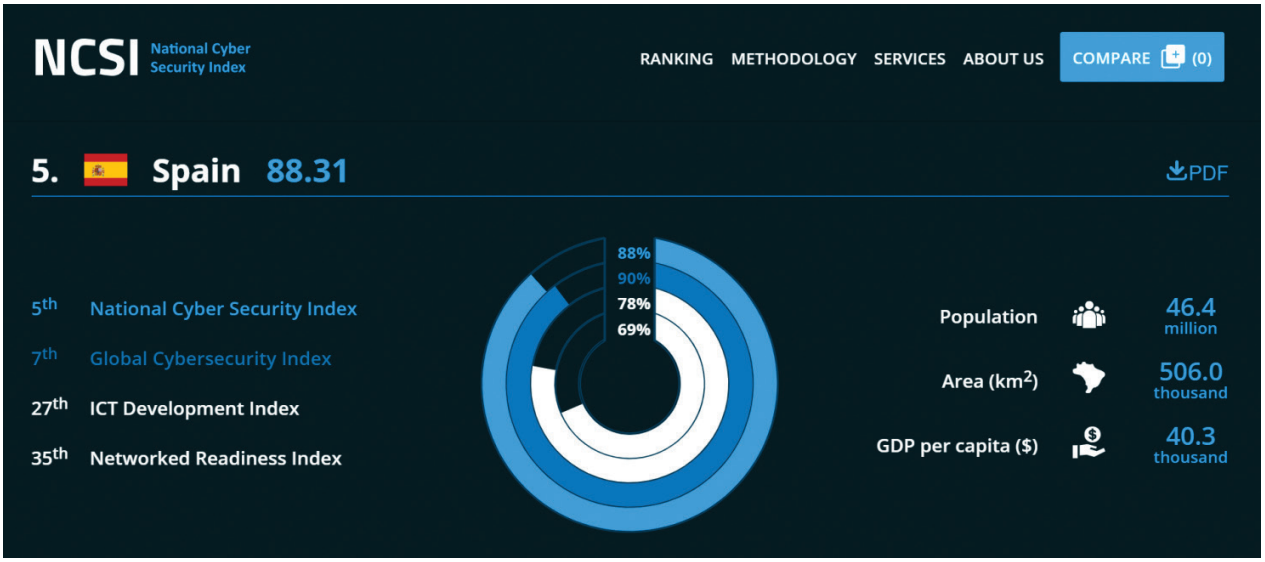
44 https://www.riigiteataja.ee/akt / 228032018002

- створення плану досліджень та розробок для кіберсектору та формування механізму досліджень і розробок, що виконуються університетами та компаніями, зокрема організація заходів підтримки компаній та фінансування освітніх проєктів і стипендій;
- постійний аналіз майбутніх тенденцій та ризиків, забезпечення швидкого реагування на нові виклики та загрози;
- сприяння конкурентній та сталій кіберспроможності країн-партнерів шляхом поширення досвіду Естонії в рамках ЄС та міжнародних проєктів.

Для реалізації у Стратегії бачення знадобляться:

- достатні компетенції, людські ресурси та фінансування;
- інтеграція кібербезпеки в усі сфери та ключові процеси планування;
- адміністрування складних проєктів та мінімізація бюрократії у державному й приватному секторі, забезпечені зав допомогою правових інструментів та заходів державного управління.

ІСПАНІЯ



Сучасне суспільство має адаптуватися до у цифрової сфери, яка потребує перегляду і постійного оновлення регуляторної бази. Державні інституції дедалі активніше й ширше використовують нові технології та комунікаційні мережі. Це вимагає правової бази, яка гарантувала б захист інтересів суспільства, зокрема громадську безпеку, забезпечувала адекватне надання публічних послуг. Разом із тим адміністрування цифрової сфери має відбуватися в рамках закону й для законних цілей, не завдаючи шкоди правам і свободам громадян.

Стратегічні питання громадської безпеки регулюються Законом про національну безпеку[45] від 28 вересня 2015 року, який визначає ризики, пов'язані з новими технологіями, як один із основних викликів сучасного суспільства.

45 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389

Законом про національну безпеку (стаття 20) визначено структуру системи національної безпеки, яка являє собою сукупність органів, агентств, ресурсів та процедур. Завдяки цій інтегрованій структурі компетентні органи у справах національної безпеки мають змогу здійснювати свої функції.

Базові компоненти, діючи в рамках власних структур та процедур, інтегруються в систему національної безпеки на основі механізмів зв'язку та координації, визначених Радою національної безпеки,. У разі потреби певні завдання можуть бути покладені на інші організації державної або приватної форми власності.

Система національної безпеки[46] відповідає за оцінку чинників та обставин, які можуть впливати на національну безпеку, збір та аналіз інформації, необхідної для ухвалення рішень у контексті реагування на кризові ситуації, окреслені цим законом, виявлення потреб та розробки відповідних заходів, координації зусиль усього спектру державних інституцій, що в результаті гарантуватиме безперебійну роботу ресурсів Системи.

Система національної безпеки складається з:

- Прем'єр-міністра уряду, якому допомагає Рада національної безпеки, що керує Системою;
- Департаменту національної безпеки, який виконує функції технічного секретаріату та постійного робочого органу Ради національної безпеки та органів його підтримки, а також інші функції, передбачені чинними положеннями;
- Органів підтримки національної безпеки, визначених спеціалізованих комітетів, що здійснюють функції, покладені на них Радою національної безпеки, у сферах, передбачених Стратегією національної безпеки, або в обставинах необхідності антикризового управління.

Система національної безпеки має бути у постійному регуляторному розвитку, узгодженому з урядовими органами, регулюванням органів координації та підтримкою Департаменту національної безпеки.

Механізм постійного зв'язку та координації всіх державних органів необхідний для того, щоб система національної безпеки могла здійснювати свої функції та виконувати свої цілі без шкоди для положень про управління кризами, що містяться у розділі III Закону про національну безпеку. Перша національна стратегія кібербезпеки Іспанії була затверджена в 2013 році. Документ містив директиви та загальні напрями дій для вирішення проблеми вразливості країни у кіберпросторі.

Стратегія національної безпеки 2017 року, затверджена Королівським указом №1008/2017 від 01.12.2017 р., визначає кіберзагрози та шпигунство як загрози, що підривають національну безпеку, і, відповідно, виділяє кібербезпеку як один із напрямів пріоритетних дій.

46 https://www.dsn.gob.es/en/sistema-seguridad-nacional

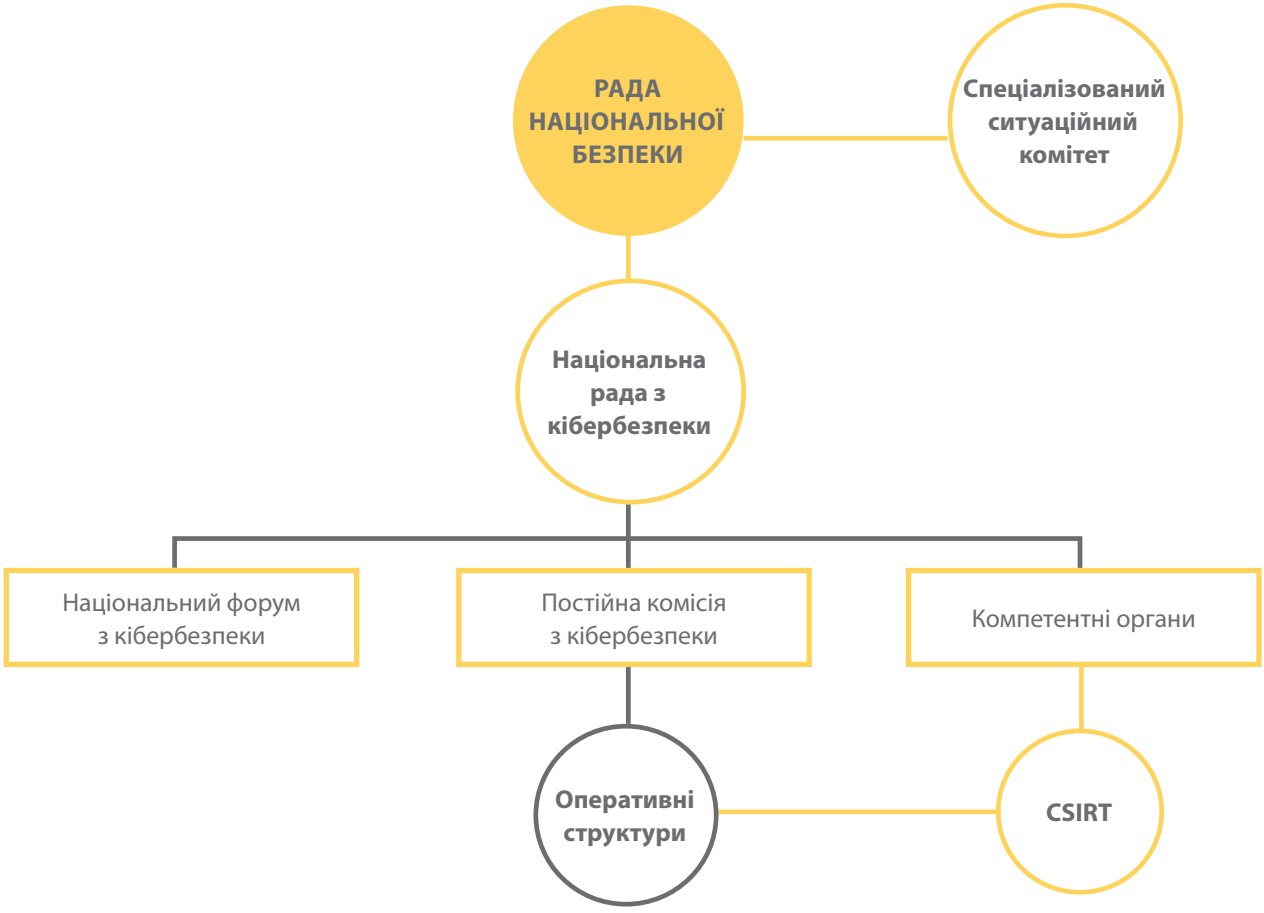
Технологічний розвиток тягне за собою сильніший вплив нових загроз, особливо пов'язаних із кіберпростором, таких як крадіжка даних та інформації, злом мобільних пристроїв та промислових систем або кібератаки проти критичної інфраструктури. Нинішній мережевий зв'язок посилює вразливості системи суспільної безпеки та вимагає кращого захисту мереж і систем, а також приватності громадянина та його цифрових прав.

Серед основних викликів, спричинених новими технологіями в контексті суспільної безпеки, — дезінформаційна діяльність, втручання в процеси політичної участі громадян та шпигунство. У рамках цих правопорушень зловмисники використовують переваги інформаційних технологій для доступу до величезних обсягів інформації та конфіденційних даних.

У розвиток Стратегії національної безпеки було ухвалено Національну стратегію кібербезпеки 2019 року[47], де окреслено нове розуміння кібербезпеки в рамках політики національної безпеки в Іспанії.

Крім того, у Стратегії закріплено модель управління національною кібербезпекою.

КІБЕРБЕЗПЕКА В СИСТЕМІ УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ ІСПАНІЇ **Рисунок 1**



47 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

На даний момент процес цифрової трансформації в уряді вже набрав обертів і відіграє вирішальну роль. Електронне урядування посилює залежність від інформаційних технологій та розширює можливе поле атак, збільшуючи ризик використання кіберпростору для здійснення незаконної діяльності, яка впливає на громадську безпеку та приватне життя громадян.

СУБ'ЄКТИ КІБЕРБЕЗПЕКИ

Національна рада з кібербезпеки надає очолюваній прем'єр-міністром Раді національної безпеки підтримку й допомогу в спрямуванні та координації політики національної безпеки з питань кібербезпеки та сприяючи координації й співпраці між громадськістю і владою та між державними органами й приватним сектором.

Департамент національної безпеки як технічний секретаріат і постійний робочий орган Ради національної безпеки діє відповідно до покладених на нього обов'язків та завдань, зокрема щодо управління кризовими ситуаціями та виконання положень закону про національну безпеку. Рада національної безпеки через Департамент національної безпеки здійснює функцію зв'язку для забезпечення транскордонної співпраці іспанських компетентних органів із компетентними органами інших держав — членів Європейського Союзу, а також із групою співпраці та мережею SCIRT.

Спеціалізований ситуаційний комітет за підтримки Ситуаційного центру Департаменту національної безпеки керує кризовими ситуаціями в галузі кібербезпеки, які за своєю суттю або масштабами виходять за межі засобів реагування на звичайні ситуації.

Національний криптологічний центр (CCN) — це організація в структурі Національного центру розвідки (CNI), створена в 2002 році для забезпечення безпеки ІКТ в різних органах державного управління та безпеки для систем, які обробляють, зберігають або надсилають секретну інформацію.

CCN-CERT — це команда реагування на інциденти в галузі кібербезпеки Національного криптологічного центру (CCN), підзвітна Іспанському національному центру розвідки (CNI). Ця служба була створена 2006 року як іспанський урядовий CERT, а її функції перераховані в Законі про CNI №11/2002, в RD 421/2004, що регулює роботу CCN, та в RD 3/2010 від 08.01.2010 р. , що регулює схему національної безпеки. Відповідно до цього регламенту, CCN-CERT забезпечує захист від кібератак на визначені (внесені до відповідного реєстру) системи, що належать державним адміністраціям та компаніям і організаціям, які мають стратегічне значення (важливі для іспанської безпеки та економіки).

Національний центр захисту інфраструктури та кібербезпеки (CNPIC) — орган, відповідальний за сприяння всім діям щодо захисту критичної інфраструктури, за які на національному рівні відповідає Державний секретаріат з питань безпеки, а також координацію цих дій і нагляд за їх виконанням. Основна мета інституції — координувати механізми, необхідні для гарантування безпеки інфраструктури, що надає важливі для суспільства послуги, і спонукати

всіх учасників Системи діяти відповідно до сфер компетенції. За допомогою всіх цих зусиль CNPIC просуває модель безпеки, засновану на взаємній довірі, підтримує державно-приватне партнерство, яке дасть змогу мінімізувати вразливості критичної інфраструктури Іспанії.

Іспанський національний інститут кібербезпеки (INCIBE) — організація, яка підпорядкована Міністерству економіки та цифрових трансформацій Іспанії, Державному секретарю з питань цифрової трансформації та штучного інтелекту і є базовою установою у сфері розвитку кібербезпеки та довіри у цифровому суспільстві – серед широких кіл громадськості, у сегментах RedIRIS (іспанської академічної та дослідницької мережі), а також бізнесу, особливо секторів, що мають стратегічне значення. Як центр передового досвіду INCIBE створений у 2006 році як Національний інститут комунікаційних технологій (INTECO), місія якого полягала у просуванні та розвитку інноваційних проектів у секторі Інформаційно-комунікаційних технологій, та у 2014 році його діяльність була уточнена іспанським урядом та зосереджена над розвитком кібербезпеки як інструмента суспільної трансформації та формування нових галузей інновацій. Задля виконання цієї місії INCIBE очолює низку ініціатив, спрямованих на забезпечення кібербезпеки як на національному, так і на міжнародному рівні й охоплює у своїй діяльності дослідження, надання послуг та співпрацю з відповідними суб'єктами.

INCIBE-CERT — центр реагування на інциденти в галузі безпеки для громадян та приватних компаній Іспанії, яким керує Іспанський національний інститут кібербезпеки (INCIBE). У процесі управління інцидентами, спрямованими проти операторів критичної інфраструктури у приватного секторі, керівництво INCIBE-CERT спільно здійснюють INCIBE та CNPIC (Національний центр захисту інфраструктури та кібербезпеки Міністерства внутрішніх справ).

РЕАЛІЗАЦІЯ КІБЕРЗАХИСТУ

Об'єднане командування з кіберзахисту (Міністерство оборони) відповідає за планування та виконання дій, пов'язаних із кіберзахистом у мережах, інформаційних системах та телекомунікаціях Міністерства оборони чи інших органів, які беруть участь у процесі кіберзахисту, а також забезпечує адекватну реакцію на загрози в кіберпросторі. Підрозділ ESP-DEF-CERT виконує функцію CERT у структурі Міністерства оборони, а також в інших мережах та системах, які спеціально їй передані під нагляд цього органу та які впливають на національну оборону. ESP-DEF-CERT співпрацює з CCN-CERT та INCIBE-CERT у ситуаціях, коли потрібна підтримка операторів основних послуг, зокрема тих, які впливають на національну оборону і визначені в нормативних актах.

Державно-приватне партнерство реалізується через дві організації — асоціацію «Іспанський кластер інновацій у кібербезпеці»[48] (AEI Ciberseguridad y Tecnologías Avanzadas) та Іспанську технологічну платформу з промислової безпеки (PESI)[49].

48 https://www.aeiciberseguridad.es/index.php/About_AEI_1

49 http://www.pesi-seguridadindustrial.org/es

Іспанський кластер інновацій в кібербезпеці (AEI)

Іспанський кластер інновацій в кібербезпеці (AEI Ciberseguridad y Tecnologías Avanzadas) об'єднує компанії, науково-дослідні центри, університети, державні та приватні організації, зацікавлені у просуванні нових технологій, промисловий сектор та інші заінтересовані сторони, що бажають зробити внесок у реалізацію цілей Асоціації в царині технологій безпеки на національному та міжнародному рівнях.

AEI виконує низку функцій:

1. Сприяння відкриттю бізнесів та впровадженню технологічних послуг, налагодження регулярного діалогу з науково-дослідними установами, компаніями та фахівцями на користь галузі. Надання своїм партнерам загальних послуг з питань досліджень і розробок, розвитку технологій науково-дослідної та технологічної розробки та запуску бізнесів.
2. Сприяння співпраці та стимулювання нових стратегій підвищення конкурентоспроможності в царині безпеки інформації та безпекових технологій на національному й міжнародному рівнях.
3. Заохочення взаємообміну досвідом та ідеями в процесі впровадження інноваційних ІКТ-проєктів з метою підвищення конкурентоспроможності іспанських компаній як на національному, так і на міжнародному рівнях.
4. Сприяння спеціалізованому навчанню серед професіоналів ІКТ-галузі та поширенню нових технологій у галузі, особливо в рамках Асоціації.
5. Підвищення серед органів управління, державних і приватних організацій зацікавленості й обізнаності щодо сектора нових технологій, усвідомлення його важливості для економічного розвитку, тобто ефективності управління компаніями, конкурентоспроможності та якості послуг.

Іспанська технологічна платформа з промислової безпеки (PESI)

Іспанська технологічна платформа з промислової безпеки (PESI) створена в жовтні 2005 року як асоціація, що об'єднує галузь і підтримує різні установи її метою є залучення компаній, технологічних центрів та університетів до програм досліджень і технологічних розробок у галузі промислової безпеки на європейському чи національному рівні, а також визначення власних потреб у контексті Порядку денного стратегічних досліджень[50], структури управління та оперативного розгортання.

50 https://aeneas-office.org/wp-content/uploads/2020/07/ECS-SRA2020_L.pdf

Основні завдання PESI — вироблення загального бачення промислової безпеки, що дає змогу стимулювати науково-дослідну діяльність, технологічні розробки та інновації (R + D +). У своїй діяльності охоплює такі сфери: безпека продуктів та споруд; безпека праці; екологічна безпека; безпека підприємств.

Також PESI здійснює підготовку стратегічних програм та науково-дослідних проектів у галузі промислової безпеки як на національному, так і на європейському рівнях, здійснює співробітництво з керівниками з безпеки важливих іспанських та європейських компаній, беручи участь у пошуку спільних рішень, є частиною Європейської технологічної платформи для промислової безпеки (ETPIS).

Державне фінансування здійснюється через дві програми — INCIBE та RENIC.

Правову основу для організації захисту критичної інфраструктури в Іспанії становлять два закони — Закон про встановлення заходів щодо захисту критичної інфраструктури[51] № 8/2011 від 28.04.2011 р. та Королівський декрет №12/2018 від 07.09.2017 р. про мережеву безпеку та інформаційні системи[52], який імплементує Директиву (ЄС) 2016/1148 Європейського парламенту та Ради від 6 липня 2016 року та доповнює закон 2011 року.

Стратегічні заходи із забезпечення та підтримки високого рівня безпеки мереж та інформаційних систем окреслені у Національній стратегії кібербезпеки, узгодженій зі Стратегією національної безпеки.

Компетентні органи:

- для основних операторів послуг: Секретаріат державної безпеки, Міністерство внутрішніх справ, а саме його структурна одиниця Національний центр захисту інфраструктури та кібербезпеки (CNPIC), а у випадку, якщо оператори не є критичними, — відповідне галузеве положення;
- для постачальників цифрових послуг: Державний секретар з питань цифрового прогресу Міністерства економіки та бізнесу;
- для операторів, що надають важливі послуги, та постачальників цифрових послуг, які не є критичними операторами та які підпадають під дію Закону про правовий режим державного сектору №40/2015 від 01.10.2015 р.: Міністерство оборони, а саме його структурна одиниця Національний криптологічний центр.

Рада національної безпеки через свій спеціалізований комітет з питань кібербезпеки створює необхідні механізми для координації дій компетентних органів.

51 https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

52 https://www.boe.es/buscar/doc.php?id=BOE-A-2018-12257

Компетентні органи виконують такі функції:

- контролюють виконання основними операторами та постачальниками цифрових послуг зобов'язань, визначених у розділу VI закону, а саме: основні оператори послуг та постачальники цифрових послуг мають вживати відповідних та доцільних технічних і організаційних заходів щодо управління ризиками для безпеки мереж та інформаційних систем, що використовуються для надання послуг відповідно до цього королівського декрету-закону, вживати заходів для запобігання та мінімізації впливу інцидентів, повідомляти про інциденти тощо;
- своєчасно створюють канали зв'язку з операторами, що надають важливі послуги, та з постачальниками цифрових послуг, які, у разі необхідності, регулюються законодавством;
- узгоджують із CSIRT протоколи доцільних дій та затверджують їх;
- отримують повідомлення про випадки, які можуть справити суттєвий руйнівний вплив на критичні послуги, які передаються в рамках цього закону через повідомлення CSIRT;
- інформують єдиний контактний пункт про інциденти;
- інформують, де це доречно, громадськість про певні інциденти, коли розповсюдження такої інформації необхідне для уникнення інциденту або управління наявною кризою;
- співпрацюють в рамках закону з компетентними органами у галузі захисту персональних даних, громадської безпеки, безпеки громадян та національної безпеки, а також із відповідними галузевими органами;
- встановлюють конкретні зобов'язання щодо забезпечення безпеки мереж та інформаційних систем та щодо інформування про інциденти, видають технічні та керівні вказівки із деталізацією змісту таких зобов'язань;
- здійснюють санкційні повноваження у випадках, передбачених законом;
- сприяють використанню стандартів та технічних умов;
- співпрацюють із компетентними органами інших держав — членів Європейського Союзу у виявленні основних операторів послуг серед суб'єктів, які пропонують такі послуги у кількох державах-членах;
- повідомляють єдиному контактному пункту про інциденти, які можуть зачіпати інші держави-члени.

Законом передбачено кілька груп з реагування на інциденти в галузі комп'ютерної безпеки (CSIRT) для забезпечення мережевої безпеки та безпеки інформаційних систем.

Для операторів основних послуг:

- CCN-CERT Національного криптологічного центру, якому відповідає співтовариство, що складається з суб'єктів загальної сфери застосування Закону 40/2015 від 1 жовтня.
- INCIBE-CERT, Національний інститут кібербезпеки Іспанії, якому відповідає інформаційна спільнота, створена тими суб'єктами, які не включені до загальної сфери застосування Закону 40/2015 від 1 жовтня.
- INCIBE-CERT спільно керуватиме INCIBE та CNPIC у всьому, що стосується управління інцидентами, які впливають на операторів критичної інфраструктури.
- ESPDEF-CERT Міністерства оборони, яке співпрацюватиме з CCN-CERT та INCIBE-CERT у ситуаціях, які потребують підтримки операторів основних послуг і, обов'язково, операторів, які впливають на Національну оборону, що визначається окремим регламентом.

Для постачальників цифрових послуг, які не входять до інформаційного співтовариства CCN-CERT:

- INCIBE-CERT.
- INCIBE-CERT також визначений як загальний орган реагування на інциденти, спрямовані проти громадян, приватних компаній та інших організацій, що не належать до груп операторів основних послуг та постачальників цифрових послуг.

Реагуючи на інциденти й здійснюючи управління ризиками для безпеки, що належать до сфери їхньої компетенції, довідкові CSIRT координують дії між собою та з рештою національних і міжнародних CSIRT. У визначених нормативними актами особливо важких випадках, що вимагають вищого рівня координації, ніж у звичайних ситуаціях, технічне реагування з боку CSIRT координує на національному рівні CCN-CERT.

Коли діяльність, яку вони здійснюють, може будь-яким чином вплинути на оператора основних послуг, CSIRT узгоджуватиме визначений законом спосіб інформування із Міністерством внутрішніх справ через Національний центр захисту інфраструктури та кібербезпеки (CNPIC).

CSIRT співпрацює з приватним сектором, стимулюючи впровадження та застосування загальних або стандартних практик і процедур управління інцидентами та ризиками, системи класифікації інцидентів, ризиків та інформації.

Рада національної безпеки через Департамент національної безпеки забезпечує зв'язок і транскордонне співробітництво компетентних органів Іспанії з компетентними органами інших держав — членів Європейського Союзу, а також із групою та мережею співробітництва CSIRT.

Компетентні органи, довідкові CSIRT та єдиний контактний пункт за необхідності консультуються з уповноваженими органами в галузі національної безпеки, громадської безпеки, безпеки громадян та захисту персональних даних та співпрацюють з ними в здійсненні відповідних функцій. Також у разі потреби консультуються і співпрацюють з органами, наділеними аналогічними повноваженнями в кожному з секторів, що належать до сфери застосування цього закону.

Коли в інцидентах, про які надійшли повідомлення, присутні ознаки злочину, компетентні органи та довідкові CSIRT якнайдетальніше інформують про це Державного секретаря з питань безпеки через Національний центр захисту інфраструктур (CNPIC) Міністерства внутрішніх справ[53].

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ІСПАНІЇ

У Національній стратегії кібербезпеки 2019 року окреслено нове розуміння цього питання в світлі політики національної безпеки.

Перша національна стратегія Кібербезпеки в Іспанії була затверджена в 2013 році. Документ містив директиви та загальні напрями дій із вирішення проблеми вразливості країни у кіберпросторі. Крім того, у Стратегії було наведено **модель управління національною кібербезпекою**.

Згідно з цією моделлю, починаючи з 2014 року головним стовпом у цій галузі є Національна рада з кібербезпеки, орган, що підтримує Раду національної безпеки. З часу свого першого засідання Національна рада з питань кібербезпеки взяла на себе завдання координувати національні компетентні організації, а також розробити Національний план кібербезпеки та заходи з його реалізації. Отже, Іспанія сьогодні може похвалитися спеціалізованими організаціями з кібербезпеки та міцною позицією не лише в Європі, а й у всьому світі.

53 http://www.interior.gob.es/es/el-ministerio/funciones-y-estructura/secretaria-de-estado-de-seguridad

Також було здійснено значну адаптацію правової бази. Для забезпечення подальшої трансформації системи та ефективного застосування досвіду, накопиченого за останні кілька років, у 2015 році було опубліковано модифікацію Основ національної безпеки – Директиву про національну оборону[54], що гарантують безпеку систем державного сектору. З іншого боку, з набранням чинності Королівським декретом №12/2018 від 7 вересня 2018 р. про безпеку інформаційних систем та мереж[55], який імплементує Директиву (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року щодо заходів забезпечення високого загального рівня безпеки інформаційних систем та мереж у Союзі (Директиву NIS)[56] в іспанську правову систему, здійснено важливі заходи з покращення кібербезпеки Іспанії, які розширюють сферу дії цієї Директиви з метою підвищення рівня кібербезпеки у стратегічних секторах.

Декрет-закон №36/2015 від 28 вересня 2015 р. «Про національну безпеку» сприяє розширенню повноважень уряду та визначає кібербезпеку як особливу сферу інтересів.

Безумовно, увага до кібербезпеки дала змогу модернізувати сферу національної безпеки загалом, у якій нині досягнуто значних успіхів. Необхідно зберегти цю позитивну динаміку. Стратегія національної безпеки 2017 року стала поворотним пунктом у національному стратегічному мисленні, оскільки формує окремий простір кібербезпеки й надає їй особливого статусу.

Серед іншого у Стратегії визначено таку глобальну тенденцію: цифровізація сприяє змінам, які тягнуть за собою певні наслідки для безпеки. Управління кризами, культура національної безпеки, спільний глобальний простір, технологічний розвиток та міжнародні прогнози — усе це формує для Іспанії нові стратегічні умови, у яких кібербезпека використовується як ключ до поточної та майбутньої моделі безпеки країни.

Нині поняття кібербезпеки виходить за межі захисту технологічної спадщини електронних комунікацій та охоплює політичну, економічну й соціальну сфери.

У Стратегії кібербезпеки Іспанії кіберпростір розглядається не лише як сукупність цифрових систем і дій, що них впливають, але й як стратегічний напрям комунікації, який може використовуватися для впливу на громадську думку та спосіб мислення людей, передбачаючи маніпулювання інформацією, зокрема дезінформаційні кампанії або гібридні дії. Потенційне застосування кіберпростору у дуже широкому діапазоні ситуацій, зокрема й виборчих процесах, надає цьому явищу надзвичайної складності.

Цей оновлений погляд на галузь, яка набуває дедалі ширших функцій і в якій ключовим чинником є державно-приватне партнерство, вимагає нового підходу — нової національної стратегії кібербезпеки.

54 https://www.defensa.gob.es/defensa/politicadefensa/directivadefensa/

55 https://www.boe.es/eli/es/rdl/2018/09/07/12

56 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

ГЛОБАЛЬНИЙ КІБЕРПРОСТІР

Відповідно до Стратегії кібербезпеки Іспанії, кіберпростір є спільним глобальним простором, що характеризується певною функціональністю та динамічністю. Відсутність суверенітету у кіберпросторі, слабка підпорядкованість тій чи іншій юрисдикції, простота доступу та труднощі з класифікацією (описом) дій усередині кіберпростору закладають якнайширший спектр можливостей і моделей його подальшого розвитку, створюючи також серйозні виклики для безпеки.

З одного боку, кіберпростір уможливлює універсальний зв'язок і полегшує вільне переміщення інформації, послуг та ідей. Таким чином, це сфера, що стимулює підприємництво, посилює соціально-економічний прогрес і щодня створює нові можливості у всіх галузях бізнесу. В усьому світі відбуваються безпрецедентно швидкі зміни, спричинені цифровою трансформацією виробничих процесів. Штучний інтелект, робототехніка, великі дані, блокчейн та Інтернет речей вже існують, хоча справжня трансформація суспільства ще не починалася. Її наслідки виходять за межі технології, поширюючись на нові соціальні моделі та особисті відносини й етику.

З іншого боку, цифровізація змінює стандарти безпеки та оголює перед світом серйозні проблеми. **Кіберпростір постає як поле битви, де конфіденційність інформації та даних є цінними надбаннями в середовищі, що відзначається великою геополітичною конкуренцією, реорганізацією влади та розширенням індивідуальних можливостей.** Отже, бурхливий розвиток зв'язку та підвищення залежності від мереж і систем, не кажучи вже про цифрові компоненти, об'єкти та пристрої, спричиняють уразливості й ускладнюють належний захист інформації.

Кіберпростір є не лише віртуальним середовищем — його підтримують фізичні та логічні елементи. **Пристрої, компоненти та комп'ютерні системи всередині інформаційно-комунікаційних мереж і систем можуть зазнавати пошкоджень, які перешкоджають належній роботі, та навмисних шкідливих дій, що ставлять під загрозу належну роботу критичних інфраструктур та основних послуг.**

Ці ризики поглиблюються з огляду на комерційні вимоги щодо безпеки апаратних та програмних продуктів, не кажучи вже про системи та сервіси, які ускладнюють процеси сертифікації та можуть загрожувати ланцюгу поставок.

Усі ці аспекти, а також зміцнення взаємозв'язку між системами, можуть спричинити каскадні ефекти з непередбачуваними результатами.

З огляду на важливість усеосяжного підходу й застосування не **лише міжнародного права та необов'язкових стандартів відповідальної поведінки у міждержавних відносинах, слід окремо наголосити на ролі Статуту Організації Об'єднаних Націй як еталону запобігання конфліктам, співробітництва та стабільності в кіберпросторі.**

В основу застосування цього документу, а також реалізації міжнародних договорів і угод, до яких приєдналася Іспанія, покладено принцип вибудовування довіри між сторонами.

Засадничо сталість передбачає **постійний захист конституційних та демократичних цінностей та принципів, а також захист основних прав громадян у кіберпросторі, особливо в частині їхніх персональних даних, конфіденційності, свободи вираження поглядів та доступу до правдивої, якісної інформації**.

Такий підхід вимагає розуміння мультидисциплінарного характеру кібербезпеки, що виходить за межі суто технічних аспектів. У цій сфері необхідно застосовувати принципи централізованого управління, координацію з приватним сектором задля досягнення ефективності дій, а також віднести кібербезпеку до царини національної безпеки як виключно державної компетенції.

Приватний сектор відіграє важливу роль адміністратора та власника цифрових активів, тож високий рівень кібербезпеки і навички її захисту в країні значною мірою залежить від її компаній. Це означає, що кібербезпека потребує підтримки, просування та інвестицій — так вона допоможе стимулювати конкурентоспроможність і економічне зростання, забезпечуючи надійне цифрове середовище.

Згідно зі Стратегією, Іспанія як країна має прагнути до підвищення рівня технологічної автономності, розвиваючи національну промислову базу кібербезпеки — R + D + I (research and development and innovation, дослідження, розробки та інновації), а також управління талантами у технологічній сфері. Критичним чинником залишаються людські ресурси. Адже вже наявний великий розрив між кількістю високоспеціалізованих робочих місць у галузі інформаційних технологій (особливо кібербезпеки) та наявною кількістю працівників із необхідним рівнем знань чи підготовки.

ЕВОЛЮЦІЯ КІБЕРЗАГРОЗ

Перехід від профілактичної та оборонної моделі кібербезпеки до більш стримувальних рамок узгоджується із глобальним контекстом, що демонструє більшу геополітичну обізнаність. Експерти давно визнають, що кіберпростір використовується як поле протистояння, сам по собі або в межах комплексної гібридної дії. Для забезпечення **стримування в галузі кібербезпеки як фундаментального складника дій держави необхідно здобувати й удосконалювати навички кіберзахисту**.

Кіберзагрози, що швидко еволюціонують, вимагають активніших кроків з боку кіберрозвідки. Її інтеграція в загальну систему кібербезпеки — ключовий чинник отримання знань про ситуацію та забезпечення запобігання проблемам на ранньому етапі, що включатиме прогнозування дій потенційних опонентів на основі вивчення їхніх навичок, прийомів, тактик і намірів. Крім того, необхідно заохочувати використання механізмів та засобів, що дають змогу провадити відповідні розслідування й притягати до відповідальності винних осіб.

У Стратегії зроблено акцент на необхідності більшого впливу з боку суспільства, стимулюванні культури кібербезпеки, усвідомлення громадянами своєї спільної з урядом і бізнесом відповідальності за національну кібербезпеку.

Стратегія кібербезпеки Іспанії визначає кіберзагрози як шкідливі збої чи маніпуляції, що впливають на технологічні елементи. Вони охоплюють широкий спектр дій. **Кіберзагрози характеризуються різноманітністю з точки зору як потенціалу, так і мотивації та впливають практично на всі сфери національної безпеки, такі як національна оборона, економічна безпека чи захист критичної інфраструктури; крім того, кіберзагрози мають транскордонний характер**.

Унаслідок цієї всепроникності кібербезпека комплексно охоплює всі аспекти життя й управління, зокрема публічне управління, державний та приватний сектор і суспільство в цілому, адже збої в кібезрбезпеці можуть потягнути за собою одночасні наслідки для широкого спектру царин, таких як суверенітет, основні права, оборона, економіка та технологічний розвиток.

Відповідно до цього сценарію сили захисту мають постійно розвиватись, адаптуючись до нових загроз, помножених на ефект тяжіння, викликаний високим ступенем безкарності злочинів у кіберпросторі. У той же час оборонна сфера з кожним днем розширюється і ускладнюється.

З огляду на це забезпечення безпеки в інформаційних мережах та системах вимагає вдосконалення заходів щодо запобігання, виявлення та реагування, програмування безпеки за замовчуванням на етапі проєктування. Забезпечення безпеки має бути складником розробки технологічних продуктів та послуг, їх оновлення та застосування.

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ

Цифрові технології відкривають нові види діяльності та способи ведення бізнесу, які необхідно належним чином регламентувати, оскільки вони можуть вплинути на стабільність та права й свободи, таким чином спричиняючи значні загрози та виклики для національної безпеки.

Адже ті самі характеристики, які допомагають кіберпростору стимулювати прогрес, можна використовувати в шкідливих цілях, чому надзвичайно сприяє можливість залишатися анонімним, красти особистість тощо.

Завдяки інтернет-революції держави, організовані групи, колективи й навіть окремі особи можуть досягти досі безпрецедентного рівня влади та спроможності впливати. Глобальні соціальні рухи набувають стратегічного значення, досі належним чином не оціненого.

Зловмисна чи незаконна діяльність у кіберпросторі набуває різних форм, зокрема кібершпигунства та кіберзлочинності.

Кібершпигунство — це порівняно дешевий, швидкий і менш ризикований, ніж традиційне шпигунство, метод отримання інформації враховуючи труднощі у забезпеченні набуття авторства. Найбільшими можливостями володіють в основному державні гравці (розвідувальні чи військові організації), які в основному діють із застосуванням так званих **«Розвинених сталих загроз»** (Advanced Persistent Threats, APT). За такого типу загрози супротивник має глибокі знання, а також ресурси та інфраструктуру, щоб розгортати атаки різних типів і взаємодіяти з об'єктами протягом тривалого періоду часу, адаптуючись до оборонних стратегій.

Публічні та приватні гравці, безпосередньо чи через посередників, використовують здатність розміщених в Інтернеті даних виступати інструментами дезінформації та пропаганди та проявляють великий інтерес до отримання та розвитку військових можливостей для роботи в кіберпросторі, включаючи наступальний потенціал у багатьох випадках.

Крім того, наразі дедалі більшого поширення набувають так звані **гібридні загрози, скоординовані та синхронізовані дії, свідомі атаки спрямовані на пошук системних вразливостей у демократичних державах та установах, здійснення операцій економічного тиску**.

Своєю чергою, кіберзлочини — це проблема безпеки громадян найвищого рівня, одна з найпоширеніших та найуніверсальніших загроз, жертвами якої постійно стають тисячі установ, компаній та громадян. Кіберзлочин (Cybercrime) — це незаконна діяльність у кіберпросторі, націлена на елементи, комп'ютерні системи чи будь-яку іншу власність, а планування, розвиток та ефективність кіберзлочину визначаються використанням технологічних засобів; залежно від характеру злочину, виконавця, мотивації або заподіяної шкоди такі дії можуть кваліфікуватися як **кібертероризм, кіберзлочин чи хактивізм**.

Використання нових методів та інструментів для здійснення фінансових і економічних операцій, зокрема криптовалюти, для забезпечення незаконного обігу та торгівлі товарами, надання послуг або вимагання, шахрайства та підробки негрошових платіжних засобів є серйозною проблемою для безпеки, адже ці методи та інструменти неоднозначні та складні, їх можна використовувати для відмивання грошей та ухилення від сплати податків, вони слугують джерелом доходу для організованої злочинності; отже, вони використовуються для інших видів незаконної діяльності, такі як фінансування тероризму, що ускладнює їх моніторинг.

Кіберзлочинці діють у рамках організованої злочинності й постійно відкривають нові методи побудови вигідних низькоризикових бізнес-моделей, користуючись тим, що їхні дії важко відстежити.

Терористичні угрупування намагаються максимально використати вразливості в кіберпросторі для кібератак чи дій, спрямованих на радикалізацію окремих осіб та груп, залучення фінансування, розповсюдження прийомів та інструментів для здійснення терористичного нападу, а також для набору кадрів чи пропаганди. Із тероризмом пов'язана й загроза для критичної інфраструктури — шкідливе використання мереж із наміром зруйнувати всю систему загальнодоступних послуг за ефектом доміно.

Хактивістські угрупування здійснюють кібератаки з ідеологічних причин, а іноді, максимально використовуючи продукти, послуги та інструменти, доступні в кіберпросторі, прагнуть організувати атаки з великим медіа- чи соціальним впливом.

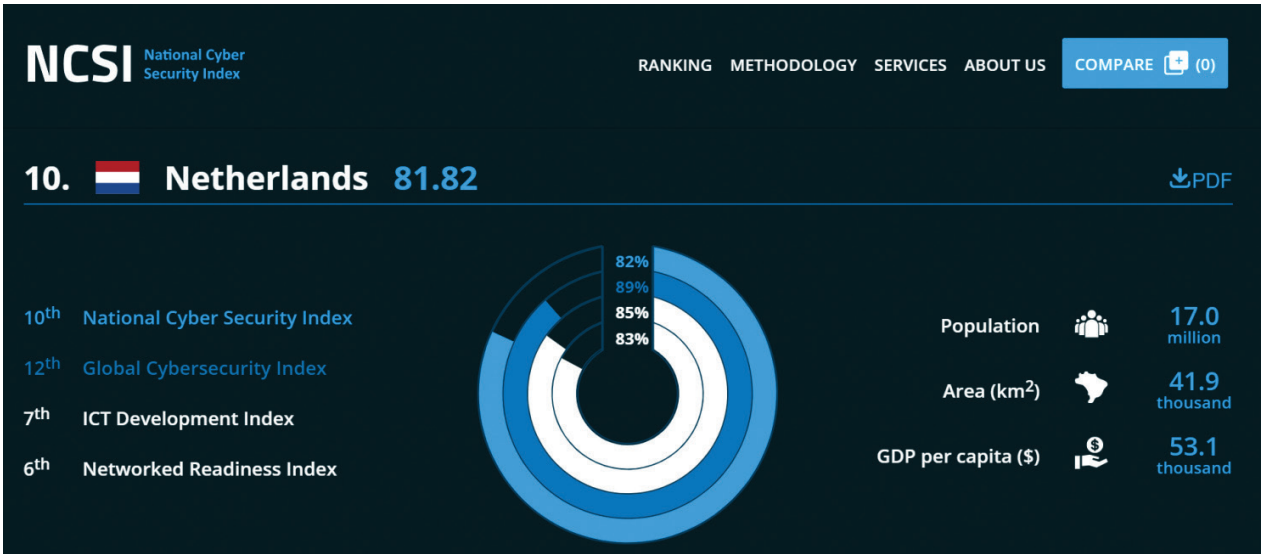
Ще одну загрозу становить зростання чисельності **організацій, які надають у кіберпросторі послуги заподіяння шкоди конкурентам та їхнім технологічним і людським ресурсам. Крім того, не слід забувати про загрози, спричинені відсутністю культури кібербезпеки**.

Цифрова інформація стала активом з високою доданою вартістю. Зловмисне використання персональних даних та дезінформаційні кампанії мають високий потенціал для дестабілізації суспільства.

Аналіз персональних даних у мережі Інтернет застосовний для широкого кола цілей — від соціологічних досліджень до рекламних кампаній. Але використання вразливостей персональних даних — це порушення їх безпеки, що впливає на приватність, а також цілісність та конфіденційність інформації.

У межах дезінформаційних кампаній для впливу на громадську думку застосовуються різні елементи, наприклад фейкові новини,. Інтернет та соціальні медіа збільшують обсяги надаваної інформації та посилюють її вплив, причому в дезінформаційних цілях можуть використовуватися навіть міжнародні організації, держави, політичні ініціативи, громадські активісти чи демократичні виборчі процеси.

НІДЕРЛАНДИ



Ролі та обов'язки із забезпечення національної кібербезпеки в Нідерландах розподілені між численними суб'єктами, зокрема міністерствами та приватними гравцями. Так, новий Закон про безпеку мережевих та інформаційних систем, що імплементує Директиву (ЄС) 2016/1148 Європейського парламенту та Ради від 6 липня 2016 року, визначає шість компетентних органів у цій царині — Міністерство юстиції та безпеки, Міністерство економічних питань та клімату, Міністерство інфраструктури та водного господарства, Міністерство з питань медичної допомоги, Національний банк Нідерландів (De Nederlandsche Bank NV). Також до відповідальних органів належать міністерства внутрішніх справ та відносин Королівства; оборони; закордонних справ; освіти, культури та науки.

Деякі завдання та відповідальність покладені на правоохоронні органи та органи внутрішньої безпеки (Службу поліції, Державну прокуратуру, Фіскальну розвідку та слідство, Інспекцію юстиції та безпеки, Службу розвідки та безпеки), а також Агентство захисту персональних даних, галузеві регуляторні органи (наприклад, у сфері телекомунікацій). Регіональні та місцеві органи влади також залучені до процесу забезпечення кібербезпеки.

У приватному секторі основна частина обов'язків, визначених у національній стратегії кібербезпеки 2014 року[57], покладається на фінансовий сектор (комерційні банки, Нідерландську банківську асоціацію (NVB) і платформи електронної комерції) та постачальників життєво важливих послуг. Для виконання певних положень необхідне залучення до процесу бізнес-спільноти.

У новій стратегії кібербезпеки Нідерландів 2018 року зазначено, що жодні нові додаткові органи створюватися не будуть. Інституційно кібербезпеку забезпечуватимуть учасники, які вже беруть участь у процесі.

СУБ'ЄКТИ КІБЕРБЕЗПЕКИ

20 квітня 2018 року міністр юстиції та безпеки Нідерландів Ферд Грапперхаус представив урядовий Національний порядок кібербезпеки (NCSA)[58]. Порядок денний містить сім комплексних амбітних цілей, що сприятимуть встановленню в Нідерландах безпечного цифрового середовища. Нідерланди мають усі переваги для використання економічних та соціальних можливостей цифровізації. Водночас вразливості та загрози у цифровій сфері зростають. Отже, безпека в цифровій галузі є головним пріоритетом для уряду. Ось чому уряд взяв на себе зобов'язання щодо додаткових структурних інвестицій у кібербезпеку. NCSA закладає підвалини для наступного кроку, необхідного для забезпечення кібербезпеки. Окреслено механізми спільного керівництва й колективного здійснення заходів. Це посилює одночасний вплив публічних та приватних дій на кібербезпеку.

Рада з питань кібербезпеки (CSR)

Рада з питань кібербезпеки (CSR)[59] — незалежний національний дорадчий орган уряду Нідерландів та бізнес-спільноти, до складу якого входять високопосадовці громадських та приватних організацій і наукових кіл. CSR на стратегічному рівні докладає зусилля до посилення кібербезпеки в Нідерландах.

Унікальний склад ради дає можливість стратегічно й усебічно розглядати пріоритети, вразливості та інциденти, виробляти інтегроване бачення можливостей та загроз. CSR налагоджує співпрацю з аналогічними органами в інших країнах і заохочує створення подібних інституцій у тих країнах, де їх ще немає.

57 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/bfe0dbf357af4f44b67d40b7cefa3f6a/file_en

58 https://english.ncsc.nl/topics/national-cybersecurity-agenda

59 https://www.cybersecurityraad.nl/005_OverdeCSR/index.aspx

Рада прагне забезпечити всеосяжне представлення всіх аспектів у сфері кібербезпеки. Тому склад органу формується за принципом 7-7-4: сім представників приватного сектора, сім — державного та чотири представники наукової спільноти.

CSR очолюють два співголови: Пітер-Яап Ольберсберг від імені державного сектора та Ганс де Йонг від імені приватного сектора (VNO-NCW). Операційну діяльність Ради забезпечує секретаріат.

Завдання CSR:

- надання рекомендацій державним і приватним інституціям;
- консультування щодо реалізації національної стратегії кібербезпеки;
- участь у Національній програмі досліджень кібербезпеки;
- консультування щодо антикризового управління в Нідерландах під час масштабних кіберінцидентів.

Крім того, члени CSR проводять публічні дискусії, щоб привернути увагу до кібербезпеки на стратегічному рівні, адже кібербезпекою в компаніях мають перейматися не лише IT-відділи — кібербезпека є стратегічним питанням у контексті безперервності функціонування бізнесу.

Рада з питань кібербезпеки здійснює планування, дає прогнози щодо ситуації з кібербезпекою в Нідерландах і рекомендації щодо нових технологічних розробок та наслідків для кібербезпеки.

Рада з питань кібербезпеки є гарним прикладом державно-приватного партнерства.

Національний центр кібербезпеки (NCSC)

Крім Ради з питань кібербезпеки, існує також Національний центр кібербезпеки (NCSC)[60] — підпорядкований міністерсту юстиції та безпеки, який працює над формуванням комплексного підходу до кібербезпеки. Центр сформовано на основі нідерландської урядової команди реагування на комп'ютерні надзвичайні ситуації (GovCert), яка з 1 серпня 2011 року діяла в складі Національного координаційного органу з питань безпеки та протидії тероризму (NCTV).

Центр має у своєму розпорядженні тактичні та оперативні знання й досвід уряду та бізнесу. Це допомагає сформувати чіткіше розуміння загроз і ефективніше боротися з інцидентами та ухвалювати рішення в надзвичайних ситуаціях, пов'язаних із цифровою безпекою.

NCSC активно співпрацює з державним та приватним секторами, зокрема з науковими колами. Організація зосереджує увагу на суспільних інтересах, тож переважно у своїй діяльності фокусується на життєво важливих галузях — енергетиці, телекомунікаціях та фінансовому секторі.

60 https://english.ncsc.nl/about-the-ncsc

Закон про безпеку мережевих та інформаційних систем[61] (WBNI) регулює статутні завдання NCSC у галузі кібербезпеки. Організації в життєво важливих секторах зобов'язані повідомляти NCSC про серйозні випадки у галузі цифрової безпеки.

Закон про безпеку мережевих та інформаційних систем спрямований на підвищення цифрової стійкості Нідерландів, обмеження наслідків кіберінцидентів і, таким чином, запобігання порушенням суспільного порядку.

Для запобігання загрозам або інцидентам у мережах та інформаційних системах життєво важливих постачальників, урядових органів або постачальників цифрових послуг (DSP) існують кризові команди, які надають допомогу в разі інцидентів із комп'ютерною безпекою. У WBNI така команда називається Computer Security Incident Response Team (CSIRT).

Відповідно до WBNI, для життєво важливих постачальників та постачальників основних послуг (AED) призначеним CSIRT є NCSC. Завдання NCSC:

- реагувати на випадки, про які повідомляють добровільно або примусово;
- контролювати інциденти на національному рівні, забезпечувати раннє оповіщення для провайдерів та поширювати інформацію про ризики й інциденти;
- брати участь у роботі міжнародної мережі CSIRT;
- підтримувати співпрацю з приватним сектором.

Відповідно до WBNI, життєво важливі постачальники та постачальники основних послуг у разі серйозних інцидентів зобов'язані звітувати перед NCSC . AED також звітують перед своїм галузевим регулятором. Постачальники цифрових послуг звітують у CSIRT.

Крім того, в законі прописано зобов'язання щодо нагляду за AED та DSP. Вони повинні вживати заходів задля зниження імовірності й подолання наслідків цифрових інцидентів. Обробка даних та зобов'язання щодо звітності в кібербезпеці (WGMC) також регулюється WBNI.

Для запобігання поширенню наслідків серйозних кіберінцидентів через національні кордони NCSC призначений національним контактним пунктом Нідерландів для країн — членів ЄС. Коли NCSC отримує повідомлення, актуальне і для інших країн, то передає цю оперативну інформацію контактним пунктам в інших державах-членах.

Відповідно до WBNI, на NCSC покладено такі завдання:

- надавати життєво важливим постачальникам та органам центральної влади допомогу в забезпеченні безперебійного надання послуг;
- інформувати й консультувати щодо загроз та інцидентів для мережевих та інформаційних систем життєво важливих постачальників та органів центральної влади;

61 https://wetten.overheid.nl/BWBR0041515/2019-01-01

- здійснювати аналіз і проводити технічні розслідування загроз та інцидентів або фактів, що свідчать про такі загрози чи інциденти;
- опрацювання добровільних повідомлень про інциденти в організаціях, які не належать до життєво важливих постачальників чи органів центральної влади;
- обмін інформацією з організаціями, які мають інформувати інші організації чи громадськість про загрози і інциденти, та групами реагування на інциденти в галузі комп'ютерної безпеки.

Центр цифрової довіри (DTC)

Нідерланди — країна зі сприятливим бізнес-кліматом і сильними конкурентними позиціями на міжнародному ринку. Цифровізація — одна з важливих конкурентних переваг. Необхідна передумова такого стану — цифрова стійкість підприємств і належний рівень цифрової безпеки. Тому Міністерство економічних справ та клімату (EZK) у 2018 році створило Центр цифрової довіри (DTC)[62].

Місія DTC — зробити 1,8 млн нідерландських компаній більш стійкими до кіберзагроз. Це всі ті компанії в Нідерландах, які не належать до життєво важливих секторів. Життєво важливі сектори, наприклад банки, телекомунікаційні, енергетичні та водопостачальні компанії, працюють з Національним центром кібербезпеки (NCSC).

DTC використовує для охоплення широкої цільової аудиторії різні інструменти.

Вебсайт пропонує доступні знання, інформацію та поради, які підприємці можуть використовувати самі.

Наприклад, DTC розробив 5 основних принципів безпечного цифрового підприємництва. Підприємці можуть використовувати ці основні принципи для забезпечення основних цифрових заходів безпеки. На вебсайті також є інформація та поради щодо важливих тем, пов'язаних із кіберстійкістю. Наведено й конкретні підприємницькі історії. Таким чином підприємці можуть надихати та заохочувати одне одного дбати про свою цифрову безпеку.

Багатьом підприємцям важко оцінити стан цифрової безпеки у своїй компанії. Тож DTC розробив програму Basic Cyber Resilience Scan[63], яка дає підприємцям змогу самотужки перевірити кіберстійкість компанії.

Співпраця — важливий чинник підвищення опірності до кіберзагроз. DTC стимулює партнерство компаній, які допомагають групам підприємців із забезпеченням безпеки цифрового підприємництва.

62 https://www.digitaltrustcenter.nl/over-het-digital-trust-center

63 https://rvo.regelhulpenvoorbedrijven.nl/basisscan-cyberweerbaarheid/#/stappen

Ці так звані мережі кіберстійкості можуть працювати разом у регіоні, секторі чи галузі. У 2018, 2019 та 2020 роках на такі проєкти виділяється фінансування в розмірі 1 млн євро на рік (максимум 200 тис. євро на проєкт).

DTC пропонує афілійованим компаніям можливість обмінюватися інформацією в закритому середовищі, а також планує поширювати через цей канал отримувану від NCSC поточну інформацію про загрози. Наразі мережа на стадії розробки та невдовзі буде запущена.

Для опрацювання інформації використовуються спеціально розроблені програми, що дають змогу контролювати великі обсяги інформації з таких джерел, як вебсайти, соціальні медіа та повідомлення надійних партнерів. Для моніторингу мережевого трафіку використовується мережа датчиків і сенсорів, це дає NCSC змогу безпечно аналізувати інтернет-загрози та напрями можливих нападів на урядові системи.

Одним із перших завдань, які Нідерланди ставили перед собою, ухвалюючи національну Стратегію 2011 року, був аудит і систематизація поточних загроз та ризиків ІКТ, які щорічно оновлюються, та виявлення потенціалу, необхідного для подолання загроз, більш цілеспрямованого реагування на них та запобігання їм[64].

У документах «Оцінка кібербезпеки Нідерландів» та «Оцінка прогресу Нідерландів у реалізації порядку денного з питань кібербезпеки» (CSBN[65] / CSAN[66]) проаналізовано різні аспекти кіберзахисту, зокрема заходи, учасників, загрози, використовувані методи та чинники вразливості (технічні, людські та організаційні). У процесі оцінювання проводиться опитування всіх заінтересованих сторін за їх тісної співпраці.

Нідерланди також підписали меморандум про взаєморозуміння з питань кібербезпеки з Люксембургом та Бельгією, який передбачає, зокрема, співробітництво та обмін досвідом у питаннях розвитку державно-приватного партнерства.

Міністр правосуддя та безпеки представляє оцінку кібербезпеки Раді міністрів, Раді з питань кібербезпеки та нижній палаті парламенту; публічна версія доступна для всіх заінтересованих сторін на вебсайті NCSC[67].

Нідерланди докладають багато зусиль до розбудови можливостей кібероперацій для своїх збройних сил.

Нідерланди вважають кіберпростір п'ятою цариною для військових операцій поряд із повітрям, морем, суходолом та космосом, а цифрові активи — невіддільним складником військових операцій.

64 https://www.cyberwiser.eu/netherlands-nl

65 https://www.ncsc.nl/onderwerpen/cyber-security-beeld-nederland/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019

66 https://www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda/documenten/kamerstukken/2019/juni/12/voortgang-ncsa

67 https://www.cybersecurityraad.nl/binaries/CSR_Advies_IACS_Onderzoeksrapport_Gartner_DEF_tcm107-442489.pdf

Керівництво нідерландської системи організації оборони (Міністерство оборони складається з 7 організаційних підрозділів – Королівський флот, Королівські наземні сили, Королівські ВПС, Королівська військова поліція, Командування оборонної підтримки, Організація оборонних матеріалів, Управлінський персонал) декларує забезпечення підвищеної безпеки цифрового середовища, або кіберпростору.

Для створення належних умов для організації успішної оборони в цифрову епоху Нідерланди окреслили у своїй стратегії кіберборони важливі напрями.

НАПРЯМИ КІБЕРОБОРОНИ

Зацікавлення кіберпрофесіоналів, їх наймання та подальший розвиток їхніх навичок

Щоб досягти успіху в цифрову епоху, системі організації оборони потрібні люди з глибокими знаннями. Щоб бути привабливим роботодавцем для цих кіберпрофесіоналів, організація має гнучко підходити до кадрової політики та шкали зарплат. Заохочуючи кар'єрний розвиток та обмін персоналом між різними підрозділами, система організації оборони також прагне зосередити пильнішу увагу на кібербезпеку як галузі знань. Для цього потрібна співпраця із зовнішніми сторонами, такими як університети та комерційний сектор.

Ефективні інновації та купівельність

Щоб не відставати від постійно оновлюваної сфери цифрових технологій, система організації оборони має за необхідності змінювати свої процедури. Збройні сили мають бути здатні швидко розвивати кіберактиви у відповідь на нові оборонні чи наступальні потреби. Крім того, система організації оборони впроваджує швидші та простіші процедури купівельності та інновацій.

Об'єднання сил та спільна робота

Кіберзнання, активи, персонал та можливості акумулюються всюди, де можливо. Важливо також співпрацювати з національними та міжнародними партнерами:

- усередині Міністерства оборони об'єднання зусиль структурних підрозділів забезпечує ефективне використання обмежених ресурсів та досвіду;
- з іншими урядовими органами. Для підвищення рівня цифрової стійкості в країні Міністерство оборони співпрацює з такими організаціями, як Національний центр кібербезпеки (NCSC). Королівська військова поліція[68] тісно співпрацює з Міністерством юстиції та безпеки та Державною прокуратурою; зокрема ідеться про перевірку повноважень щодо використання кіберактивів під час військових дій.

68 https://www.defensie.nl/organisatie/marechaussee/taken

- з комерційним сектором — у межах спільних науково-дослідних програм, розвитку спільних можливостей у галузі освіти та навчання.
- з міжнародними партнерами. НАТО може підтримувати Нідерланди в підготовці стандартів безпеки для держав-членів, у сприянні обміну інформацією та знаннями,у забезпеченні кращої взаємодії країн.

Знання та кіберсвідомість: розвиток і розширення

Дослідження та навчання забезпечують поширення вживання кіберзнань на всіх щаблях організації, що збагатило цифровий курс, а особовий склад оборони більше знає про можливості та небезпеки цифрового світу. Міністерство оборони інвестує в освіту всього персоналу в галузі IT, комунікацій та інформаційних систем, завдяки чому працівники зможуть швидше виявляти кібератаки й запобігати їм.

Посилення цифрової стійкості. Подальше зміцнення цифрових активів

Міністерствоя оборони планує створити центр безпеки операцій, що здійснюватиме моніторинг та захист усіх мереж системи оборони, IT-служб та систем у Нідерландах та місцях операцій. Міністерство оборони також надаватиме пріоритет розвитку активів, що сприяють обміну секретною інформацією. Планується оновити для оборонних контрактів загальні вимоги щодо безпеки , які описують, як зовнішні постачальники послуг повинні поводитися з секретною інформацією від Міністерства оборони.

Посилення цифрового інтелекту

Для забезпечення достатньої свободи в цифровій сфері було модернізовано Закон про розвідувальні та охоронні послуги 2017 року[69] (набрав чинності у 2020 році). Передумовою для виявлення кібератак на ранній стадії є доступ до телекомунікацій.

Міністерство оборони має на меті зміцнити Об'єднаний кіберпідрозділ (JSCU)[70], спільний кіберпідрозділ, створений у 2014 році Службою військової розвідки та безпеки[71] й Генеральною службою розвідки та безпеки[72].

69 https://wetten.overheid.nl/BWBR0039896/2020-01-01

70 https://english.aivd.nl/about-aivd/the-aivd-who-we-are

71 https://www.defensie.nl/organisatie/bestuursstaf/eenheden/mivd

72 https://english.aivd.nl/about-aivd

Посилення кіберактивів під час місій

Для забезпечення можливостей використання цифрових активів у військових операціях Міністерство оборони надалі цілеспрямовано зосередиться на:

- подальшому розвитку кібердоктрини оборони;
- розробці кіберактивів та підготовці керівних принципів щодо підготовки кіберодиниць та активів з подвійним призначенням;
- створенні оборонних цифрових активів під час місій;
- розвитку кіберактивів та засобів кіберрозвідки для тактичного використання;
- урахуванні кібераспектів під час ухвалення оперативних рішень до і після операцій.

Кіберстратегію оборони, вперше оприлюднену 2012 року, оновлено в лютому 2015 року.

У межах Міністерства оборони з 2013 року працює Спільне командування управління інформацією (Joint InformatieVoorzienings Commando, JIVC[73]), яке відповідає за забезпечення стійкості мереж та систем Міністерства оборони.

JIVC забезпечує ефективну спільну роботу всіх учасників оборонних операцій (цивільних та військових), які працюють у Нідерландах і безпосередньо в місці проведення місії, 24 години на добу 7 днів на тиждень. Ідеться про всі аспекти діяльності, від проєктування інформаційних систем та системи у забезпечення інформацією до інформаційних технологій, керування та управління, від кіберпростору до IT-машин, від криптовалют та великих даних до робочих місць вдома і за кордоном. Як приклади можна навести засоби зв'язку на кораблях і транспорті, експлуатацію систем озброєння та радарів. Крім того, зараз стандартним обладнанням для військових під час місії є смартфони та планшети. Без засобів комунікації, які належно функціонують, місії та навчання стають небезпечними чи навіть неможливими. JIVC забезпечує доступність цих ресурсів у будь-який час і в будь-якому місці. Крім того, JIVC забезпечує створення та обслуговування понад 50 000 робочих місць. У різних місцях JIVC працюють понад 3500 людей.

Команда реагування на комп'ютерні надзвичайні ситуації (DefCERT), що повноцінно функціонує з 2012 року, входить до складу JIVC і несе відповідальність за безпеку основних мереж оборони.

Завдання DefCERT — забезпечити відсутність перешкод для забезпечення військових дій і надійність інформаційних систем у сфері оборони.

Для цього DefCERT має:

- вчасно помітити кіберзагрозу;
- дослідити масштаб загрози;
- забезпечити зниження рівня чи усунення загрози.

73 https://www.defensie.nl/organisatie/dmo/onderdelen/jivc

Крім того, у випадку боротьби з кіберзагрозами DefCERT може також підтримувати цивільні органи влади.

У своїй діяльності DefCERT тісно співпрацює з іншими командами:

- Національним центром кібербезпеки NCSC;
- Координаційним центром НАТО з реагування на комп'ютерні інциденти (NCIRC);
- Форумом команд реагування на інциденти інформаційної безпеки (FIRST)[74].

У Кіберстратегії оборони наголошено на необхідності «значних інвестицій» у зміцнення кіберможливостей як невіддільного складника загальної військової спроможності збройних сил. Кібероборона здійснюється під керівництвом начальника збройних сил (CDS)[75].

Оскільки кіберпростір у Нідерландах вважається частиною сфери оборони, зросла роль Служби військової розвідки та безпеки (Militaire Inlichtingen-en Veiligheidsdienst, MIVD)[76].

Крім стандартних повноважень щодо надання розвідувальної та безпекової інформації Міністерству оборони та Збройним силам Нідерландів, MIVD забезпечує збір та аналіз важливої з військової точки зору інформації щодо захисту комп'ютерних мереж (запобігання загрозам та їх виявлення), експлуатації комп'ютерних мереж (посилення розвідувальних позицій у цифровій сфері, зокрема для підтримки військових операцій) та з забезпеченням розвитку комп'ютерної мережі Збройних сил (CNA).

Відповідно до Білої книги оборони Нідерландів, спроможність кіберрозвідки MIVD буде зміцнюватися[77].

Було модернізовано й взаємодію MIVD зі Службою загальної розвідки та безпеки (Algemene Inlichtingen en Veiligheidsdienst, AIVD), що зосереджується на внутрішніх невійськових загрозах національній безпеці: так, перехоплення сигналів зв'язку (SIGINT) та кіберкомпоненти AIVD та MIVD у червні 2014 року[78] було об'єднано у новий Спільний підрозділ SIGINT (JSCU)[79].

У рамках спільного підрозділу служби мають право надавати одна одній технічну та інші форми підтримки, але кожна зберігає свою чітку юридичну відповідальність і повноваження, передбачені Законом про розвідувальні та охоронні служби 2002 р..

Управління кризовими ситуаціями здійснює уряд Нідерландів.

74 https://www.first.org/

75 https://www.defensie.nl/organisatie/bestuursstaf/cds

76 https://www.defensie.nl/organisatie/bestuursstaf/eenheden/mivd

77 https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vjebqn0inhyj

78 https://blog.cyberwar.nl/2013/09/project-symbolon-completed-the-dutch-joint-sigint-cyber-unit-jscu-is-born/

79 https://www.aivd.nl/onderwerpen/over-de-aivd

На Національний координаційний орган з питань безпеки та протидії тероризму (NCTV) як структурний підрозділ Міністерства юстиції та безпеки покладено завдання запобігати катастрофам та кризам і мінімізувати їх наслідки. NCTV відповідає за безпеку в Нідерландах на національному рівні.

NCTV забезпечує надання регіональним органам влади достатнього обсягу інформації для узгодження підходів до вирішення проблеми. NCTV вживає заходів для захисту користувачів мережі Інтернет від збитків через неправильне використання (кіберзлочинність) та виходу мережі з ладу.

Мережа аналітиків з питань національної безпеки (ANV)[80] розробляє Національні оцінки ризиків[81] [82].

Захист критичної інфраструктури загалом покладено на Міністерство юстиції табезпеки[83].

Стратегічний консультативний орган з питань критичної інфраструктури (Strategisch Overleg Vitale Infrastructuur, SOVI) був створений Міністерством внутрішніх справ та відносин Королівства у 2006 році[84].

До його складу входять представники громадського сектора та бізнес-спільноти. Орган здійснює моніторинг критичної інфраструктури, захист на стратегічному рівні, зокрема відстеження вразливостей, взаємозалежностей та ризиків.

Нідерландські державні органи з питань надзвичайних ситуацій, розвідувальні служби та приватні підприємства, що займаються захистом критичної інфраструктури, тісно співпрацюють між собою. Завдяки цій співпраці NCSC отримує сучасні знання про кібербезпеку. Також NCSC працює над інноваційними рішеннями разом із відомими навчальними та науково-дослідними інститутами.

Завдання щодо цифрової безпеки покладаються на різні державні та приватні структури. NCSC є сполучною ланкою між цими сторонами. NCSC забезпечує узгодженість різноманітної діяльності, зокрема інноваційних досліджень та розробок. NCSC залучається до проєктів, зазначених у Національній програмі досліджень кібербезпеки (NCSRA).

Програма досліджень NCSC 2019–2022 рр.[85] сфокусована на чотирьох головних питаннях: управління кризами, управління ризиками, стратегії та соціальні аспекти кібербезпеки й нових технологій. Таким чином, NCSC шукає баланс між фундаментальними дослідженнями, дослідженнями, що сприяють виконанню завдань NCSC, та дослідженнями, що допомагають забезпечити цифрову безпеку в Нідерландах.

---

80 https://www.rivm.nl/en/about-rivm/organisation/centre-for-environmental-safety-and-security/national-network-of-safety-and-security-analysts

81 https://english.nctv.nl/topics/national-security-strategy/priority-assessment-of-threats-and-risks

82 https://english.nctv.nl/topics/national-security-strategy/documents/publications/2019/09/18/dutch-national-risk-assessment

83 https://english.nctv.nl/themes/crisis-management

84 https://wetten.overheid.nl/BWBR0019781/2006-04-28

85 https://www.ncsc.nl/onderzoek/documenten/publicaties/2019/september/26-9-2019/ncsc-onderzoeksagenda-2019-2020

Завдяки Програмі досліджень на 2019–2022 роки реалізуються проєкти з розвитку знань відповідно до NCSA.

Третя програма NCSRA (National Cyber Security Research Agenda – частина досліджень, що стуосується кібербезпеки)) вже опублікована (NCSRA-III)[86]. Основна увага в ній приділена дослідженням за тематикою, що відповідає Національній стратегії кібербезпеки.

NCSRA надає конкретну форму п'ятій цілі с тратегії: «Нідерланди мають достатньо знань та досвіду в галузі кібербезпеки та вкладають кошти в інновації в галузі ІКТ для досягнення наших цілей в галузі кібербезпеки»[87]. NCSRA також є основою для коротко- та довгострокових досліджень у національному й міжнародному контексті. NCSRA III окреслює рамки досліджень, в основу яких покладено п'ять тем: розробки, оборона, наступальні дії, управління та конфіденційність.

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ НІДЕРЛАНДІВ

Нідерландський порядок денний з кібербезпеки (NCSA) визначає основи подальших кроків для забезпечення кібербезпеки.

ПІДХОДИ ДО КІБЕРБЕЗПЕКИ

У Стратегії окреслено такі підходи, як спільне управління та реалізація низки публічних заходів. Такий формат посилює спільний вплив дій громадськості й приватного сектора. Визначено такі провідні принципи діяльності:

- Кібербезпека нерозривно пов'язана з національною безпекою: внаслідок цифровізації інтересам національної безпеки можуть загрожувати цифрові атаки.
- Безпеку в цифровій сфері можна забезпечити лише у співпраці, залучаючи до неї також і бізнес-спільноту. Таким чином, державно-приватне партнерство є основою національного підходу до кібербезпеки.

86 https://www.ncsc.nl/onderzoek/documenten/publicaties/2019/juni/26/ncsra-iii

87 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

- Уряд представляє суспільні інтереси: захищені з точки зору кібербезпеки Нідерланди, де визнають загрози для життєво важливих інтересів і посилюють стійкість. Бізнес-спільноту і громадян заохочують брати на себе певні зобов'язання в царині безпеки. Крім того, уряд як державний орган зобов'язаний забезпечити кібербезпеку власних процесів, даючи тим самим взірець для наслідування.
- Знання мають вирішальне значення для кібербезпеки: для посилення кібербезпеки в цілому необхідні обмін наявними знаннями та сприяння обміну інформацією між державним та приватним сектором. Крім того, необхідно й надалі стимулювати як фундаментальні, так і прикладні дослідження в галузі кібербезпеки, щоб розвинути відповідну базу знань у Нідерландах.
- Мета діяльності в рамках Стратегії — забезпечення кібербезпеки: цифровий захист має стати невіддільною частиною повсякденних процесів кожної організації.
- Цифрова сфера не обмежується національними кордонами. У національних підходах до кібербезпеки слід враховувати міжнародний вимір даних, зв'язків, управління Інтернетом та суб'єктів, які здійснюють цифрові атаки. Отже, безпечніший кіберпростір є одним із пріоритетів Нідерландів як країни — члена НАТО та ЄС.
- У контексті розвитку кібербезпеки актуальним є питання дисбалансу й суперечностей між інтересами свободи, безпеки та економічного зростання. З огляду на це необхідно всебічно враховувати дилеми в питаннях кібербезпеки та визначати курс на основі прозорого й обґрунтованого ухвалення рішень.

Цифрові диверсії чи втручання можуть завдати безпосередньої шкоди національній безпеці. Найбільшу загрозу в кіберпросторі становлять дії правопорушників та державних акторів.

Цифровізація охоплює всі щаблі нідерландського суспільства та економіки. Суспільство стало повністю залежним від цифрових ресурсів. Безперебійне функціонування цих ресурсів має критичне значення для життєво важливих процесів у бізнесі та урядуванні, дохідності компаній та повсякденного життя громадян. Інциденти останніх років допомогли зрозуміти, що цифрові атаки можуть мати великий вплив на суспільство і завдавати шкоди безпеці людей, організацій та національній безпеці.

Зростає загроза з боку професійних злочинців, розвиваються й урізноманітнюються успішні моделі отримання кримінального доходу, наприклад програми-вимагачі. Правопорушників особливо приваблює можливість практично безмежного масштабування цифрових атак. Жертвами стають не лише окремі споживачі, але й бізнес, зокрема фінансові установи. Кіберзлочинці отримують доступ до дедалі складніших інструментів і методів здійснення атак — вони вже надаються як послуги. Унаслідок цього дедалі більше суб'єктів з обмеженими знаннями та ресурсами можуть здійснювати атаки, які подекуди справляють безпосередній вплив на суспільство.

Суб'єкти інших держав, які займаються кібершпигунством, обирають мішенями урядові установи та компанії Нідерландів. Наприклад, жертвами цифрового шпигунства стали міжнародні корпорації та науково-дослідні інститути в галузі енергетики, високих технологій та хімії . З використанням цифрових прогалин було вкрадено терабайти конфіденційної інформації, що становить значну економічну цінність. Суб'єкти інших держав зосереджуються на цифровому економічному та політичному шпигунстві та підготовці цифрових диверсій. Збільшується кількість країн, які розвивають можливості кібератак, разом із тим ускладнюються й самі атаки. Крім того, минулого року державні суб'єкти також зосередилися на цифровому впливі на демократичні процеси задля отримання геополітичних переваг. Для захисту геополітичних інтересів країни вкладають кошти в цивільні та військові кібер-можливості.

Приклад: *Кіберзлочинність як послуга та викупне програмне забезпечення*

Кіберзлочинці не здійснюють злочинні дії виключно самотужки. Вони часто купують послуги та знання. Прикладом цього є викупне програмне забезпечення: тип шкідливого програмного забезпечення, яке блокує системи та / або інформацію, яку вони містять, і робить їх знову доступними лише після сплати викупу. Якщо злочинець хоче розповсюдити викупне програмне забезпечення, то, наприклад, платить комусь за його розробку, а хтось інший поширює повідомлення з вимогою викупу електронною поштою мільйонам адресатів. Ці послуги надаються на високому професійному рівні та в повному обсязі: від технічних ресурсів до інфраструктури та функцій служби довідки.

Кібератаки впливають на суспільство. Наприклад, громадянам доводиться боротися з наслідками крадіжок ідентичності або втратою особистих фотографій через шкідливі віруси-вимагачі. Такі атаки можуть потенційно підірвати довіру до цифрового суспільства. Кібератаки злочинців чи іноземних розвідслужб можуть зашкодити економіці Нідерландів, адже крадіжки конфіденційної чи цінної інформації руйнують довіру до економічної діяльності.

Приклад: *NotPetya*

Випадок із вірусом NotPetya — приклад цифрової атаки, що потягнула за собою значні наслідки для нідерландського бізнесу. У червні 2017 року організації в усьому світі зазнали атаки шкідливих програм-вимагачів. У Нідерландах ця програма вплинула, зокрема, на функціонування портового оператора APM Terminals (там зупинилася обробка контейнерів) та компанії доставки TNT Express (спостерігалися затримки відправлень і доставок). Хоча, імовірно, основною метою цієї атаки була Україна, бізнес Нідерландів також серйозно постраждав.

ЄС

Для організації взаємодії країн ЄС у питаннях забезпечення безпеки спеціально створене Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA).

Стратегії мережевої та інформаційної безпеки, оприлюднені інституцією, органом, офісом або агентством ЄС чи державою-членом, мають бути надані ENISA для отримання інформації та уникнення дублювання. ENISA має аналізувати стратегії, сприяти представленню їх у форматі, що надається до порівняння, забезпечувати за допомогою електронних засобів доступність для громадськості стратегій та результатів їх аналізу.

ЗАКОНОДАВСТВО

Директива з безпеки мережевих та інформаційних систем (Директива NIS)[88] становить першу частину законодавства ЄС щодо кібербезпеки. Вона забезпечує правові заходи, спрямовані на підвищення загального рівня кібербезпеки в ЄС. Документ ухвалений Європейським Парламентом 6 липня 2016 року і набрав чинності в серпні 2016 року, але держави-члени мали 21 місяць, щоб транспонувати Директиву до своїх національних законів, і понад 6 місяців, щоб визначити операторів основних послуг.

Директива NIS передбачає юридичні заходи для підвищення загального рівня кібербезпеки в ЄС. Для цього вона вимагає забезпечити:

- готовність держав-членів, їхнє належне оснащення, наприклад, наявність групи з реагування на інциденти в галузі комп'ютерної безпеки (CSIRT) та компетентного національного органа (HIC);
- співробітництво між усіма державами-членами шляхом створення групи співпраці з метою підтримки та сприяння стратегічній взаємодії та обміну інформацією між державами-членами.

88 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Крім того, їм необхідно буде встановити мережу CSIRT, щоб сприяти швидкому та ефективному оперативному співробітництву щодо конкретних випадків кібербезпеки та обміну інформацією про ризики;

- культуру безпеки між секторами, що є життєво важливими для економіки та суспільства і, крім того, сильно залежать від ІКТ, наприклад: енергетика, транспорт, водопостачання, банківська справа, інфраструктура фінансового ринку, охорона здоров'я та цифрова інфраструктура. Підприємства в цих секторах, що визначені державами-членами як оператори основних послуг, мають вживати відповідних заходів безпеки та повідомляти відповідним національним органам про серйозні інциденти. Крім того, основні цифрові постачальники послуг (пошукові системи, служби хмарних обчислень та інтернет-магазини) повинні відповідати вимогам безпеки та інформування відповідно до нової Директиви.

Сьомий пріоритет Східного партнерства до 2020 року «Зосередження уваги на ключових пріоритетах та відчутних результатах» також підтверджує необхідність узгодження безпекових стратегій для досягнення єдиного цифрового ринку як в ЄС, так і з третіми країнами.

7 червня 2019 року в Офіційному журналі ЄС опубліковано Регламент про кібербезпеку Європейського Союзу (Регламент (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з питань кібербезпеки) та про сертифікацію кібербезпеки в галузі інформаційних та комунікаційних технологій та скасування Регламенту (ЄС) №526/2013 (Закон про кібербезпеку))[89] Документ набув чинності 27 червня 2019 року.

Законодавство ЄС має на меті зміцнити спроможність Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) допомагати державам-членам подолати загрози кібербезпеки.

Законодавство ЄС про кібербезпеку має дві основні цілі:

- посилення мандата ENISA як наглядового органа ЄС у царині кібербезпеки задля підтримки держав-членів ЄС у подоланні загроз та атак у цій сфері;
- створення загальноєвропейської системи сертифікації кібербезпеки (Основи), в якій ENISA відіграватиме ключову роль.

Відповідно до нових принципів, ENISA координує підготовку запропонованих схем сертифікації кібербезпеки, що подаються для ухвалення до Європейської Комісії. Принципи дадуть можливість видавати європейські сертифікати кібербезпеки та акти про відповідність продукції, послуг і процесів інформаційних та комунікаційних технологій (ІКТ) у всіх країнах-членах ЄС.

Законодавство про кібербезпеку пропонує бізнесам можливість засвідчити, що їхня продукція відповідає стандартам кібербезпеки ЄС. Сертифікація з питань кібербезпеки буде добровільною, якщо інше не встановлено законодавством ЄС або країнами-членами. Комісія ЄС регулярно оцінюватиме необхідність впровадження обов'язкових сертифікацій.

89 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Схема сертифікації може визначати один або кілька рівнів забезпечення безпеки: базовий, значний або високий. На базовому рівні виробники ІКТ або постачальники послуг зможуть самі здійснювати оцінку відповідності. У випадку значного чи високого рівня оцінювання здійснюватимуть національні органи з сертифікації кібербезпеки.

Держави-члени ЄС мають розробити правила щодо покарань за порушення у сфері кібербезпеки та за порушення схем сертифікації кібербезпеки ЄС.

Законодавство про кібербезпеку є частиною загальної кіберекосистеми Європейського Союзу, мета якої — підвищення безпеки цифрового середовища Європейського Союзу. Ця законодавча база включає Директиву щодо безпеки мережевих та інформаційних систем (Директиву NIS), яка встановлює вимоги щодо сповіщення та безпеки для операторів основних послуг та постачальників цифрових послуг, таких як постачальники хмарних послуг. Проект Регламенту електронної конфіденційності[90] спрямований на захист права на конфіденційність (таємницю) комунікацій, а також на просування надійного та безпечного Інтернету на єдиному цифровому ринку. Загальне положення про захист даних[91] (GDPR) вимагає від контролерів та операторів у всіх галузях промисловості впроваджувати відповідні заходи щодо захисту даних.

Таким чином, Законодавство Європейського Союзу про кібербезпеку не розглядає окремо заходи з кібербезпеки і захист приватності, а має на меті узгоджені дії із захисту засобів, інформації та приватності як частину екосистеми кібербезпеки.

СУБ'ЄКТИ КІБЕРБЕЗПЕКИ

На рівні ЄС група співробітництва NIS Cooperation Group (CG), створена відповідно до статті 11 Директиви NIS. Головування забезпечує держава-член, яка головує в Раді Європейського Союзу (ЄС). Вона збирає представників держав-членів, Європейської Комісії (виконуючи функції секретаріату) та ENISA. З огляду на важливість міжнародної співпраці у сфері кібербезпеки Група має сприяти стратегічному співробітництву та обміну інформацією між державами-членами й поглибленню довіри між ними. Наразі за період із лютого 2017 року CG провела чотирнадцять засідань[92]. Завдання Групи описані у статті 11 (3). Її функціонування додатково регулюється Виконавчим рішенням Комісії, що встановлює механізми роботи Групи відповідно до статті 11 (5) Директиви[93].

Мережі національних CSIRT

Статтею 12 Директиви NIS визначено створення мережі національних CSIRT. Мережа CSIRT складається з представників CSIRT держав-членів та CERT-EU (Команд реагування на комп'ютерні надзвичайні ситуації для організацій, установ та органів ЄС). Серед завдань, що належать до

90 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

91 https://eur-lex.europa.eu/eli/reg/2016/679/oj

92 https://ec.europa.eu/digital-single-market/en/news/nis-cooperation-group-meetings-agendas

93 https://eur-lex.europa.eu/eli/dec_impl/2017/179/oj

компетенції мережі CSIRT, — обмін інформацією про послуги, операції та можливості співпраці CSIRT, обмін інформацією щодо інцидентів та пов'язаних із ними ризиків, скоординована реакція на інциденти та надання державам-членам підтримки у подоланні транскордонних інцидентів. Комісія бере участь у Мережі CSIRT як спостерігач.

Секретаріат ENISA

ENISA надає послуги секретаріату, активно підтримуючи співпрацю між CSIRT. Через два роки після набуття чинності Директивою NIS та кожні 18 місяців після цього Мережа CSIRT звітуватиме про оцінку переваг оперативного співробітництва, надаючи також висновки й рекомендації. Звіт надсилатиметься Комісії і слугуватиме інструментом аналізу функціонування Директиви. Недержавні суб'єкти, зокрема бізнес-структури, зобов'язані брати участь у спільній діяльності, нести відповідальність за кібербезпеку й частково поступитися звичною автономією та можливостями контролю задля отримання довгострокової вигоди для всіх.

Сертифікація кібербезпеки (ECCG)

Також на підставі Закону про кібербезпеку на рівні ЄС створено Європейську групу з сертифікації кібербезпеки (ECCG)[94]. Вона має на меті консультування та допомогу Європейській Комісії в процесі забезпечення послідовного виконання та застосування вищезгаданого Закону.

Завдання ECCG:

- надавати консультації та допомагати Комісії в роботі із забезпечення послідовного виконання та застосування Закону про кібербезпеку, зокрема в рамках постійної робочої програми Союзу, політики сертифікації кібербезпеки, координації політичних підходів та підготовки європейських схем сертифікації кібербезпеки;
- допомагати, консультувати та співпрацювати з ENISA у питаннях підготовки нових можливих схем сертифікації кібербезпеки;
- давати висновки щодо можливих схем сертифікації кібербезпеки, підготовлених ENISA;
- звертатися до ENISA із запитом щодо підготовки можливих схем сертифікації кібербезпеки;
- приймати адресовані Комісії висновки щодо підтримки та перегляду чинних європейських схем сертифікації кібербезпеки;
- вивчати відповідні розробки в галузі сертифікації кібербезпеки та обмінюватися інформацією й найкращими практиками в питаннях схем сертифікації кібербезпеки;
- відповідно до Закону про кібербезпеку сприяти співпраці між національними органами сертифікації кібербезпеки шляхом нарощування потенціалу та обміну інформацією, зокрема шляхом впровадження методів ефективного обміну інформацією в царині сертифікації кібербезпеки;

94 https://ec.europa.eu/digital-single-market/en/european-cybersecurity-certification-group

- підтримувати впровадження механізмів експертної оцінки відповідно до правил, встановлених в європейській сертифікації з кібербезпеки;
- сприяти приведенню європейських схем сертифікації кібербезпеки у відповідність до міжнародно визнаних стандартів, зокрема шляхом перегляду чинних європейських схем сертифікації кібербезпеки та, де це доцільно, надання рекомендацій ENISA щодо співпраці з відповідними міжнародними організаціями зі стандартизації для усунення недоліків або прогалин у доступних міжнародно визнаних стандартах.

До складу ECCG входять представники національних органів сертифікації кібербезпеки або представники інших відповідних національних органів. Член ECCG не може представляти більш ніж дві держави-члени. Крім того, до участі в засіданнях та роботі ECCG можуть бути запрошені інші заінтересовані й треті сторони.

Уряди та органи державної влади неохоче діляться інформацією про кібербезпеку, боячись поставити під загрозу територіальну безпеку та конкурентоспроможність. Компанії неохоче розкривають інформацію про свої кібервразливості, оскільки бояться втратити важливі комерційні дані та нематеріальні активи, зокрема репутацію. Політики не надто схильні впроваджувати на законодавчому рівні жорсткіші заходи з кібербезпеки, оскільки у поєднанні з ухиляннням приватного сектора від відповідальності за національну безпеку державно-приватне партнерство в цій царині досі характеризується розмитими межами підзвітності.

Дослідження Центру довгострокової кібербезпеки Каліфорнійського університету Берклі свідчить, що до 2020 року партнерство між державними і приватними компаніями стане нормою: «Успішне налагодження відносин між приватними особами та урядами стане джерелом значних переваг для безпеки міста, регіону, країни тощо. І в міру розширення цих партнерських відносин важче буде відрізнити те, що робить приватний актор і що робить уряд для захисту мереж та даних» (CLTC, 2016)[95].

ВИРІШЕННЯ ПРОБЛЕМ КІБЕРБЕЗПЕКИ

Ситуація в Європі є певним зрізом світової ситуації. Рівень здатності вирішувати проблеми кібербезпеки в різних членів ЄС сильно відрізняється. Деякі з них вже розвинули національну кібербезпеку, стратегії тощо, інші поки зосереджені на виборі конкретних підходів, наприклад, до розподілу відповідальності між державним та приватним секторами, видів інструментів та стимулів. Стратегії держав-членів також відрізняються в силу неоднакових культурних та політичних уподобань.

Одна з відмінностей європейської ситуації від світової полягає в тому, що установи ЄС докладають спільних зусиль до подолання вищезазначених проблем управління кібербезпекою хоча б на макрорегіональному рівні.

95 Elsewhere, Choucri et al (2013)

Крім того, попри внутрієвропейські відмінності, в ЄС досягнуто значного консенсусу щодо основних принципів та цінностей, а також спільних стратегічних інтересів, які можна покласти в основу ефективного управління кібербезпекою ЄС. Чинне законодавство ЄС та механізми координації (Директива NIS, Агентство ЄС з питань мережевої та інформаційної безпеки ENISA, Європол та Європейський центр протидії кіберзлочинності (European Cybercrime Centre, EC3), CERT та різні служби Європейської Комісії) сприяють активізації обміну даними про кібербезпеку в ЄС.

Європейська Комісія у 2017 році запропонувала створити Мережу центрів знань у сфері кібербезпеки та новий Європейський центр кібербезпеки індустріальної, технологічної та дослідницької компетенції з питань кібербезпеки для забезпечення інвестицій в інновації в ЄС[96].

Створення цих центрів має допомогти ЄС зберегти й розвинути технологічний та промисловий потенціал кібербезпеки, необхідний для забезпечення єдиного цифрового ринку. Ця пропозиція корелює з основною метою щодо підвищення конкурентоспроможності галузі кібербезпеки ЄС та перетворення кібербезпеки на конкурентну перевагу інших європейських галузей.

Ініціатива щодо центрів допоможе створити взаємопов'язану загальноєвропейську промислову та дослідницьку екосистему кібербезпеки та буде керувати фондами кібербезпеки в рамках наступної багаторічної фінансової програми 2021–2027 років. Ініціатива ґрунтується на досвіді понад 660 експертних центрах з питань кібербезпеки з усіх держав-членів, які взяли участь у недавньому опитуванні[97], проведеному Європейською Комісією.

Такі кроки допоможуть ЄС та державам-членам окреслити довгострокову стратегічну перспективу промислової політики в галузі кібербезпеки, що виходить за рамки досліджень та розробок. Такий підхід не лише посприяє розробці проривних рішень для проблем приватного й державного сектора в царині кібербезпеки, але й підтримає ефективне їх впровадження. Завдяки цьому наукові й бізнесові кола та державні органи отримають доступ до ключових можливостей, зокрема для випробувань та експериментів, які часто недоступні окремими державам-членам через обмеженість фінансових і людських ресурсів. Крім того, ініціатива сприятиме усуненню прогалин у вміннях та запобігатиме відпливу талантів, забезпечуючи найталановитішим фахівцям доступ до масштабних європейських науково-дослідних та інноваційних проєктів з кібербезпеки[98], що стануть цікавими професійними викликами.

Кожна держава-член має визначити один Національний координаційний центр. Вони будуть функціонувати як контактні пункти національного рівня для Спільноти компетенцій та Центру компетенцій.

Спільнота з кібербезпеки залучатиме широкий спектр різноманітних суб'єктів, які займаються технологіями кібербезпеки, зокрема науково-дослідні установи, галузі попиту / попиту та державний сектор. Він зробить внесок у діяльність та план роботи Центру компетентностей,

96 https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre

97 https://ec.europa.eu/jrc/en/research-topic/cybersecurity/cybersecurity-competence-survey

98 https://cordis.europa.eu/article/id/400141-securing-cyberspace-delivering-concrete-results-through-eu-research-and-innovation/en

а також отримає користь від діяльності спільнот щодо розвитку Центру компетентностей та Мережі. Європейський центр з питань кібербезпеки промисловості, технологій та досліджень з кібербезпеки допомагатиме координувати роботу Мережі й розвиватиме Спільноту компетенцій, керуючи технологічною програмою в галузі кібербезпеки та полегшуючи доступ до надбань і досвіду національних центрів.

Однією з десяти засад політики ЄС у сфері кібербезпеки є розвиток державно-приватного партнерства. У рамках реалізації стратегії кібербезпеки ЄС Європейська Комісія та Європейська організація кібербезпеки (ECSO)[99] 5 липня 2016 року підписали угоду з кібербезпеки про посилення заходів, спрямованих на подолання кіберзагроз[100].

Метою партнерства визначено сприяння співпраці між державними та приватними суб'єктами на ранніх етапах процесу досліджень та інновацій задля забезпечення європейцям доступу до інноваційних та надійних рішень (ІКТ-продуктів, послуг та програмного забезпечення). Ці рішення мають враховувати основні права людини, зокрема право на повагу до приватного життя. Угода має на меті стимулювати галузь кібербезпеки, сприяючи зрівноваженню попиту та пропозиції з тим, щоб галузь могла передбачати майбутні потреби кінцевих споживачів, а також секторів, які є важливими замовниками рішень у сфері кібербезпеки (наприклад, енергетика, охорона здоров'я, транспорт, фінанси).

Державно-приватне партнерство відіграватиме важливу роль в забезпеченні кібербезпеки промисловості в Європі та охоплюватиме широке коло учасників — від інноваційних малих та середніх підприємств до виробників комплектуючих та обладнання, операторів критичної інфраструктури та науково-дослідних інститутів, об'єднаних під егідою ECSO.

ЄС визначила суму інвестицій у це партнерство в рамках своєї науково-дослідної та інноваційної програми Horizon 2020 у розмірі 450 млн євро. Але очікується, що гравці ринку кібербезпеки інвестують утричі більше. Перші конкурсні пропозиції були запущені в першому кварталі 2017 року.

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ЄС

Стратегія кібербезпеки ЄС визначає підходи, які мають забезпечити якнайефективніше запобігання кіберінцидентам та атакам і реагування на них. У документі детально описано низку заходів з підвищення кіберстійкості ІТ-систем, зниження рівня кіберзлочинності й посилення міжнародної політики кібербезпеки та кіберзахисту.

99 https://ecs-org.eu/

100 https://ec.europa.eu/digital-single-market/en/news/commission-signs-agreement-cybersecurity-industry-increase-measures-address-cyber-threats

ПРІОРИТЕТНІ СФЕРИ:

- досягнення кіберстійкості;
- значне зниження рівня кіберзлочинності;
- розробка політики та можливостей кіберзахисту, пов'язаних зі спільною політикою безпеки та оборони ЄС (EU's common security and defence policy — CSDP);
- розвиток промислових та технологічних ресурсів для кібербезпеки;
- впровадження для ЄС узгодженої міжнародної політики в кіберпросторі.

3 червня 2020 року Єврокомісія узгодила новий мандат на переговори з Європейським Парламентом щодо запропонованого регламенту про нові повноваження **Європейського центру компетентності з кібербезпеки та Мережі координаційних центрів.**

Центр компетенцій повинен стати головним органом, який керуватиме фінансовими ресурсами ЄС, присвяченими дослідженням кібербезпеки за двома запропонованими програмами - «Цифрова Європа» та «Горизонт Європи» – протягом наступних багаторічних фінансових рамок на 2021-2027 роки. В межах Європейського парламенту цей файл було передано Комітету з промисловості, досліджень та енергетики (ITRE).

Звіт був прийнятий 19 лютого 2019 року в комітеті ITRE і проголосований парламентом на пленарному засіданні 1 березня 2019 року. Хоча тристоронні переговори відбулись у березні 2019 року, з огляду на короткі терміни до кінця законодавчого терміну домовитись не вдалося, і Парламент тоді прийняв свою позицію в першому читанні напередодні виборів у травні 2019 року. Третя зустріч у триалозі відбулася більш ніж через рік, 25 червня 2020 року, і подальші переговори заплановані на вересень 2020 року.

В ЄС у 2019 році також було представлено сучасний стан впровадження інструментальної програми **ЄС щодо безпеки мереж 5G**[101].

ПРОБЛЕМИ БЕЗПЕКИ

У звіті визначено низку важливих проблем безпеки, які можуть виникнути або стати більш помітними в мережах 5G, порівняно із ситуацією в існуючих мережах, виклики безпеці в основному пов›язані з:

- ключовими нововведеннями в технології 5G (що також призведе до певних поліпшень безпеки), зокрема важлива частина програмного забезпечення та широкий спектр послуг та додатків, що підтримуються 5G;
- роль постачальників у побудові та експлуатації мереж 5G та ступінь залежності від окремих постачальників.

101 https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049

9 червня Рада ЄС схвалила висновки[102], що стосуються широкого кола питань, пов'язаних із реалізацією **цифрової стратегії ЄС**. У тексті висвітлено вплив цифрової трансформації на боротьбу з пандемією та її критичну роль у відновленні після COVID-19.

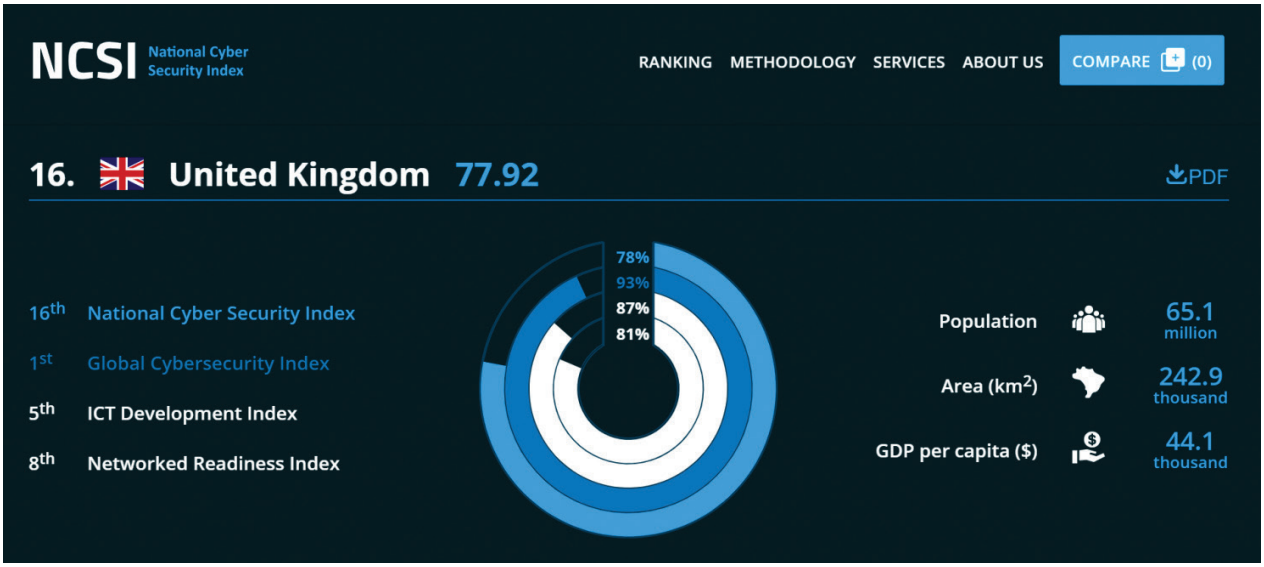
Оскільки кількість, масштаби й складність кіберзагроз та кіберзлочинів різко зростають, міністри ЄС прагнуть **покращити можливості ЄС щодо реагування на них** та захистити цілісність, безпеку і стійкість цифрової інфраструктури, мереж зв'язку та послуг. ЄС також підтримує необхідність **узгодженого підходу до зниження ризиків**, пов'язаних із кібербезпекою, та забезпечення безпечного **розгортання 5G**.

РАДА ЄС:

- визнала важливість цифрових технологій для трансформації європейської економіки та суспільства, особливо як засобу досягнення кліматично нейтральної зони в ЄС до 2050 року — як визначено в Європейській програмі «Зелена угода», а також для створення робочих місць, підвищення кваліфікації та опанування нових цифрових навичок, посилення конкурентоспроможності та інновацій, забезпечення загального благополуччя та ширшої залученості громадян;
- схвалила останній цифровий пакет Європейської Комісії: програми «Формування цифрового майбутнього Європи» та «Європейську стратегію даних», а також Білу книгу «Про штучний інтелект — європейський підхід до досконалості та довіри»;
- визнала, що Європа має активи та сильні сторони, зокрема надійну промислову базу та єдиний цифровий ринок, для успішного використання можливостей та вирішення проблем, що стоять перед цифровим сектором, забезпечення його доступності, особливо для найбільш вразливих груп, стійкості, географічного балансу та переваг для всіх держав-членів за повного дотримання загальних цінностей ЄС та основних прав;
- закликає Європейську Комісію, держави-члени, приватний сектор, громадянське суспільство та наукове співтовариство підтримати ці зусилля та долучитися до них;
- визнає, що задля ефективності ці дії мають враховувати специфічну ситуацію у найвіддаленіших європейських регіонах і гарантувати поширення цифрової трансформації на всі території;
- визнає, що прискорення цифрової трансформації буде важливою складовою реакції ЄС на економічну кризу, спричинену пандемією COVID-19, як наголошено у спільній заяві членів Європейської Ради від 26 березня 2020 р.

102 https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf

ВЕЛИКА БРИТАНІЯ



Велика Британія є лідером у багатьох питаннях забезпечення кібербезпеки, хоча окремого спеціального закону про кібербезпеку країна не ухвалювала.

Натомість існують численні законодавчі акти, що посилаються на загальні закони, підкріплені можливістю цивільних позовів за загальним правом. Зокрема:

- Закон про зловживання комп'ютером 1990 року[103] (CMA);
- Закон про шахрайства 2006 року[104] (FA);
- Закон про слідчі повноваження 2016 року (IPA)[105];

103 http://www.legislation.gov.uk/ukpga/1990/18/enacted
104 http://www.legislation.gov.uk/ukpga/2006/35/contents
105 http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

- Загальний регламент про захист даних (GDPR)[106];
- Закон про захист даних 2018 року (DPA)[107];
- Регламент мережевих та інформаційних систем 2018 року (NISR)[108];
- Закон про авторські права, зразки та патенти 1988 року[109].

Англійське законодавство переважно спонукає до забезпечення кібербезпеки покаранням за порушення (зокрема, нездатність розпорядників та власників даних захистити персональні дані), а не винагородою.

Дії, які здійснюються державними органами і у виконанні інших були б порушеннями закону, вважаються законними в інтересах національної безпеки, а також задля запобігання тяжким злочинам та їх виявлення в межах повноважень, встановлених IPA, Законом про поліцію 1997 року та Законом про розвідувальні служби 1994 року.

GDPR поширюється на обробку персональних даних, здійснювану організаціями, що працюють в межах ЄС, і тими, що працюють за межами ЄС, але пропонують товари чи послуги фізичним особам у ЄС. Регламент не поширюється на обробку, здійснену для правоохоронних органів чи в цілях національної безпеки або на побутову обробку фізичними особами. Контролери даних також повинні дотримуватися семи принципів захисту даних високого рівня. Управління уповноваженого з інформації (ICO) надало рекомендації щодо посилення цих принципів. Їх порушення може призвести до накладання значних адміністративних штрафів від ICO.

DPA доповнює, посилює GDPR та окреслює деякі винятки з його положень. З урахуванням конкретних законодавчих засобів захисту DPA криміналізує певне поводження з особистими даними, зокрема свідоме чи необережне їх отримання чи розголошення без згоди контролера (крім виправлення помилок). Закон також регламентує обробку даних різними органами влади, зокрема Управління боротьби з шахрайством(SFO), Регулятором у фінансовій сфері (FCA) та Національним агентством з питань злочинності (NCA).

NISR застосовується до операторів основних послуг (OES) (наприклад, послуги водопостачання, транспорту та енергетики) і постачальників цифрових послуг (RDSP) (наприклад, онлайнових пошукових систем, доступних для населення, онлайн-ринків та послуг хмарних обчислень). NISR вимагає відповідних та доцільних технічних і організаційних заходів для управління ризиками збоїв. Про інциденти, які мають істотний вплив на безперервність важливої послуги, необхідно повідомити відповідний компетентний орган. Також операторам наполегливо рекомендують звернутися до Національного центру кібербезпеки (NCSC), якщо вони вважають, що у своїй діяльності мають справу з елементами кібербезпеки.

106 https://eur-lex.europa.eu/eli/reg/2016/679/oj
107 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
108 http://www.legislation.gov.uk/uksi/2018/506/made
109 http://www.legislation.gov.uk/ukpga/1988/48/contents

CMA визначає правопорушення, виходячи з того, що:

1) особа змушує комп'ютер виконувати будь-яку функцію з наміром забезпечити доступ до будь-якої програми чи даних, що зберігаються на будь-якому комп'ютері, або забезпечити захист такого доступу;
2) доступ, який особа має намір здійснити або забезпечити, несанкціонований;
3) особа в момент виконання певної функції за допомогою комп'ютера знає про мету і специфіку цієї функції.

Ці злочини караються позбавленням волі аж до довічного ув'язнення, коли напад спричиняє або створює значний ризик завдавання серйозної шкоди добробуту людей або національній безпеці.

Забезпечення доступу до комп'ютера чи програми охоплює багато різних дій.

Термін «комп'ютер» у CMA не визначено. Доступ визначений як несанкціонований, якщо його здійснює особа, яка не несе відповідальності за комп'ютер і має право визначити, чи може діяльність чи бездіяльність відбуватися без згоди такої особи.

CMA визначає й інші пов'язані правопорушення, за яких спроби несанкціонованого доступу здійснюються з метою вчинення інших правопорушень (наприклад, крадіжок або шахрайства) або для порушення роботи комп'ютера, зокрема поширення вірусів чи шпигунських програм та DDoS-атак. У цих випадках закон встановлює термін покарання до 10 років позбавлення волі. CMA також встановлює кримінальну відповідальність за дії щодо отримання, виготовлення, пристосування, постачання чи пропонування дій, з метою вчинення правопорушень.

На законодавчому рівні уряд впровадив GDPR, Директиву (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у контексті обробки персональних даних компетентними органами з метою запобігання правопорушенням, їх розслідування, виявлення чи переслідування злочинців або виконання покарань, а також про вільний рух таких даних та скасування Рамкового рішення Ради 2008/977/JHA[110], NISR та Директиви 2013/40/ЄС Європейського Парламенту та Ради від 12 серпня 2013 року про напади на інформаційні системи та заміну Рамкового рішення Ради 2005/222/JHA[111], яка рекомендує виробити єдині підходи до видів покарань за кіберправопорушення у ЄС. Уряд також ухвалив Положення про конфіденційність та електронні комунікації 2003 (PECR), яке імплементує Директиву 2002/58/ЄС Європейського Парламенту та Ради від 12 липня 2002 року щодо обробки персональних даних та захисту конфіденційності в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації)[112], тим самим покладаючи на публічних постачальників послуг електронного зв'язку зобов'язання вживати відповідних технічних та організаційних заходів для захисту безпеки своїх послуг.

110 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

111 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040

112 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

На недержавному рівні серія міжнародних стандартів ISO 27000:2013 встановлює процедури щодо інформаційної безпеки, зокрема вимоги щодо оцінювання ризиків та поводження з ними з урахуванням потреб організації, а також загальні вимоги. ISO 27000: 2016 містить огляд систем управління інформаційною безпекою, термінів та визначень, які зазвичай використовуються в 27000 серії стандартів «Системи управління інформаційною безпекою».

У Великій Британії немає юридичної вимоги щодо обов'язковості застосування стандартів, але якщо організація застосовує їх до своїх операцій з даними, це може забезпечити додаткові докази належного управління даними у випадку цивільного позову, цивільного покарання або навіть у випадку притягнення до відповідальності за злочин, визначений у DPA.

Критична національна інфраструктура та сектори, що надають основні послуги, у NISR підпадають під визначення OEC. Вони повинні вживати відповідних та доцільних технічних і організаційних заходів з управління ризиками, пов'язаними з безпекою мережі та інформаційних систем, через які надаються їхні основні послуги, та вживати відповідних і доцільних заходів для запобігання безпековим інцидентам та мінімізації їхнього впливу. Якщо певна OEC не дотримується цих стандартів, можуть бути застосовані штрафи та інші стягнення.

У разі кібернападів винні особи можуть бути притягнуті до відповідальності відповідно до CMA за свідоме використання комп'ютера з несанкціонованою метою, що спричиняє або створює значний ризик завдавання шкоди добробуту людини, довкіллю, економіці чи національній безпеці будь-якої країни (розділ 3ZA CMA). До інфраструктури та секторів, які цей закон прагне захистити від «збоїв», зараховано сфери постачання продовольства, енергетики, палива та водопостачання, крім комунікаційних і транспортних мереж та медичних послуг. За злочини, передбачені цим розділом (коли виникає значний ризик завдавання серйозної шкоди добробуту людини або національній безпеці), встановлено максимальні покарання аж до довічного позбавлення волі (від 14 років позбавлення волі за будь-яке інше правопорушення, передбачене цим розділом).

Кібербезпека належить до сфери компетенції міжурядової групи Government Emerging Technology and Innovation Analysis Cell (ETIAC), створеної з метою виявлення технологічних загроз і визначення можливостей, пов'язаних із національною безпекою. Крім того, питаннями кібербезпеки у своїй діяльності опікуються й такі усталені структури, які займаються питаннями «сканування горизонтів»: зокрема, урядова група Government Futures Group (GFG) і консультативна група при секретарі кабінету (Cabinet Secretary's Advisory Group, CSAG).

У листопаді 2019 року уряд опублікував Дослідження щодо стимулювання кібербезпеки та перегляд регламенту 2020: Заклик до доказів[113].

Уряд прагне стимулювати інвестиції у зменшення кіберризиків, просуваючи думку про те, що це сприяє безперервності бізнесу та його сталості. В огляді викладено, як уряд може безпосе-

113 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/844081/Call_for_Evidence_-_Cyber_Security_Incentives___Regulation_Review.pdf

редньо втручатися в цю сферу, не покладаючи зайвих тягарів на бізнес, а також підтримувати та стимулювати промисловість, сприяючи усуненню бар'єрів для ефективного управління кіберризиками.

Організації заохочують повідомляти про напади, і це ключовий чинник боротьби з кіберінцидентами. Ніяких вимог чи стимулів немає, хоча уряд намагався сприяти обміну інформацією про кіберзагрози в рамках Партнерства для обміну інформацією про кібербезпеку (CiSP)[114].

Міська поліція міста Лондона створила вебсайт, що використовуватиметься у боротьбі з шахрайством, для повідомлення про шахрайство, афери та вимагання в Інтернеті. Про кіберінциденти можна повідомити безпосередньо NCSC, якщо вони впливають на національну безпеку Великої Британії чи економічний добробут, зачіпають значну частку населення країни або ставлять під загрозу подальше функціонування організації.

У Національній стратегії кібербезпеки до 2021 р. визнано важливість трансформацій, що сприятимуть впровадженню цифрових технологій як публічними, так і приватними підприємствами, але наголошено на значній ролі бізнесу та організацій у реагуванні Великої Британії на кіберзагрози.

З огляду на важливість партнерства між урядом та приватним сектором у розробці стандартів кібербезпеки на вебсайті NCSC створено спеціалізовану сторінку, де перераховані зусилля, спрямовані на розвиток можливостей міжсекторної кібербезпеки у Великій Британії, зокрема навчальні заходи та створення робочих місць для виховання майбутніх спеціалістів з кібербезпеки, освітні заходи для поточних фахівців з кібербезпеки, та ініціативу «Промисловість 100», орієнтовану на сприяння тісній співпраці з талантами приватного сектору в галузі кібербезпеки шляхом заохочення роботи на NCSC на неповний робочий день та підтримки обміну досвідом і знаннями.

Що ж до окремих галузей, то у Великій Британії реалізується також ініціатива techUK, що представляє понад 850 комерційних організацій, дотичних до кіберсфери, зокрема 100 компаній FTSE, малі та середні підприємства й стартапи. NCSC працює з ключовими заінтересованими сторонами, інформуючи спільноту про подальший розвиток та застосування технологій.

У Великій Британії доступний ще один інструмент — страхування для зменшення ризиків кібербезпеки. Цей ринок зазвичай вважали недостатньо розвиненим, але зараз обсяги такого страхування постійно зростають. Внаслідок потенційного ризику впливу, недооцінки звітів та дефіциту актуарних розрахунків страхові компанії з обережністю надавали продукти страхування. Тим не менше, із збільшенням кількості випадків і наслідків порушення кібербезпеки попит на страхування зростає. Потенційна фінансова та репутаційна вартість для бізнесу надзвичайно висока, особливо коли компанія стикається з подвійною катастрофою — прямими фінансовими втратами внаслідок порушення та великим штрафом за порушення конфіденційності особистих даних.

114 https://www.ncsc.gov.uk/information/cyber-security-information-sharing-partnership--cisp-

За дотримання правил кібербезпеки в основному відповідають такі регуляторні органи.

GCHQ — провідна агенція з питань розвідки, кібербезпеки та безпеки у світі, місією якої є захист Великої Британії. Для виявлення, аналізу та нівеляції загроз співробітники агенції використовують передові технології, технічні винаходи та широкі партнерські зв'язки. Пріоритети агенції визначені Стратегією національної безпеки та рішенням Ради національної безпеки під головуванням прем'єр-міністра, а також Об'єднаного комітету з розвідки.

Для виконання своїх завдань агенція використовує низку інструментів, зокрема суворо регламентовані законодавством методи збору інформації, що містить цінні дані; аналіз зв'язків та зібраних даних для укладення звітів про розвідку; засоби в таких царинах:

- протидія тероризму — запобігання терактам у Великій Британії та діям, спрямованим проти британських інтересів за кордоном;
- кібербезпека — перетворення Великої Британії на найбезпечніше місце для життя та ведення бізнесу в Інтернеті;
- стратегічна перевага — протистояння загрозам з боку ворожих держав, сприяння процвітанню Великої Британії та формування міжнародного середовища;
- тяжкі злочини та організована злочинність — зменшення соціальної та фінансової шкоди, яку тяжкі злочини та організована злочинність завдають Великій Британії;
- підтримка оборони — захист персоналу та активів оборони й підтримка комплексного підходу до воєнних дій.
- Конкретніше цілі й завдання NCSC визначено на сайті організації. Так, ця інституція:
- «розуміє кібербезпеку і перетворює ці знання на практичні вказівки, доступні для всіх;
- реагує на інциденти в сфері кібербезпеки, щоб зменшити шкоду, якої вони завдають організаціям та загалом Великій Британії;
- використовує галузеві та академічні знання для розвитку можливостей забезпечення й захисту кібербезпеки у Великій Британії;
- зменшує ризики для Великої Британії, забезпечуючи захист мережі державного та приватного секторів»[115].

NCSC створений у жовтні 2016 року зі штабквартирою в Лондоні й об'єднав компетенції CESG (відділу забезпечення інформації GCHQ), Центру оцінювання кібербезпеки, CERT-UK та Центру захисту національної інфраструктури.

NCSC є єдиним контактним пунктом для малого і середнього бізнесу, великих організацій, державних установ, широкої громадськості та урядових департаментів. Центр співпрацює з іншими правоохоронними органами, оборонними відомствами, службами розвідки та безпеки Великої Британії та міжнародними партнерами.

115 https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

Регуляторним органом, відповідальним за виконання правил кібербезпеки, є спеціалізований Національний підрозділ з кіберзлочинності (NCCU) в рамках NCA та ICO. У випадку загроз національній безпеці залучаються органи безпеки та розвідки Великої Британії.

Окрім NCCU та ICO, працюють такі професійні регулятори, як FCA та Орган, що регулює здійснення адвокатської діяльності, які контролюють забезпечення кібербезпеки в окремих секторах.

Кіберзлочинців, як правило, переслідує Королівська прокурорська служба, хоча ICO також має повноваження притягнути до кримінальної відповідальності відповідно до CMA та DPA.

Наразі Велика Британія стикається з певними труднощами в частині регулювання питань кібербезпеки у зв'язку з виходом з Європейського Союзу (Brexit).

З огляду на транснаціональний характер кіберзлочинності доведено, що регулювання кібербезпеки та боротьби з кіберзлочинністю суто на національному рівні недостатньо, а участь Великої Британії у міжнародних органах після Brexit є предметом значних дискусій. Постійне міжнародне співробітництво в інтересах кожного, і можна сподіватися, що після Brexit Велика Британія й надалі братиме участь у роботі органів кібербезпеки ЄС, зокрема Європейського агентства з мережевої та інформаційної безпеки [116] та Групи співробітництва з питань захисту мереж та інформації, як сторонній учасник, що, з огляду на значний передовий досвід Британії, значно посилило б європейську кібербезпеку.

Оскільки GDPR все ще перебуває на стадії впровадження, Велика Британія декларує подальші законодавчі заходи, спрямовані на підвищення стандартів кібербезпеки.

Важливо, що Велика Британія планує впровадження стандартів, рівнозначних GDPR, коли закінчиться перехідний період для Brexit — 31 грудня 2020 року або пізніше. Стандарти ЄС усталилися як загальноприйняті норми обробки даних та контролю відносин між суб'єктом даних і тим, хто ці дані обробляє або контролює; по суті, обов'язок зберігати дані залишається вирішальним для ефективної демократії та ведення бізнесу, незалежно від того, входить країна до складу ЄС чи ні.

Компанії можуть впливати на рівень кібербезпеки, дотримуючись найкращих практик та за допомогою договірних умов наполягаючи на тому, щоб весь їхній ланцюг постачання й треті сторони, з якими вони працюють, втілювали так само високі стандарти; тим самим ці компанії підвищують рівень кіберзахисту і, як правило, знижують ризик штрафних санкцій.

Виняток із законодавчих правил може становити сфера штучного інтелекту (AI). AI є дуже потужним інструментом для розуміння та виявлення кібератак, тим більше, з огляду на унікальну здатність AI виявляти структури діяльності та екстраполювати дані, передбачати появу наступного покоління, зійснювати самонавчання. Однак AI залишається суперечливим інстру-

116 https: //www.enisa.europa.eu/about-enisa

ментом. Будь-які законодавчі акти, що регулюватимуть його контроль, мають укладатися з урахуванням тієї вирішальної ролі, яку штучний інтелект відіграватиме в забезпеченні ефективного та кращого кіберзахисту.

Тому найближчим часом Велика Британія приділятиме значну увагу саме питанням регулювання AI[117].

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ВЕЛИКОЇ БРИТАНІЇ

1 листопада 2016 р. канцлер казначейства Великої Британії Філіп Хеммонд офіційно представив нову національну стратегію кібербезпеки, в якій викладено цілеспрямовані заходи щодо захисту економіки країни та недоторканності особистого життя громадян. Стратегія розроблена на період з 2016 до 2021 року включно.

Велика Британія є країною з високим рівнем проникнення цифрових технологій, які суттєво збагатили економіку й повсякденне життя людей. Але трансформація, пов'язана з повсюдним проникненням цифрових технологій в життя, створює нові залежності. Економіка, управління державою і надання основних послуг залежать від цілісності кіберпростору, а також інфраструктури, систем і даних, що лежать у його основі. Втрата впевненості в цій цілісності може поставити під загрозу переваги технологічної революції.

Значна частина обладнання та програмного забезпечення, яка від початку розробляється для підтримки цього взаємозалежного цифрового середовища, головним чином орієнтована на аспекти ефективності, вартості й зручності користування, але не завжди враховує безпеку. **Зловмисники — ворожі держави, злочинні або терористичні організації та особи** — можуть скористатися вразливостями, пов'язаними з цим розривом між зручністю й безпекою. Скорочення цього розриву є одним з національних пріоритетів Великої Британії.

З виходом Інтернету за рамки комп'ютерів і мобільних телефонів — в інші кібернетичні або «розумні» системи — небезпека віддаленого несанкціонованого використання поширюється на цілу низку нових технологій. Системи і технології повсякденного життя, такі як електромережі, системи управління повітряним рухом, супутники, медичні технології, промислові підприємства й світлофори, підключені до Інтернету, тож їм потенційно загрожує несанкціоноване втручання.

117 https://www.gov.uk/government/publications/technology-innovation-in-government-survey/technology-innovation-in-government-survey

Національна стратегія безпеки 2015 року (NSS) ще раз підтвердила, що загрози для британських інтересів в кіберпросторі є ризиками першого рівня. У NSS окреслено твердий намір Уряду боротися з кіберзагрозами і, «будучи світовим лідером у галузі кібербезпеки, розробити жорсткі інноваційні заходи»[118].

Розробляючи цю стратегію, уряд Великої Британії спирався на досягнення, цілі та оцінки першої п'ятирічної Національної стратегії кібербезпеки, ухваленої 2011 року. Протягом 2011–2016 років Велика Британія інвестувала в кібербезпеку 860 млн фунтів. Політика, інститути та ініціативи, розроблені за останні п'ять років, допомогли зміцнити позиції Великої Британії як провідного глобального гравця в галузі кібербезпеки.

Для ефективного захисту інтересів країни в кіберпросторі уряд наголошує на необхідності комплексного підходу, тож для заходів, сформованих на основі аналізу за попередні роки, планується виділити ще більше коштів. Зокрема уряд дійшов таких висновків: :

- унаслідок масштабу й динамічної природи кіберзагроз, а також вразливості й залежності, поточний підхід сам по собі не забезпечує достатнього рівня безпеки;
- **ринковий підхід до просування елементарних правил кібербезпеки не забезпечив необхідних темпів і масштабу змін**; тому уряд має виявити ініціативу й уживати активніших заходів, використовуючи свій вплив і ресурси для боротьби з кіберзагрозами;
- уряд сам по собі не в змозі охопити всі аспекти національної безпеки. Потрібно впроваджувати інтегрований і сталий підхід, який передбачає залучення громадян, представників галузі та інших партнерів в суспільстві й владі до повноцінної участі в забезпеченні безпеки мереж, послуг і даних;
- Великій Британії потрібен життєздатний сектор кібербезпеки і відповідний кадровий резерв, які допоможуть йти в ногу із загрозами, що еволюціонують, і випереджати їх розвиток.

Стратегія спрямована на формування політики уряду, а також послідовного та переконливого бачення, яке можна представити громадськості, бізнесу, громадянському суспільству, науковим інституціям і ширшим колам населення.

Стратегія охоплює все Сполучене Королівство Великої Британії та Північної Ірландії, передбачає співпрацю з адміністративними частинами — Шотландією, Уельсом та Північною Ірландією — та їхніми урядами, застосування окреслених у документі засад і принципів на цих територіях (із повагою до наявних у країні трьох окремих правових юрисдикцій і чотирьох систем освіти).

Запропоновані у Стратегії дії націлені на всі сектори економіки і суспільства, від урядових департаментів і до провідних підприємств та окремих громадян. Метою стратегії визначено підвищення кібербезпеки на всіх рівнях задля загального блага.

118 https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

Відповідно до оцінки викликів і задля зміцнення й розширення досягнень стратегії 2011 року в Стратегії викладено:

- оновлену оцінку стратегічного контексту, зокрема поточних і майбутніх загроз: хто становить найбільшу небезпеку для інтересів країни і які кошти є в їхньому розпорядженні;
- огляд вразливостей і їх еволюцію протягом останніх п'яти років;
- бачення кібербезпеки у 2021 році та основні віхи на шляху його реалізації, керівні принципи, ролі й обов'язки, а також опис того, яким чином і в яких галузях втручання уряду може справити позитивний вплив;
- шляхи реалізації політики з описом галузей, у яких уряд має очолити роботу, і галузей, в яких він працюватиме в партнерстві з іншими інституціями;
- методи оцінювання прогресу в досягненні поставлених цілей.

ОСНОВНІ ЗАГРОЗИ Й ВИКЛИКИ, ВИЗНАЧЕНІ В СТРАТЕГІЇ

Кіберзлочинці

Стратегія розглядає кіберзлочинність у контексті двох взаємопов'язаних форм злочинної діяльності:

- кіберзалежні злочини — злочини, які можна скоїти тільки з використанням пристроїв на основі інформаційно-комунікаційних технологій (ІКТ) і в яких ці пристрої є як знаряддям, так і метою злочину (тобто ідеться про розробку та поширення шкідливих програм з метою фінансового збагачення, злам з метою крадіжки, пошкодження, спотворення або знищення даних та / або мережі чи діяльності;
- злочини з використанням кіберпростору — «традиційні» злочини (наприклад, шахрайство або крадіжка даних), масштаб і охоплення яких можна збільшити за рахунок використання комп'ютерів, комп'ютерних мереж тощо.

ІКТ

Більшу частину найсерйозніших кіберзлочинів проти Великої Британії (в основному, шахрайства, крадіжки й вимагання), як і раніше, здійснюють **фінансово мотивовані організовані російськомовні злочинні угруповання (ОЗУ) в країнах Східної Європи**, при цьому значна частина ринку кримінальних послуг розміщується на комп'ютерах в цих країнах. **Однак загрози походять також із інших країн і регіонів, включно із Великою Британією; при цьому дедалі більшу стурбованість викликає поява загроз із країн Південної Азії і Західної Африки**.

Навіть коли вдається встановити головних осіб, причетних до найбільш руйнівних кібератак проти Великої Британії, і міжнародні, і британські правоохоронні органи не часто в змозі притягти їх до відповідальності, бо вони перебувають під юрисдикцією країн, із якими домовленості про екстрадицію обмежені або взагалі відсутні.

У розробці й розгортанні дедалі досконаліших шкідливих програм, що заражають комп'ютери і мережі британського суспільства, підприємств і уряду, передусім винні ці ОЗУ. Їхня діяльність впливає на всю територію Великої Британії, справляючи значний сукупний ефект. Ці атаки стають дедалі агресивнішими й зухвалішими, про що свідчать зрослі масштаби використання програм-вимагачів і загроз використання розподілених атак типу «відмова в обслуговуванні» (DDoS) в здирницьких цілях. **ОЗУ можуть становити значну загрозу колективному добробуту й безпеці, утім, не меншу стурбованість викликає загроза не таких складних, але більш поширених кіберзлочинів проти окремих осіб і невеликих організацій.** Обсяги **шахрайства** в дистанційному банківському обслуговуванні, зокрема шахрайського зняття коштів із банківських рахунків клієнтів за допомогою інтернет-банкінгу, збільшилися на 64% і сягнули 133,5 млн фунтів у 2015 р. Кількість злочинів зростала повільно (23%), що, на думку організації Financial Fraud Action UK (дані відстежуються кожні три роки)[119], свідчить про схильність злочинців вибирати об'єкти для атаки серед компаній і заможних клієнтів.

Загрози, що виходять від іноземних держав і спонсоруються ними

Велика Британія регулярно спостерігає спроби з боку держав і груп, що користуються державною підтримкою, проникнути в британські мережі, щоб отримати політичні, дипломатичні, технологічні, комерційні та стратегічні переваги, насамперед у державному, оборонному, фінансовому, енергетичному і телекомунікаційному секторах. Обсяг і вплив таких державних кіберпрограм може бути різним. Самі технологічно розвинені держави продовжують стабільно покращувати свої можливості, інтегруючи в свої інструментальні засоби сервіси шифрування й анонімізації, щоб приховати своє втручання. Хоча вони й мають в своєму розпорядженні технічні можливості для розгортання складних атак, своїх цілей вони часто досягають за допомогою елементарних інструментів і прийомів, користуючись слабкою захищеністю і вразливістю об'єктів злочину. Лише деякі держави мають технічні можливості для розгортання атак, які становлять серйозну загрозу для безпеки й добробуту Великої Британії в цілому. Однак багато інших держав займаються розробкою новітніх кіберпрограм, які можуть становити загрозу інтересам Великої Британії в недалекому майбутньому. Багато держав, які прагнуть розширити свої можливості кібершпигунства, мають можливість купити інструментальні засоби, що дають змогу використовувати вразливості мереж, в готовому вигляді й переорієнтувати їх для шпигунства. Крім засобів шпигунства, незначна кількість ворожих іноземних зловмисників розробляють і розгортають можливості наступальних дій у кіберпросторі, зокрема руйнівного характеру. Це загрожує безпеці критично важливої національної інфраструктури Великої Британії та промислових систем управління.

119 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2018

Деякі держави використовують такі можливості в порушення міжнародних законів, бо впевнені у своїй відносній безкарності, тож таким чином заохочують інших наслідувати їхній приклад. Хоча руйнівні атаки залишаються рідкісним явищем у світі, їх кількість зростає і вплив посилюється.

Терористи

Терористичні групи й надалі плекають плани руйнівних кібератак проти Великої Британії та її інтересів. Наразі технічні можливості терористів оцінюються як низькі. Проте вплив, який досі мала їхня діяльність, навіть така непрофесійна, проти Великої Британії, був непропорційно високим: **простий дефейс сайтів і доксинг (оприлюднення розкритих особистих даних у мережі) дали терористичним групам і їхнім прихильникам змогу привернути увагу ЗМІ та залякати своїх жертв**. «Використання терористами Інтернету в своїх цілях не прирівнюється до кібертероризму. Однак можна припустити, що з активізацією їхньої діяльності в кіберпросторі і за наявності доступу до кіберзлочинів як послуги вони могли б отримати можливість здійснення кібератак»[120].

Згідно з поточними оцінками експертів, у майбутньому пріоритетом для терористичних груп залишатимуться саме фізичні терористичні атаки, а не кібератаки. **З долученням до екстремістської діяльності покоління з високими цифровими навичками і появою можливості обміну просунутими технічними вміннями** можна очікувати збільшення обсягу діяльності проти Великої Британії (дефейс або DDoS-атаки). Крім того, **підвищується ймовірність появи низки кваліфікованих екстремістів-одинаків**, як і ризик намагань з боку терористичних організацій завербувати інсайдерів з числа співробітників, що давно працюють в організаціях. Досить імовірно, що терористи звертатимуться до будь-яких кіберзасобів для досягнення максимального ефекту. Таким чином, навіть помірне розширення можливостей терористів може являти собою істотну загрозу для Великої Британії та її інтересів.

Хактивісти

Групи хактивістів децентралізовані і орієнтовані на певні ідеї. Вони формуються і вибирають об'єкти для атак як відповідь на те, що викликає в них невдоволення, привносячи таким чином в багато своїх дій елемент «народної помсти». Значна частина кібердіяльності хактивістів дезорганізуюча за своєю природою (дефейс веб-сайтів або атаки DDoS), та дії найталановитіших із них заподіяли набагато серйознішу шкоду й спричинили тривалі наслідки для їхніх жертв.

120 ENISA Threat Landscape 2015

Інсайдери

Інсайдерські загрози залишаються ризиком для безпеки британських організацій у кіберпросторі. **Найбільшу загрозу становлять внутрішні зловмисники, які користуються довірою у своїх організаціях і мають доступ до критично важливих систем і даних**. Вони здатні заподіяти фінансові втрати і підірвати репутацію шляхом крадіжки секретних даних і об'єктів інтелектуальної власності. Вони також можуть становити загрозу деструктивної кібердіяльності, якщо скористаються особливими знаннями чи доступом для здійснення атаки або сприяння їй з метою виведення з ладу чи погіршення критично важливих послуг у мережі організації або знищення даних. Не меншу стурбованість викликають і ті інсайдери або співробітники, які можуть випадково завдати шкоди організації, якщо ненавмисно перейдуть за посиланням у фішинговому повідомленні, вставлять у комп'ютер USB-накопичувач, заражений вірусом, або знехтують правилами безпеки і завантажать небезпечний вміст із мережі. І хоча у них немає наміру навмисне нашкодити, вони здатні завдати організації не менш істотної шкоди, ніж внутрішні зловмисники, бо володіють особливими правами доступу до систем і даними. **Ці особи часто стають жертвами соціальної інженерії**. **Вони можуть, самі не усвідомлюючи того, надати шахраям доступ до мереж своєї організації або з найкращих намірів виконати їхні вказівки.** Загальний ризик для організації, пов'язаний із інсайдерськими погрозами, стосується не тільки несанкціонованого доступу до інформаційних систем і їх вмісту. Не менше значення мають засоби фізичної безпеки, використовувані для захисту цих систем від незаконного втручання або виносу секретних даних чи захищеної авторським правом інформації, записаних на носіях будь-якого типу. Тож важливим елементом комплексного підходу до безпеки є розвинута культура безпеки серед персоналу, яка сприяє виявленню загроз з боку незадоволених працівників, випадків шахрайства серед персоналу, а також промислового і іншого шпигунства.

«Скрипт-кідді»

За оцінками, наведеними у Стратегії, так звані «скрипт-кідді» — це, як правило, дилетанти, які користуються скриптами або програмами, розробленими іншими, для атаки комп'ютерних систем і мереж; вони не становлять серйозної загрози для економіки або суспільства. Однак вони мають доступ до хакерських посібників, ресурсів та інструментів через Інтернет. В силу вразливостей систем із виходом в Інтернет, що використовуються багатьма організаціями, дії «скрипт-кідді» можуть у деяких випадках мати непропорційно серйозні наслідки для постраждалої організації.

ВРАЗЛИВОСТІ

Дедалі більше розмаїття пристроїв

Коли в 2011 році була опублікована Національна стратегія кібербезпеки Великої Британії, більшість людей сприймали кібербезпеку крізь призму захисту пристроїв на кшталт комп'ютерів чи ноутбуків. Відтоді Інтернет інтегрується в усі сфери життя, хоча люди часто цього не усвідомлюють. **«Інтернет речей» відкриває нові можливості для зловмисників і підвищує ймовірність атак, здатних завдати фізичної шкоди, спричинити травми і, в гіршому випадку, смерть**. Швидке впровадження можливостей підключення до мережі в критично важливих промислових системах управління процесами в низці таких галузей, як енергетика, видобувна промисловість, сільське господарство і авіація, призвело до виникнення «промислового інтернету речей». Так з'являються можливості злому пристроїв і процесів, які в минулому були невразливими до такого втручання, що може мати катастрофічні наслідки. **Таким чином, країні загрожує небезпека, пов'язана не тільки з неналежною кібербезпекою особистих пристроїв, але і з взаємопідключенням систем, що має фундаментальне значення для суспільства, здоров'я і добробуту**.

Низький рівень елементарних правил кібербезпеки і дотримання нормативних вимог

Без сумніву, рівень усвідомлення технічних вразливостей програмного забезпечення і мереж, як і розуміння необхідності дотримання елементарних правил кібербезпеки у Великій Британії за останні п'ять років зріс. З одного боку, це результат таких ініціатив, як урядовий план «10 кроків до кібербезпеки», а з іншого — наслідок розголосу навколо кіберподій, що спричиняють негативні наслідки для урядів і корпорацій. Кібератаки не завжди бувають просунутими або неминучими, часто вони є результатом використання вразливостей, які можна легко усунути або запобігти їм. **У більшості випадків саме вразливість жертви, а не винахідливість злочинця є чинником, що визначає успіх кібератаки.** Компанії та організації приймають рішення про вкладення коштів в кібербезпеку, виходячи з оцінки ефективності витрат, і зрештою несуть відповідальність за безпеку своїх даних і систем. *Знизити ймовірність кібератаки можна тільки завдяки досягненню необхідного балансу між ризиком порушення безпеки критично важливих систем і конфіденційних даних, з одного боку, і вкладенням достатніх коштів у людей, технології та управління, з іншого.* «Не існує системи інформаційної безпеки, здатної виключити ймовірність, що хоча б одна людина зі ста відкриє фішингове повідомлення, і цього може бути достатньо для зловмисника»[121].

121 Киаран Мартін, генеральний директор з кібербезпеки, GCHQ, червень 2015 р

Низький рівень підготовки та кваліфікацій

Щоб задовольнити потреби в кібербезпеці в масштабах державного і приватного секторів, бракує фахівців. У компаніях рівень обізнаності персоналу в питаннях кібербезпеки низький, працівники не розуміють своєї відповідальності в цій царині, що частково пояснюється недостатнім рівнем планового навчання. Населення також недостатньо поінформоване про кібербезпеку.

«У минулому році менш ніж 20% компаній організували для своїх співробітників тренінги з питань кібербезпеки»[122]. У Стратегії йдеться про необхідність підготовки фахівців і розвитку можливостей, які дадуть змогу не відставати від технологій, що швидко еволюціонують, і управляти кіберризиками. **Брак кваліфікованих кадрів є вразливістю на національному рівні, яку необхідно усунути.**

Застарілі системи і невиправлені вразливості

Багато організацій у Великій Британії продовжують використовувати вразливі застарілі системи аж до наступного етапу модернізації своїх IT-систем. У цих системах часто використовуються старіші, невиправлені версії програмного забезпечення. Зловмисники знаходять уразливості в таких застарілих версіях, маючи необхідні засоби для їх використання. Інша проблема полягає у використанні деякими організаціями непідтримуваного програмного забезпечення, для якого немає режиму виправлення. «Нещодавно ми проаналізували 115000 пристроїв Cisco, використовуваних в інтернеті й у середовищах наших клієнтів, щоб привернути увагу до ризиків безпеки, пов'язаних із застарілою інфраструктурою, адже побачили, що усуненню вразливостей не приділяють належної уваги... Аналіз показав, що 106000 з 115000 пристроїв містять відомі вразливості у використовуваному на них програмному забезпеченні»[123].

Доступність хакерських ресурсів

Доступність в інтернеті хакерської інформації і простих у використанні хакерських інструментів дає все необхідне в руки тих, хто зацікавлений у розвитку хакерських можливостей. Інформація, необхідна хакерам для успішного злому, часто перебуває у відкритому доступі, й отримати її можна досить швидко. Кожна людина, від простого користувача до члена ради директорів, має усвідомлювати рівень небезпеки, що загрожує її персональним даним і системам в Інтернеті, ступінь своєї уразливості до зловмисних кібератак у зв'язку з цим.

«99,9% вразливостей були використані зловмисниками більш ніж через рік після того, як була опублікована інформація про них»[124].

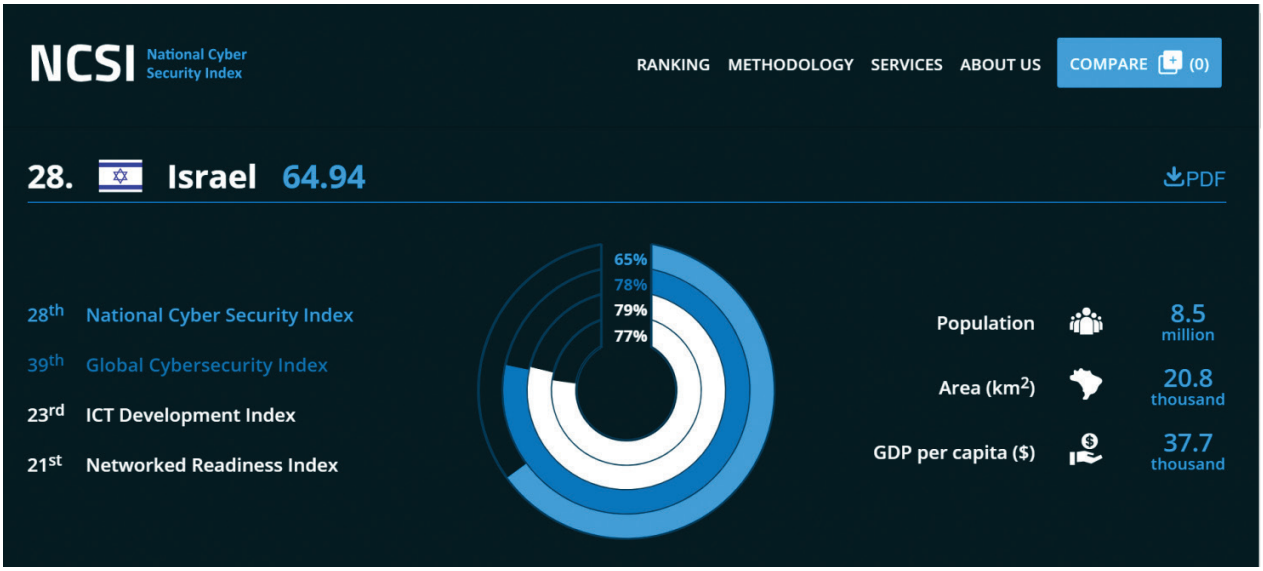
---

122 Опитування думок про порушення кібербезпеки, 2016 р

123 Щорічний звіт Cisco з інформаційної безпеки, 2016 р.

124 Звіт про розслідування Verizon 2015 Data Breach

ІЗРАЇЛЬ



Національні заходи та інституції кібербезпеки в Ізраїлі впроваджені вже доволі давно — Національне кібербюро Ізраїлю (INCB) створено двадцять років тому. І ця царина й надалі активно розвивається в складних умовах військових та цивільних загроз. Розгалужена система кібербезпеки й наявність Національного кібербюро цілком виправдані, адже в країні дуже високий рівень комп'ютеризації і, відповідно, багато організацій вразливі до кібератак.

INCB покликане допомагати прем'єр-міністру, уряду та його комітетам у формуванні національної кіберполітики та забезпеченні всіх аспектів національної безпеки. Зокрема, INCB було доручено розробити національну стратегію кібербезпеки.

Процес розробки стратегії посприяв розгортанню на національному рівні важливої фахової дискусії щодо можливостей створення оперативного органа, відповідального за захист цивільного кіберпростору.

Потреба в цьому ніколи не викликала сумнівів; однак навколо способів реалізації точилося чимало гострих суперечок. Зрештою було ухвалено урядове рішення про створення цивільного органу в кабінеті прем'єр-міністра — NCSA (National Cyber Security Authority)[125].

«Ізраїль постійно в стані протистояння і змушений підтримувати готовність до відбиття кібератак, — каже Андрій Тархов, директор департаменту захисту інформаційних систем компанії RedSys. — Внаслідок цього всі «технічні» аспекти життя ізраїльтян зведені до питань кібербезпеки. Це формує відповідні потреби — щодо технологій та їх реалізації в кінцевих продуктах»[126].

У листопаді 2010 року кібербезпека стала для Ізраїлю чітко визначеною національною метою — прем'єр-міністр оголосив про започаткування «Національної кіберініціативи» в рамках проєкту Міністерства науки під егідою Національної ради з досліджень та розробок. Цю спеціальну мультидисциплінарну робочу групу очолив голова Національної ради з досліджень і розробок, до складу якого входять близько вісімдесяти фахівців — військові, представники урядових структур, науковці та представники приватного сектора.

Прем'єр-міністр доручив «Національній кіберініціативі» працювати над забезпечення лідерської позиції Ізраїлю в питаннях кібербезпеки на глобальному рівні.[127]. У серпні 2011 року уряд ухвалив постанову №3611 «Посилення національних можливостей у кіберпросторі».

СУБ'ЄКТИ КІБЕРБЕЗПЕКИ

Постановою Уряду №2444[128] від 15 лютого 2015 року Ізраїль також постановив створити нову державну структуру – Національне управління з питнаь кібербезпеки National Cyber Security Authority (NCSA).

Національне управління з питнаь кібербезпеки (NCSA)

NCSA розпочав свою діяльність у 2016 році й став осередком накопичення інформації, першим кіберрегулятором та оперативним центром управління кіберінцидентами. NCSA також проводило спільні оборонні заходи з національними оборонними відомствами та правоохоронними органи.

NCSA створено як орган, який поєднує в собі військову безпеку та можливості цивільних структур й призначений у синергії з усіма іншими організаціями у сфері національної безпеки організовувати захист від кібератак, спрямованих на цивільні інституції Ізраїлю.

Одне з основних завдань NCSA — надання ізраїльським організаціям та громадськості допомоги в боротьбі з кіберзагрозами незалежно від їхнього джерела й виконавця.

125 https://www.haaretz.com/shin-bet-loses-authority-over-civilian-cyberspace-1.5304267

126 http://goldameir.institute/uk/2017/10/izrayil-lidiruye-v-rejtingu-krayin-za-rivnem-borotbi-z-kiberzlochinnistyu/

127 https://mfa.gov.il/MFARUS/PressRoom/2011/Pages/Israeli_government_increases_cybersecurity.aspx

128 https://ccdcoe.org/uploads/2019/06/Government-Resolution-No-2444-Advancing-the-National-Preparedness-for-Cyber-Security.pdf

Ця допомога реалізується через CERT NCSA (національний CERT). Розташований у місті Беер-Шева на півдні Ізраїлю, CERT цілодобово надає допомогу широким колам суб'єктів — від національних компаній критичної інфраструктури до пересічних громадян. На додачу до CERT створено спеціальні галузеві центри, які допомагають міністерствам, фінансовому та енергетичному сектору і вже засвідчили, наскільки цінним є накопичення такого галузевого досвіду.

Національне кібербюро (INCB)

Постановою №2443[129] того ж року було створено Національне кібербюро (INCB) як перший національний консультативний та консолідаційний орган у сфері кібербезпеки.

INCB — це національна агенція з безпеки та технологій, відповідальна за захист національного кіберпростору Ізраїлю, а також за встановлення лідерства Ізраїлю в кіберсили. INCB працює на національному рівні над постійним посиленням захисту організацій та громадян, запобіганням кібератакам та боротьбою з ними, розширенням можливостей реагування на надзвичайні ситуації. У межах своїх завдань і повноважень INCB просуває інноваційні кіберрішення та перспективні технологічні рішення, формулює стратегії та політику на національній та міжнародній аренах та розвиває свою кібер-робочу силу. INCB має на меті підтримувати захищений, безпечний та відкритий кіберпростір для всіх громадян Ізраїлю і сприяти зростанню та потужності Ізраїлю.

Постановами №№2443 та 2444 передбачено окреслення національних пріоритетів та розширення інституційного потенціалу в галузі — шляхом створення Національної дирекції з кіберзахисту, яка буде реалізовувати обидва завдання.

Перший із цих документів — Постанова №2443 «Посилення уряду та національного регулювання» Лідерство в галузі кібербезпеки.[130]

У цьому документі окреслено підхід до інтеграції нових правил кібербезпеки до вже сформованих сфер діяльності чинних міністерств та інших регуляторних органів, надання цим органам додаткових регуляторних можливостей у власній сфері відповідальності (наприклад, Міністерство транспорту здійснюватиме стягнення з регулювання кібербезпеки задля транспортного сектору). Крім того, у Постанові №2443 викладено описано важелі регулювання ринку, що належить до сфери INCB для професіоналів кібербезпеки, служб та вироби; елементи якого детально розроблені в політичному документі 2015 року.

Другий — Постанова №2444 «Підвищення національної готовності до кіберзахисту», згідно з якою створюється новий орган: NCSA.

129 https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202443%20-%20Advancing%20National%20Regulation%20and%20Governmental%20Leadership%20in%20Cyber%20Security.pdf

130 https://www.gov.il/he/Departments/policies/2015_des2443

На NCSA покладено завдання забезпечувати захист кіберпростору шляхом впровадження та координації «всіх» оперативних оборонних зусиль у кіберпросторі на національному рівні задля постійного повномасштабного реагування на кібератаки, зокрема боротьбу із кіберзагрозами та інцидентами в режимі реального часу, гарантувати поточну ситуаційну обізнаність, консолідуючи та аналізуючи таємні дані, та співпрацювати з оборонними відомствами.

Серед інших завдань, на NCSA покладено обов'язок підтримувати ізраїльський CERT, підвищувати рівень готовності та стійкості країни до кіберзагроз, розробити національну кібердоктрину та закон про пропаганду кібербезпеки, який розширить чинне законодавство у відповідній галузі. Таким чином, урядова структура, передбачена постановами №№ 2443 та 2444, а саме Національна дирекція з кібербезпеки (Ma'arach), складається з двох інституцій — чинного INCB та нового NCSA.

Крім того, широку основу для подальшого спільного втілення цілей та пріоритетів кібербезпеки забезпечує створення у кожному міністерстві відповідних окремих підрозділів та окреслення галузевих орієнтирів для реалізації політики в галузі кібербезпеки.

Ізраїльська команда реагування на комп'ютерні надзвичайні ситуації (CERT-IL)

Ізраїльська команда реагування на комп'ютерні надзвичайні ситуації (CERT-IL) — це підрозділ урядової структури NCSA, створений відповідно до Резолюції №2444.

CERT-IL несе відповідальність за управління кіберінцидентами, з якими стикається держава, обмін інформацією з надійними партнерами в Ізраїлі та закордоном, розробку найкращих практик у галузях кібербезпеки, підвищення обізнаності з питаннями кібербезпеки, у разі кіберзагроз та кіберінцидентів виступає єдиним контактним пунктом в Ізраїлі для міжнародних корпорацій, компаній, які опікуються кібербезпекою, та інших CERT.

17 грудня 2017 року ізраїльський уряд постановою №3270 затвердив пропозицію прем'єр-міністра Біньяміна Нетаніягу про об'єднання Національного кібербюро і Національного управління з кіберзахисту в єдину Національну систему кібербезпеки, яка відповідатиме за всі аспекти кіберзахисту в цивільній сфері: від розробки політики та нарощування технологічних потужностей до оперативної роботи[131].

Армія оборони Ізраїлю (IDF)

Армія оборони Ізраїлю (IDF) десятиліттями займається питаннями кібербезпеки та кіберзагрозами, однак, згідно зі своїми підходами до оборонної політики, не оприлюднює деталей щодо бачення національної безпеки та політики у військовій сфері; зазвичай ці питання не обговорюються з громадськістю. Але у серпні 2015 року Стратегію IDF вперше було опубліковано[132].

131 https://mfa.gov.il/MFARUS/PressRoom/2017/Pages/Israeli-government-approves-creation-of-unified-cybersecurity-system.aspx

132 https://www.washingtoninstitute.org/policy-analysis/view/new-idf-strategy-goes-public

У документі окреслено кілька аспектів позиції IDF щодо кібербезпеки, зокрема вказано, що кіберпростір — це військова сфера; зроблено акцент на пріоритетності подальшої розбудови кіберзахисту та усунення порушень на стратегічному, оперативному й тактичному рівнях; визнано наявність загроз у кіберпросторі та необхідність ініціювання на організаційному рівні створення кіберкоманд у межах IDF.

У Стратегії IDF зазначено, що в умовах війни та надзвичайних ситуацій кіберзахист важливий для забезпечення сталого функціонування національних установ у періоди напруженості, а також ефективної діяльності IDF.

Загалом, серед поточних цілей та пріоритетів Ізраїлю в галузі кібербезпеки наразі слід відзначити забезпечення вищого рівня прозорості, впровадження інституційних інновацій та забезпечення державних інвестицій, як короткострокових (дотацій для компаній на заходи в галузі кібербезпеки), так і довгострокових (наприклад, програми Magshimim[133] Міністерства освіти та випускного іспиту в дослідженнях кібербезпеки для старшокласників). З 2011 року офіс прем'єр-міністра взяв на себе керівну роль у сприянні забезпеченню кібербезпеки Ізраїлю як усередині країни, так і на міжнародному рівні[134].

Питання інформаційної безпеки детально висвітлені в низці ізраїльських законів. Серед них:

- Закон про комп'ютери, 1995 р.[135];
- Закон про захист конфіденційності, 1981 р.[136];
- Відповідні нормативні акти, зокрема Положення про захист конфіденційності (Безпека даних) №5777 2017 р.
- Закон про заохочення промислових досліджень та розробок, 1984 р.[137];
- Закон про контроль над експортом оборонної продукції 2007 р.[138];
- Закон про комунікації (телекомунікації та радіомовлення), 1982 р.[139];
- Закон про регулювання безпеки в державних органах, 1998 р.[140];
- Закон про електронні підписи, 2001 р.[141].

Також 20 червня 2018 року офіс прем'єр-міністра Ізраїлю опублікував законопроєкт про кібербезпеку та національну директорат з кібербезпеки. Цей проєкт став останньою стадією процесу, що розпочався у 2010 році із створення в Ізраїлі національного органу з кібербезпеки як частини національної стратегії кібербезпеки.

133 https://www.rashi.org.il/magshimim-cyber-program
134 https://www.gov.il/he/departments/Units/yahavsoc
135 http://law.co.il/media/computer-law/computers_law_nevo.pdf
136 http://www.justice.gov.il/En/Units/ILITA/Documents/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf
137 http://www.tamas.gov.il/NR/exeres/DEAF9131-D2B3-4BA4-A804-B10C6BC7E2F7.htm
138 http://www.moital.gov.il/NR/exeres/D7EEC291-DF6C-4AE9-856F-1D45624DB4B0.htm
139 http://www.nevo.co.il/law_html/Law01/032_002.htm
140 http://www.nevo.co.il/law_html/Law01/111M1_001.htm
141 http://www.financeisrael.mof.gov.il/FinanceIsrael/Docs/En/legislation/Others/5761-2001_Electronic_Signature_Law.pdf

Перша частина законопроєкту слугує правовою основою для створення Ізраїльського національного директорату з кібербезпеки (INCD). INCD визначається як орган оперативної безпеки, підпорядкований офісу прем'єр-міністра, що повинен опікуватися захистом кіберпростору та утвердженням Ізраїлю як світового лідера в галузі кібербезпеки. На INCD покладається завдання захисту держави проти кіберзагроз, посилення спроможності Ізраїлю в боротьбі з кібератаками та просування ізраїльської кіберполітики, а також сприяння міжнародному співробітництву в кіберсфері та консультування уряду з питань, пов'язаних із кібербезпекою.

У першій частині законопроєкту окреслені певні організаційні аспекти роботи INCD. Працівники INCD підпадають під дію положень про конфіденційність, а також інших обмежень, які можуть ухвалюватися рішенням прем'єр-міністра. За законопроєктом, також створюється посада спеціаліста з кібербезпеки INCD, який контролює кіберзахист самої INCD. Крім того, згідно з першою частиною законопроєкту, формується система нагляду, що складається із зовнішнього наглядового комітету та внутрішнього підрозділу нагляду за захистом конфіденційності.

Повноваження INCD детально викладені у другій частині законопроєкту. INCD уповноважений отримувати та збирати інформацію, що стосується кібербезпеки (будь-яку інформацію, яка може сприяти виявленню, подоланню кібератак чи запобіганню їм), та дані, які можна використати для подальшого отримання інформації щодо кібербезпеки; обробляти дані з метою створення інформації, що стосується кібербезпеки, відповідно до положень законопроєкту; поширювати інформацію щодо кібербезпеки та здійснювати обмін такою інформацією із суб'єктами приватного сектора відповідно до положень законопроєкту; надавати допомогу організаціям у реагуванні на кібератаки. INCD керуватиме національною командою реагування на комп'ютерні надзвичайні ситуації (CERT), яка вже працює.

Відповідно до положень другої частини законопроєкту, працівники INCD мають право вимагати у будь-якої організації інформацію або документи, необхідні для виявлення кібератак, їх подолання або запобігання їм. Співробітникам INCD дають право входити до нежитлових приміщень та захоплювати будь-які об'єкти, якщо є обґрунтовані підстави вважати, що там може міститися «інформація, що стосується кібербезпеки». На таке вторгнення до житлових приміщень потрібна згода їхніх власників або рішення суду (за винятком надзвичайно термінових випадків).

Уповноважені працівники INCD можуть також давати організаціям (органам державної, місцевої влади, бізнес-структурам, організаціям, які надають послуги громадськості) вказівки з метою запобігання кібератакам, їх виявлення або реагування на них. Крім того, INCD може звернутися по судовий ордер, який дозволяє виконувати певні дії на комп'ютері (отримувати доступ, змінювати або копіювати комп'ютерні матеріали, наприклад дані чи програмне забезпечення, контролювати зв'язок між комп'ютерами, давати комп'ютеру команди за допомогою машиночитаної мови або встановлювати комп'ютери чи інші пристрої в комп'ютерах або в комп'ютерних мережах організацій).

Такий ордер буде наданий, якщо, на переконання суду, є розумні підстави вважати, що сталася кібератака або що існує кіберзагроза, яка може завдати шкоди життєвим інтересам. INCD може також подати запит на отримання судового ордера для відбору фіксованих даних, що дозволяють дії з мережею в організації, якщо суд вважає, що така діяльність, імовірно, допоможе виявити кібератаку. За певних надзвичайних обставин керівник INCD може дозволити здійснення таких повноважень без судового ордеру протягом максимум 24 годин, при цьому такі дії надалі має розглянути суд.

У другій частині законопроєкту містяться також положення щодо захисту конфіденційності. Зокрема, окреслено певні винятки з принципу конфіденційності у проекті, мінімізації даних та загальної заборони на розкриття інформації, отриманої INCD: інформацію можна розкрити у кримінальному провадженні у зв'язку з тяжким злочином. Крім того, згідно із законопроектом, прем'єр-міністра має встановити правила для обміну інформацією про кібербезпеку з іншими органами безпеки, зокрема поліцією.

У третій частині законопроєкту окреслено основи національного регулювання кібербезпеки для забезпечення стійкості різних секторів ізраїльської економіки та їх здатності реагувати на кібератаки. Відповідно до Постанови уряду №2118 (щодо зменшення регуляторного тиску), будь-які заходи щодо регулювання кібербезпеки, згідно із законопроєктом, мають упроваджуватися з урахуванням сумісності з міжнародними чи внутрішніми стандартами, а також доцільності їх обсягів та характеру відповідно до особливостей суб'єктів, які постраждали, виду кіберзагроз та ймовірності їх реалізації. Крім того, нормативно-правові акти вводяться в дію після оцінювання їх прямих та непрямих економічних наслідків.

Законопроєкт закладає підвалини для коригування рівня втручання уряду відповідно до серйозності ризиків, з якими стикаються різні сектори та організації. В умовах децентралізованої гібридної структури чинні регулятори, які вже працюють у тих чи інших галузях, виконуватимуть у них функції компетентних органів з питань регулювання кібербезпеки. За таких умов на ці органи покладено завдання скласти карту кіберзагроз сектора, яким вони опікуються, надавати організаціям відповідні вказівки й рекомендації на основі керівних принципів кібербезпеки INCD за погодженням із керівником INCD. Компетентний орган може також розпорядитися призначити в регульованій ним організації відповідального з кібербезпеки, який подаватиме періодичні звіти про дотримання вимог у цій галузі. Компетентні органи можуть обумовити видачу чи поновлення ліцензії такій організації відповідністю її дій наказам або вказівкам щодо кібербезпеки.

Нормативно-правове регулювання, викладене в законопроекті, також має цілеспрямований вектор надання INCD можливості безпосередньо регулювати кібербезпеку певних галузей чи організацій. INCD уповноважений регулювати кібербезпеку у галузях, перелічених у Додатку 3 закону, який ше не оприлюднений, замість того компетентного органу, що регулює сектор. Сектори можуть додаватися до додатку наказом про внесення змін, виданим прем'єр-міністром, за умови, якщо вони включають організації, що піддаються кіберзагрозам, які можуть завдати шкоди життєво важливим національним інтересам.

За таких умов керівник INCD може підпорядковувати конкретну організацію в питаннях кібербезпеки безпосередньо INCD на строк, що не перевищує трьох місяців. Для організацій та галузей із низьким рівнем ризику у нормативно-правовому акті запропоновано непримусову модель, згідно з якою INCD може використовувати різні методи м'якого втручання для підвищення кібербезпеки, такі як сприяння обізнаності громадськості, належна підготовка тощо.

Щодо кримінального переслідування, то 2012 року поліція Ізраїлю створила кібервідділ для боротьби з кіберзлочинністю; він має виконувати роль головного координаційного центру з розвитку експертизи в галузі цифрової криміналістики та доказів. Центр утворено в межах спецпідрозділу національної поліції Лахав 433.

З 2002 року з ухваленням Постанови №B/84 Комітету з питань національної безпеки[142] Ізраїль розпочав реалізацію національної політики щодо забезпечення кібербезпеки критичної інфраструктури.

Цією Резолюцією передбачено захист та нагляд щодо комп'ютеризованих систем, які вважаються «життєзабезпечувальними» (хоча їх не називають «критичною інфраструктурою»). Згодом ці положення було включено до Закону про регулювання безпеки в державних органах.

Згідно з Постановою також створено нове агентство — Національне агентство з інформаційної безпеки (NISA), яке працює в межах Служби загальної безпеки (GSS) і визначає критерії регулювання в тих чи інших сегментах державного та приватного секторів. Завданням NISA є визначення цілей щодо кібербезпеки, розробка плану їх досягнення та контроль за виконанням плану спільно з відповідним міністерством. Постановою №B/84 передбачено створення керівного комітету, який здійснюватиме управління та нагляд за NISA в цьому аспекті. Під регулювання підпадають міністерства; судова та пенітенціарна системи; Банк Ізраїлю та інші банки; деякі підприємства оборонної промисловості; енергетичні компанії, підприємства газо- та водопостачання; лікарні; оператори зв'язку, зокрема іінтернет-провайдери; національна авіакомпанія «Ель Аль»; Ізраїльська залізниця; порти; фондова біржа; орган соціального забезпечення Bituach Leumi.

Наразі NISA переходить у підпорядкування до NCSA.

INCB — головний орган, який здійснює перевірку та здійснює регулювання для критичної інфраструктури. Діяльність конкретних суб'єктів регулюється за галузевим принципом.

За готовність країни до надзвичайних ситуацій та управління кризовими ситуаціями в цивільному секторі відповідають Міністерство громадської безпеки, Міністерство оборони та Командування армією оборони Ізраїлю.

142 https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf

NISA та NCSA в межах своєї компетенції також несуть відповідальність за готовність до надзвичайних ситуацій та функціонування певних утворень.

Національне управління з питань надзвичайних ситуацій спільно з Армією оборони Ізраїлю IDF проводило навчання, націлене, зокрема, на відбиття кібератак на критичну інфраструктуру, наприклад національну електромережу.

Кіберрозвідка в Ізраїлі належить до військового та оборонного секторів. Збір та обробка відповідних розвідданих здійснюються відповідно низки нормативно-правових актів, зокрема, в разі необхідності, Закону про нагляд 1979 року та Закону про захист конфіденційності 1981 року.

2012 року, на додачу до кількох інших навчальних програм у царині військової кібербезпеки, IDF було запроваджено навчальний курс «Кіберзахисник».

Ізраїль одним із перших почав налагоджувати співпрацю у сфері кібербезпеки між заінтересованими сторонами, науковими установами та організаціями приватного сектора. Така співпраця — логічне продовження парадигми аналогічної взаємодії в усіх інших сферах функціонування суспільства й держави.

Одна з провідних ініціатив Ізраїлю в цій царині — проєкт CyberSpark Innovation Initiative[143] в Беершебі, 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 підтримує ізраїльську галузь кібербезпеки та відповідний бізнес через кілька 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 та Magnet та підтримку інкубаторів; і програму Meimad з підтримки досліджень у царині кібербезпеки та розробок подвійного призначення. Деякі з цих ініціатив також підтримуються у співпраці з INCB.

Крім CyberSpark, близько 20 науково-дослідних центрів у галузі кібербезпеки, що працюють над безпековими рішеннями 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.

143 http://cyberspark.org.il/#!new-page/cwzu

Israel Aerospace Industries (IAI) очолює Ізраїльський консорціум кіберкомпаній (IC3)[144] — групу провідних ізраїльських компаній у сфері кібербезпеки. IC3 розпочав роботу в січні 2016 року в складі ізраїльської Програми Консорціуму Міністерства економіки. Члени IC3 співпрацюють з провідними урядовими установами у сфері кіберзахисту, передовими технологічними компаніями, стартапами та міжнародними кіберрозвідувальними організаціями.

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) . Відповідно до визначених на національному рівні пріоритетів щодо фінансування наукових досліджень з питань кібербезпеки 2012 року Міністерство науки і технологій та INCB досягли домовленості про створення у кількох університетах окремих удосконалених кіберцентрів; першим 2014 року став міждисциплінарний дослідницький центру у галузі кібербезпеки при Тель-Авівському університеті[145]. Компанії з трансферу технологій, пов'язані з усіма ізраїльськими університетами, пропонують готові механізми співпраці з бізнесом, що захищають наукові та інтелектуальні надбання.

У рамках національних програм у середніх школах Ізраїлю проводяться дослідження й тренінги з кібербезпеки. Програми Magshimim і Nitzanei Magshimim для випускників шкіл із віддалених районів та незабезпечених соціальних прошарків. Програма Gvahim готує учнів середньої школи до випускного іспиту з кібербезпеки, математики та інформатики. Усі ці програми отримують підтримку Міністерства освіти, IDF та INCB.

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ІЗРАЇЛЮ

Армія оборони Ізраїлю (IDF) десятиліттями займається питаннями кібербезпеки та кіберзагрозами, однак, згідно зі своїми підходами до оборонної політики, не оприлюднює деталей щодо бачення національної кібербезпеки та політики у військовій сфері. Від цієї схеми вперше відступили у серпні 2015 року, коли начальник Генерального штабу Гаді Айзенкот опублікував резюме стратегії IDF.

144 http://www.iai.co.il/Sip_Storage//FILES/4/42124.pdf

145 https://icrc.tau.ac.il/

У 2018 році була презентована оновлена Стратегія IDF[146].

У цьому документі[147] окреслено кілька аспектів позиції IDF щодо кібербезпеки, зокрема вказано, що кіберпростір — це військова сфера; зроблено акцент на пріоритетності подальшої розбудови кіберзахисту та правопорушень на стратегічному, оперативному й тактичному рівнях; визнано наявність загроз у кіберпросторі та необхідність ініціювання на організаційному рівні створення кіберкоманд у межах IDF.

У Стратегії IDF зазначено, що в умовах війни та надзвичайних ситуацій кіберзахист важливий для забезпечення сталого функціонування національних установ у періоди напруженості, а також ефективної діяльності IDF.

Сьогодні Ізраїль існує в умовах мінливих загроз.

Основна відмінність полягає в тому, що головним супротивником більше не є коаліція арабських держав, яка налаштована на знищення Ізраїлю в рамках масштабної наземної операції. Зараз серед противників — недержавні організації, що дотримуються стратегії обмеженого нападу та вторгнень на ізраїльську територію.

Хоча загальна мета цих ворогів залишається тією самою — спричинити крах держави Ізраїль і тим самим усунути її як політичну одиницю, спосіб роботи кардинально змінився. Зараз противники поєднують два підходи — фізичний та інтелектуальний. Інтелектуальний підхід передбачає здійснення постійного тиску на ізраїльське суспільство та вплив на становище Ізраїлю в міжнародній спільноті.

Серед основних цілей національної безпеки визначені збереження суверенітету, охорона важливих активів держави та забезпечення безпеки її жителів.

З цього випливає одне з найважливіших завдань у безпековій площині — зміцнення IDF як офіційної військової сили, що може реалізувати свою місію захисту держави, підтримуючи здатність протистояти всьому спектру загроз, спрямованих протидержави Ізраїль, її громадян, активів та життєвих інтересів. У будь-який момент, у будь-якій ситуації, у будь-якому місці (у фізичному просторі — у морі, повітрі, на суходолі чи в космосі; у нефізичному — кіберпросторі), у будь-яких фізичних чи віртуальних сферах IDF має бути готовою до застосування сили, необхідної для підтримки та розвитку національних інтересів.

У Стратегії IDF наведено таку класифікацію загроз та викликів для держави Ізраїль.

146 https://www.israeldefense.co.il/en/node/35633

147 https://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus160-EisenkotSiboni.pdf

ВНУТРІШНІ ЗАГРОЗИ

- загрози з боку (відносно) функціональних держав, наприклад Лівану;
- загрози з боку регіонів із низьким рівнем суверенітету, наприклад Синайського півострова та Сирії;
- виклики всередині Ізраїлю, наприклад соціальні заворушення, порушення громадського порядку, заподіяння шкоди суверенітету держави в частині країни.

ЗОВНІШНІ ЗАГРОЗИ

Звичайні загрози

Їх джерело — державні військові чи недержавні організації, які діють як державні військові та володіють низкою комплексних можливостей, зокрема можливостями вести повітряний та наземний вогонь, провадити масштабні наземні маневри, спеціальні операції, операції в кіберпросторі та інформаційні операції з використанням розвідувальних та матеріально-технічних інструментів. Такі загрози загострятьcя, якщо сунітські держави втратять свою прихильність до Ізраїлю.

Нетрадиційні загрози

Їх спричиняють зусилля різних держав, спрямовані на створення військових ядерних можливостей, що дали б змогу загрожувати Ізраїлю літаками або ракетами великої дальності. Яскравий приклад — Іран, який переміщує ракети великої дальності на іракську територію. Надалі ці ракети можуть бути оснащені нетрадиційними боєголовками і спрямовані на Ізраїль.

Субконвенційні загрози

Вони охоплюють широкий спектр можливих інцидентів, зокрема кризи вищошго рівня, головна мета якої — завдавання шкоди громадянам Ізраїлю, та використання підземного простору для військових і терористичних дій. У разі зростання точності удару й активності противників у кіберпросторі загроза посилюється. Прикладами є «Хезболла» і «Хамас». Ця загроза включає тероризм з боку суб'єктів як в межах району, так і поза ним.

Кіберзагрози та інформаційні загрози

Ці загрози, що надходять від держав та організацій противника, спрямовані на порушення функціонування життєво важливих систем Ізраїлю, розлад повсякденного життя, шпигунство та крадіжки даних.

Вони також можуть впливати на громадську думку та свідомість громадян, підривати легітимність використання сили Ізраїлем, завдавати шкоди правовій системі та заохочувати економічні та суспільні бойкоти.

Загалом на сьогодні серед цілей та 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.

Уряд Ізраїлю так визначає власну місію: Ізраїль має стати провідною державою в питаннях використання кіберпростору як рушія економічного зростання, суспільного добробуту та національної безпеки.

Національна стратегія кібербезпеки Ізраїлю — це насамперед засіб реалізації візії Ізраїлю в царині кібербезпеки, захисту кіберпростору та протистояння різноманітним кіберзагрозам відповідно до національних інтересів країни. Крім того, завдяки втіленню цієї Стратегії Ізраїль має впевнено посісти на міжнародній арені місце лідера в галузі технологічних інновацій та активного партнера в глобальних процесах формування кіберпростору.

Національна стратегія кібербезпеки є концептуальною та практичною основою для досягнення цих цілей. Документ ефективно структурує державні зусилля та пропонує стабільні, довгострокові рішення, окреслює нові концепції та підходи, адаптовані до унікальних особливостей та проблем, що виникають у зв'язку з використанням кіберпростору. Стратегія кібербезпеки Ізраїлю базується на загальній концепції операцій з національної безпеки — концептуальній основі для всіх зусиль і дій держави в контексті національної кібербезпеки. Нею передбачено як прямі дії держави із протистояння кіберзагрозам, так і непрямі зусилля, спрямовані на заохочення та підтримку заходів безпеки в приватному секторі та співпрацю з ним.

Концепція операцій визначає три операційні рівні: «Сукупна кіберстійкість», «Системна кіберстійкість» та «Національний кіберзахист». Трирівневий підхід випливає з унікальної природи кіберзагрози та центральної ролі приватних організацій у досягненні національної кібербезпеки. Рівні відрізняються один від одного своїми цілями, роллю держави та відносинами між державою й приватними організаціями.

Сукупна кіберстійкість — це здатність організацій продовжувати свою діяльність попри виникнення кіберзагроз шляхом реагування на атаки та їх подолання. Це базовий рівень кібербезпеки. Ізраїль поставив собі за мету підвищити загальний рівень кіберстійкості, щоб запобігти загрозам на вищому щаблі та знизити сукупні ризики.

Резолюцією уряду №2443 від 15 лютого 2015 року148 визначено загальнодержавні заходи з підвищення стійкості, що забезпечуються за допомогою сприяння зусиллям організацій у царині безпеки (підтримка найкращих практик, рекомендації, положення, стимули тощо) та регулювання ринку кібербезпеки.

Окремих зусиль було докладено до забезпечення високого рівні кібербезпеки в урядових інституціях — задля створення взірця й впровадження технологічних рішень та процесів для підвищення загальної стійкості ринку.

Другий рівень — це системна кіберстійкість, тобто здатність систематично протистояти кібератакам до, під час та після інцидентів, запобігати їх поширенню та зменшувати сукупні збитки для держави. Хоча перший рівень орієнтований на зменшення атак апріорі, незалежно від будь-якої конкретної події, другий рівень визначається подією за визначенням.

Системної кіберстійкості можна досягти за допомогою заохочення з боку держави обміну інформацією, генерування та поширення цінних відомостей і надання організаціям допомоги під час кіберінцидентів. Цими зусиллями керує NCSA через національний CERT.

Національний CERT тісно співпрацює з приватним сектором, як безпосередньо, так і через галузеві кіберцентри, що працюють під його егідою. CERT розвиває співпрацю на глобальному та місцевому рівнях, підтримуючи інновації та використовуючи її для досягнення своїх цілей.

Необхідна кампанія на національному рівні проти серйозних загроз з боку рішучих, забезпечених ресурсами нападників, які становлять серйозну небезпеку для держави. Національні кампанії з протистояння загрозам передбачають поєднання захисних заходів зі стримування таких атак та подолання їх наслідків із активним протистоянням джерелам загроз.

Трирівневий підхід являє собою цілісне рішення з урахуванням відмінностей у рівнях ризику, характері загрози та ступені її очевидності.

Наприклад, рівень кіберстійкості забезпечує першу реакцію на інциденти, які не становлять негайної та серйозної загрози, але можуть з часом завдати кумулятивної шкоди, або ж на інциденти, тлумачення яких із часом змінюється.

Протягом кількох десятиліть Ізраїль перебуває у світовому авангарді інновацій та науково-технологічних знань у галузі кібербезпеки. Кібербезпека сильно залежить від інновацій, спрямованих на відсіч динамічним підходам нападника. Культура інновацій Ізраїлю, його унікальний людський капітал та зусилля з національної безпеки створюють ідеальне середовище для кіберінновацій, таким чином задовольняючи цю потребу як на місцевому, так і на глобальному рівні.

148 https://ccdcoe.org/uploads/2019/06/Government-Resolution-No-2443-Advancing-National-Regulation-and-Governmental-Leadership-in-Cyber-Security.pdf

У Постанові Уряду №3611 від 7 серпня 2011 р. «Просування національних можливостей кіберпростору»149 пріоритетним завданням визначено зміцнення наукових технологічних можливостей у кіберпросторі та сприяння інноваціям в Ізраїлі. Ці завдання покладено на Національне бюро з питань кіберзахисту як найважливіший компонент національної стратегії кібербезпеки задля забезпечення довгострокового потенціалу кібербезпеки Ізраїлю. Завдання передбачає два основні заходи.

1. Дослідження, розробка та впровадження можливостей і технологій безпеки на національному рівні, зокрема: безпечні та ефективні платформи обміну інформацією; рішення, що підтримують зусилля держави, спрямовані на викриття, дослідження та кібератак; надійні кіберпроцеси; централізовані служби безпеки.
1. Зміцнення національної бази науки та технологій у кіберсфері: сприяння промисловим інноваціям, підтримка наукових досліджень (зокрема створення шести науково-дослідних центрів у провідних університетах Ізраїлю), посилення людського капіталу в кіберсфері та сприяння розвитку екосистеми та взаємне збагачення сфер. Тут ідеться, зокрема, про унікальний проект CyberSpark — потужну екосистему кібербезпеки, що складається з ізраїльських стартапів, глобальних компаній, академічних, цивільних та військових центрів кібербезпеки.

Кіберпростір — це глобальна сфера, а кібербезпека — це глобальна проблема.

Ізраїль розглядає міжнародне співробітництво як найважливіший елемент у створенні кіберпростору як безпечної, вільної та глобальної сфери діяльності, а також як компонент, що доповнює національні зусилля із забезпечення кібербезпеки.

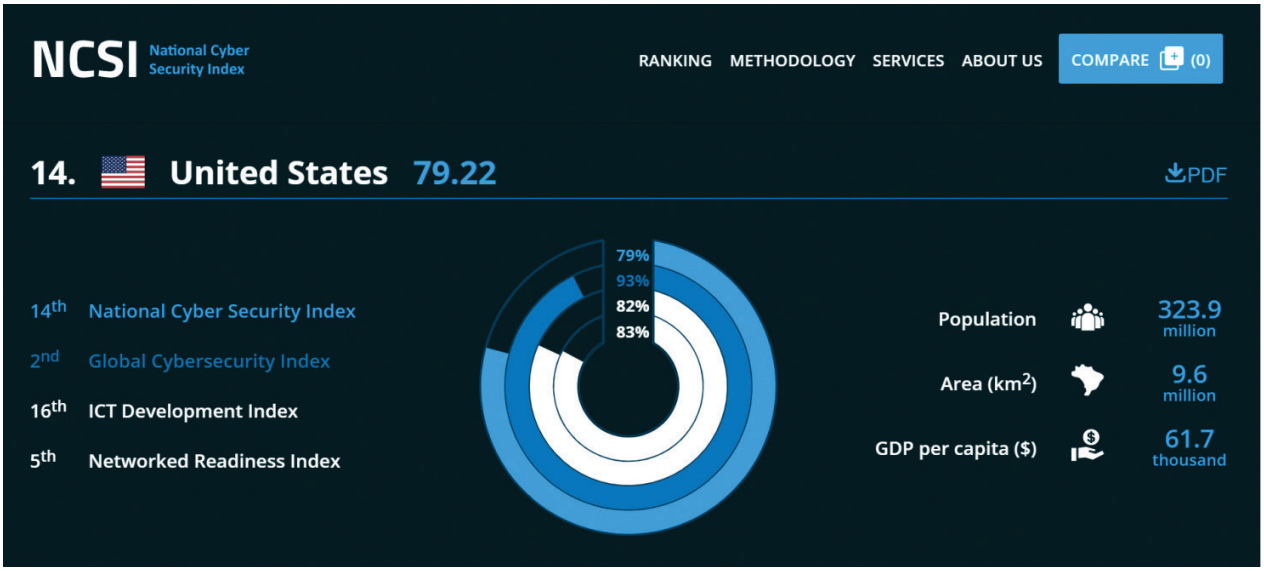
Ізраїль також допомагає країнам-партнерам у зміцненні їхньої національної кібербезпеки. Ізраїль пропонує партнерам у всьому світі працювати разом, обмінюватися знаннями, розробляти нові рішення на глобальному рівні та реалізовувати спільне бачення безпечного й ефективного кіберпростору.

Останнім часом Ізраїль в рамках реалізації стратегічного завдання з налагодження тісної міжнародної співпраці вибудував співробітництво з Австралією, Вірменією, країнами Вишеградської групи (Польщею, Чехією, Словаччиною, Угорщиною), Німеччиною, Японією, країнами Африки — Гондурасом Замбією, Ефіопією, Угандою, Південним Суданом, Руандою, Кенією, Танзанією150.

149 https://mfa.gov.il/MFARUS/PressRoom/2011/Pages/Israeli_government_increases_cybersecurity.aspx

150 https://cyberpolicyportal.org/en/states/israel

США



США перебувають в авангарді розробки політики та стратегії кібербезпеки. Ще в 2003 році уряд США опублікував першу національну стратегію кібербезпеки.

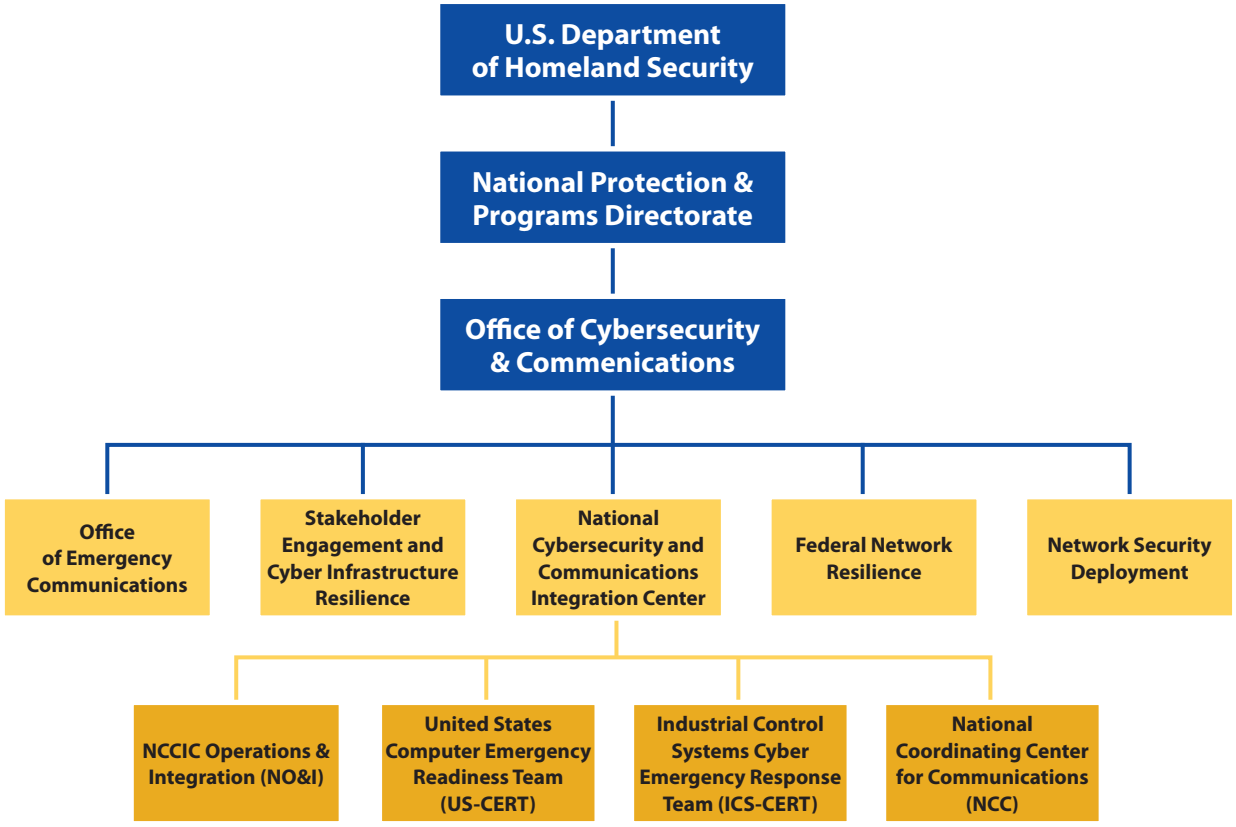
У вересні 2018 року адміністрація США ухвалила Національну кіберстратегію Сполучених Штатів Америки (National Cyber Strategy of the United States of America) (далі — Стратегія кібербезпеки США). Стратегія кібербезпеки США базується на ухваленій у грудні 2017 року Стратегії національної безпеки США та на Указі Президента США (Executive Order, EO) №13800 «Про посилення кібербезпеки федеральних мереж та критичної інфраструктури» (Executive Order, «Strengthening of Federal Networks and Critical Infrastructure).

Попри те, що у Стратегії кібербезпеки США немає формальних посилань на ухвалену раніше Стратегію кіберпростору США 2003 року, ключові підходи й терміни (кібербезпека, процвітання, безпека, відкритість) залишаються незмінними, як і прихильність до стратегічних цілей і завдань щодо функціонування й використання кіберпростору.

У Стратегії кібербезпеки США визначені такі ключові напрямки зміцнення потенціалу кібербезпеки, а також забезпечення захисту США від кіберзагроз: захист США за допомогою збереження мереж, систем, функціональних елементів і даних; сприяння процвітанню держави шляхом забезпечення безпечної, ефективної цифрової економіки та стимулювання потужних внутрішніх інновацій; збереження миру і безпеки за допомогою зміцнення спроможності США стримувати тих, хто використовує кіберінструменти в зловмисних цілях, і, в разі необхідності, вживати заходів впливу на них, причому такі кроки здійснюються у взаємодії з союзниками і партнерами; посилення американського впливу закордоном задля поширення засадничих принципів відкритого, функціонально сумісного, інтероперабельного, надійного й безпечного Інтернету.

Рада національної безпеки США узгоджує з департаментами, агенціями та Адміністративно-бюджетним управлінням (Office of Management and Budget, OMB) відповідний план і ресурси для реалізації Стратегії. Департаменти та агенції виконують свої завдання, доносячи стратегічні рекомендації.

Структура управління кібербезпекою США[151] наведена на рисунку.



151 https://www.us-cert.gov/nccic

Для підвищення рівня кібербезпеки США планується залучити федеральні міністерства і відомства, приватний сектор, громадянське суспільство, а також союзників і партнерів. Основна увага приділяється захисту інформаційних ресурсів, розвитку безпечної «цифрової економіки», стимулюванню інновацій, нарощуванню можливостей припинення ворожої кіберактивності, а також активізації зовнішньополітичних заходів із примусу третіх країн у кіберпросторі до «відповідальної поведінки».

ЗАКОНОДАВСТВО

Федеральний закон про управління інформаційною безпекою (FISMA)

У Федеральному законі про управління інформаційною безпекою (FISMA) — як складовій Закону про електронне урядування 2002 року[152] — наведено структуру управління ризиками, розроблену Національним інститутом стандартів і технологій (NIST) для стандартизації процесів кібербезпеки в урядових установах США. Закон вимагає від кожного федерального агентства розробити, задокументувати та впровадити загальнодержавну програму забезпечення інформаційної безпеки даних та систем, на яких базуються операції та активи агентства зокрема тих, які надаються або управляються іншим агентством, підрядником чи іншими суб'єктами.

Відповідно до цього закону:

- Федеральний директор з інформаційних технологій в Адміністративно-бюджетному управлінні відповідальний за нагляд за використанням урядом технологій з точки зору як витрат, так і стратегії;
- посилено відповідальність NIST щодо розробки стандартів безпеки для федеральних комп'ютерних систем (крім системи оборони та розвідки), створено центральний федеральний центр інцидентів, на OMB покладено відповідальність щодо оприлюднення федеральних стандартів кібербезпеки.

В оновленому FISMA від 2014 року роз'яснено відповідальність керівників директивних служб, встановлено чіткіші рекомендації щодо звітності з акцентом на швидкості, OMB доручено роз'яснювати політику щодо повідомлення про порушення, пов'язані з особистим виявленням витоків інформації.

Федеральний Закон про модернізацію інформаційної безпеки 2014 року[153] вносить зміни до Федерального закону про управління інформаційною безпекою 2002 року (FISMA) і передбачає кілька модернізаційних змін до практики федеральної безпеки у цій царині. Згідно з цими змінами, зменшуються обсяги загальної звітності, посилюється безперервний моніторинг у системах, більше уваги приділяється дотриманню агенціями вимог та складанню ними звітності з акцентом на інцидентах у царині безпеки.

152 https://www.congress.gov/bill/107th-congress/house-bill/2458

153 https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

У FISMA, а також Законі про скорочення паперового документообігу 1995 року та Законі про реформу управління інформаційними технологіями 1996 року (Законі Клінгера — Коена) чітко наголошено на пріоритеті ризик-орієнтованого підходу до економічної безпеки.

На підтримку та посилення цього законодавства Адміністративно-бюджетне управління (OMB) видало Циркуляр А-130 «Управління федеральною інформацією як стратегічний ресурс»[154], який:

- вимагає від федерального уряду відновити для директора Адміністративно-бюджетного управління (OMB) функцію нагляду за політикою інформаційної безпеки агентства та практикою в цій сфері;
- встановлює повноваження очільника Міністерства внутрішньої безпеки (DHS) щодо адміністрування реалізації такої політики та практики в інформаційних системах;
- вимагає від DHS розробити оперативні директиви, що вимагають від органів виконувати стандарти та вказівки щодо захисту федеральної інформації та систем від відомої або обґрунтовано підозрюваної загрози інформаційної безпеки, вразливості чи ризику, і наглядати за виконанням цих директив. Уповноважує директора переглядати чи скасовувати чинні директиви, які не відповідають політиці директора;
- вимагає від DHS (зараз директора OMB) забезпечити роботу федерального центру реагування на інциденти в галузі інформаційної безпеки (FISIC);
- доручає DHS здійснювати процедури розгортання технологій на вимогу агентства, щоб допомогти останньому постійно діагностувати та зменшувати кіберзагрози та вразливі місця;
- вимагає від директора OMB щорічно звітувати перед Конгресом щодо ефективності політики захисту інформації для оцінки відповідності агентства процедурам сповіщення щодо порушення даних OMB;
- передбачає, що функції OMB в галузі інформаційної безпеки будуть делеговані Директору національної розвідки (DNI) для певних систем, якими керують відомства Розвідувальної спільноти;
- наказує DHS проконсультуватися з Національним інститутом стандартів і технологій (NIST) і розглянути розроблені ним рекомендації, щоб експлуатаційні директиви не суперечили стандартам інформаційної безпеки NIST;
- наказує керівникам установ забезпечити: (1) процеси управління інформаційною безпекою, інтегровані з бюджетним плануванням; (2) виконання обов'язків щодо захисту інформації вищих посадових осіб агентств зокрема головних служб з питань інформації; (3) відповідальність усього персоналу за виконання програми інформаційної безпеки на рівні агентства;

154 https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

- забезпечує використання автоматизованих засобів у програмах інформаційної безпеки агентств, у тому числі для періодичного оцінювання ризиків, тестування процедур безпеки та виявлення інцидентів із безпекою, звітування про них і реагування на них;
- вимагає від агентств включати секретаріат адвоката як одержувача повідомлень про інциденти з безпекою. Вимагає від органів, які повідомляють Конгрес про великі інциденти з безпекою протягом семи днів після того, як є розумні підстави зробити висновок про те, що стався великий інцидент;
- доручає агенціям подавати щорічний звіт щодо великих інцидентів до OMB, DHS, Конгресу та Рахункової палати (GAO). Вимагає включати до таких звітів: (1) загрози та їх джерела, вразливості та наслідки; (2) оцінку ризиків постраждалих систем до інциденту цього та стан цих систем на момент інциденту; (3) дії з виявлення загроз, реагування та відновлення; (4) загальну кількість інцидентів; (5) кількість осіб, які постраждали, та інформація, якій основні інциденти, пов'язані з порушенням особистої інформації становлять загрозу;
- уповноважує GAO надавати технічну допомогу агенціям та загальним інспекторам, зокрема шляхом перевірки та контролю процедури захисту інформації;
- вимагає від GAO забезпечити розробку керівних принципів щодо: (1) оцінки ефективності програм та практик захисту інформації; (2) визначення великого інциденту;
- дає розпорядження FISIC надавати агенціям розвіддані щодо кіберзагроз, вразливостей та інцидентів для оцінки ризиків;
- наказує OMB протягом дворічного періоду після набуття чинності Законом про кібербезпеку включити до щорічного звіту Конгресу оцінку застосування агентствами технологій безперервної діагностики та інших сучасних інструментів безпеки;
- вимагає від OMB гарантувати наявність пункту в політиці про сповіщення про порушення даних: у разі виявлення несанкціонованого розголошення чи доступу до даних органи мають повідомити про це: (1) Конгресові — протягом 30 днів; (2) постраждалим особам — якнайшвидше. Дозволяє Генеральному прокурору, керівникам відомств Розвідувальної спільноти або DHS відкласти сповіщення постраждалих осіб з метою розслідування інциденту правоохоронними органами, органами національної безпеки чи здійснення заходів з усунення небезпеки;
- вимагає від OMB внести зміни або переглянути Циркуляр A-130 для усунення неефективної та марної звітності;
- керує Консультативною радою з питань інформаційної безпеки та конфіденційності для консультування та надання щорічних звітів DHS.

NIST несе відповідальність за розробку стандартів та рекомендацій щодо інформаційної безпеки, зокрема мінімальних вимог до федеральних систем, але такі стандарти та рекомендації не застосовуються до систем національної безпеки без схвалення з боку відповідних посадових осіб федерального рівня, які здійснюють політичні повноваження щодо таких систем.

Публікації FISMA відповідають вимогам Циркуляру A-130 Адміністративно-бюджетного управління (OMB).

Публікації FISMA розроблені NIST відповідно до його статутних обов'язків, що регламентовані Федеральним законом про модернізацію інформаційної безпеки (FISMA) від 2014 року, 44 USC § 3551 та наступних. Публічне право (PL) 113-283.

В рамках процесу імплементації FISMA NIST також розробив інтегровану Основу управління ризиками, яка ефективно об'єднує всі стандарти безпеки та рекомендації, пов'язані з FISMA, і має сприяти розробці агентствами комплексних та збалансованих програм інформаційної безпеки.

У січні 2008 року Президент США оприлюднив Директиву про національну безпеку №54 та Директиву про внутрішню безпеку №23. Директиви дозволяють DHS спільно з OMB встановлювати мінімальні експлуатаційні стандарти для цивільних мереж федерального уряду.

Комплексна національна ініціатива з питань кібербезпеки (CNCI)

В обох директивах представлено загальнодержавний підхід до забезпечення кібербезпеки, який згодом був втілений у Комплексній національній ініціативі з питань кібербезпеки[155] (CNCI). CNCI визначає метою захист від повного спектру загроз і зміцнення середовища кібербезпеки, впровадження комплексного підходу, який охоплює правоохоронні органи, розвідку, контррозвідку та військові відомства.

Основні дії, передбачені CNCI:

- забезпечення або підвищення рівня поінформованості про ситуацію в межах федерального уряду, інших державних установ та приватного сектора;
- забезпечення або удосконалення здатності швидко реагувати на вторгнення;
- розширення можливостей контррозвідки;
- підвищення безпеки ланцюга постачання ключових інформаційних технологій;
- розширення кіберосвіти;
- координація та переспрямування зусиль на дослідження та розробки; і
- розробка стратегій стримування.

155 https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

CNCI охоплює12 підініціатив:

1. Управління Федеральною мережею як єдиним мережевим підприємством з надійним підключенням до Інтернету.
2. Розгортання системи датчиків виявлення вторгнень у всій Федеральній мережі.
3. Подальше впровадження систем запобігання вторгненням до Федеральної мережі.
4. Координація та переспрямування досліджень і розробок.
5. Підключення діючих центрів кібероперацій для покращення ситуаційної обізнаності.
6. Розробка і впровадження загальнодержавного плану кіберконтррозвідки.
7. Підвищення безпеки класифікованих мереж.
8. Розширення кіберосвіти.
9. Розробка сталих технологій, стратегій та програм «стрибків уперед».
10. Розробка сталих стратегій та програм стримування.
11. Розробка всебічного підходу до управління ризиками глобального ланцюга поставок.
12. Визначення ролі Федерального уряду в забезпеченні вищого рівня кібербезпеки критичної інфраструктури.

2009 року спільно з Конгресом та представниками приватним сектора президент США ініціював перегляд політики в кіберпросторі[156]. Підсумковий огляд містив критику щодо прогресу уряду США, вказав на головні недоліки в політиці, правових структурах, управлінні, координації та дослідженнях, які обумовлюють вразливість США у площині кібербезпеки. Крім того, в огляді було запропоновано посилити лідерську роль Білого дому, а також відповідальність федеральних органів за кібербезпеку. Крім того, в документі викладено 10 короткострокових дій та 14 середньострокових дій на підтримку загальних цілей CNCI[157].

Стратегічний план Федеральної програми досліджень та розвитку кібербезпеки (2011 р.) окреслює стратегічні напрями для DHS, Національного наукового фонду (NSF) та NIST, визначає пріоритети досліджень для забезпечення надійної комунікаційної інфраструктури.

В основу стратегічного підходу США до захисту критичної інфраструктури (CIP) покладено державно-приватне партнерство, тоді як на урядові органи покладено обов'язки координації та визначення пріоритетів. Директива президента США №63 від 1998 р. забезпечила створення структури під керівництвом Білого дому для координації діяльності федерального уряду щодо захисту критичної інфраструктури від кібератаки[158].

156 https://digital.library.unt.edu/ark:/67531/metadc743582/

157 https://obamawhitehouse.archives.gov/administration/eop/nsc/cybersecurity/progressreports/july2010

158 https://fas.org/irp/offdocs/pdd/pdd-63.htm

СУБ'ЄКТИ КІБЕРБЕЗПЕКИ

Міністерство внутрішньої безпеки (DHS)

У 2002 році створено Міністерство внутрішньої безпеки (DHS), на яке покладено, зокрема, координацію національних зусиль щодо захисту критичної інфраструктури в IT та секторі комунікації.

Національний план захисту інфраструктури (NIPP), вперше ухвалений 2006 року, визначає критерії партнерства між федеральним урядом, власниками й операторами критичної інфраструктури.

Національним планом захисту інфраструктури на 2013 рік передбачено розробку спільних національних пріоритетів для інформування про розподіл ресурсів та ухвалення рішень з боку важливих інфраструктурних партнерів.

2014 року DHS вперше опублікувало Спільні національні пріоритети задля забезпечення управління критичною інфраструктурою та покращення їїбезпеки та стійкості. Пріоритети[159] містять викладені дані для відображення критичних змін у середовищі зростаючого ризику та для узгодження із визначеними пріоритетами та ключовими проблемами. Ці оновлені Пріоритети передбачають:

- зниження ризиків для національних критичних інфраструктур;
- посилення реагування на інциденти та покращення можливостей відновлення після них;
- покращення обміну інформацією;
- Захист критичної інфраструктури від кіберзагроз;
- підтримання безпеки та стійкості в інвестиціях та інноваціях.

2003 року разом із Національною стратегією розвитку кіберпростору була опублікована Національна стратегія фізичного захисту критичної інфраструктури та основних активів. У документі визначено об'єкти критичної інфраструктури та перелік загроз. Як і Національна стратегія розвитку кіберпростору 2003 року, більшість обов'язків цей документ покладає на DHS. Також Президент США видав Указ №13636 «Поліпшення кібербезпеки критичної інфраструктури» (EO 13636). Цей важливий документ доповнює всі попередні документи та регулює обмін інформацією між федеральним урядом іприватним сектором. Він також встановлює мінімальні вимоги до підвищення безпеки критичної інфраструктури.

159 https://www.cisa.gov/sites/default/files/publications/Joint-National-Priorities-Fact-Sheet-20180928-508.pdf

Директива президента про політику безпеки та стійкості критичної інфраструктури[160] (PPD-21), видана разом із Указом №13636, не внесла жодних істотних змін у політику, обов'язки чи програми; проте документ вимагав оцінити чинну модель державно-приватного партнерства, визначити базові дані та системні вимоги до ефективного обміну інформацією та забезпечення широкої обізнаності заінтересованих сторін із ситуацією у сфері кібербезпеки[161]. У документі також міститься рекомендація оновити Національний план захисту інфраструктури на 2009 рік (NIPP). Перегляд Плану на 2009 рік завершився підготовкою та схваленням третьої редакції плану, яка була видана в 2013 році.

Задля усунення недоліків FISMA в Указі №13636 міститься доручення федеральному уряду розвивати засади добровільної кібербезпеки, що знайшло своє відображення пізніше у Федеральному законі про модернізацію інформаційної безпеки 2014 року. Засади для вдосконалення кібербезпеки критичної інфраструктури 2014 року, що складаються з настанов, практик та добровільних стандартів для приватного сектору, мають на меті сприяння захисту критичної інфраструктури[162].

Крім перелічених документів, ухвалено ще чотири закони, що стосуються захисту критичної інфраструктури:

1. Федеральний закон про модернізацію інформаційної безпеки 2014 року, яким вносяться зміни до FISMA 2002 року, уточнюється роль DHS у забезпеченні цифрової інформації федеральних агентств, визначено відповідальність OMB за впровадження вимог FISMA на федеральному рівні та встановлено вимоги до звітності щодо кіберінцидентів[163].
2. Закон про захист національної кібербезпеки 2014 року, який дозволяє DHS обмінюватися інформацією з приватним сектором, реагувати на кіберінциденти, надавати допомогу як приватним компаніям, так і федеральним агенціям і рекомендувати заходи з кібербезпеки[164].
3. Закон про національну кібербезпеку та захист критичної інфраструктури (NCCIP) 2013 року визначає роль DHS у запобіганні інцидентам у царині кібербезпеки та реагуванні на них та встановлює правила обміну інформацією між DHS та власниками й операторами критичної інфраструктури[165].
4. Закон про підвищення рівня кібербезпеки 2014 року надає Національному інституту стандартів та технологій дозвіл та повноваження для розробки стандартів з метою зниження ризику кібератак на об'єкти критичної інфраструктури[166].

160 https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
161 https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
162 https://www.nist.gov/cyberframework
163 https://www.govtrack.us/congress/bills/113/s2521/text
164 https://www.congress.gov/bill/113th-congress/senate-bill/2519
165 https://www.congress.gov/bill/113th-congress/house-bill/3696
166 https://www.congress.gov/bill/113th-congress/senate-bill/2519

GAO в свою чергу звернула увагу на відсутність керівництва з питань кібербезпеки для управлінь та відомств федерального уряду в частині відвернення конкретних критичних ситуацій інфраструктурних секторів, за які вони відповідають.

Критична інфраструктура, яка належать до різних галузей, має відповідати конкретним вимогам кібербезпеки, що вимагається законодавством чи нормативно-правовими актами, але при цьому вимоги є надзвичайно різноманітними. Попри велику різницю між державними та приватними структурами та федеральними та державними структурами, зауважило GAO недостатня чіткість щодо того, де відповідальність лежить серед цих сторін[167].

Національні засади реагування[168] являють собою керівні принципи, що дають змогу забезпечити єдину національну відповідь на стихійні лиха та надзвичайні ситуації, зокрема й у сфері кібербезпеки, мають широку цільову аудиторію, яка охоплює приватний сектор, неурядові організації та навіть окремих осіб, хоча для неурядових організацій дотримання цих стандартів є добровільним.

Міністерство юстиції (DoJ)

Відповідальність за виконання законів у царині кібербезпеки значною мірою покладено на Міністерство юстиції (DoJ).

Воно протидіє кіберзагрозам шляхом розслідування справ про втручання та кіберзлочини, що належать до його юрисдикції; провадить внутрішні операції із захисту національної безпеки від кіберзагроз, зокрема зриву операцій зовнішньої розвідки, терактів чи інших загроз національній безпеці; здійснює збір, аналіз та розповсюдження інформації про кіберзагрози.

Задля забезпечення загальнодержавного підходу до боротьби з кіберзагрозами національній безпеці відділ кібербезпеки Агентства безпеки Департаменту національної безпеки США спільно з іншими структурами департаменту розпочав підготовку загальнодержавної мережі спеціалістів кіберслужб національної безпеки для забезпечення ефективнішого вирішення проблем із кібервторгненнями та нападами інших держав чи терористичних організацій.

Відділ комп'ютерної злочинності та інтелектуальної власності Агентства безпеки Департаменту національної безпеки США запобігає комп'ютерним злочинам та розслідує їх, співпрацюючи з іншими державними установами, приватним сектором, академічними установами та іноземними партнерами.

167 https://www.gao.gov/products/GAO-13-283

168 https://www.fema.gov/emergency-managers/national-preparedness/frameworks

Загальнодержавної мережі спеціалістів кіберслужб

Як інтегровані елементи NCCIC, які підтримують одне одного, ці гілки забезпечують можливості та партнерства, необхідні для реалізації загальнонаціонального підходу до вирішення питань кібербезпеки та комунікацій на операційному рівні.

Відділ операцій та інтеграція NCCIC NO&I планує, координує та інтегрує можливості з метою синхронізації аналізу, обміну інформацією та об'єднання зусиль щодо управління інцидентами в усіх галузях та операціях NCCIC.

US-CERT має значний досвід мережевого та цифрового медіа-аналізу зловмисної діяльності, спрямованої на мережі країни. US-CERT розробляє своєчасні та корисні інформаційні матеріали, які поширюються серед федеральних відомств, місцевих органів влади, організацій приватного сектора та міжнародних партнерів. Крім того, US-CERT працює з Національною системою захисту кібербезпеки (NCPS), яка забезпечує можливості виявлення вторгнень до федеральних відомств та запобігання їм.

ICS-CERT знижує ризики для критичної інфраструктури країни шляхом посилення безпеки систем управління за допомогою державно-приватних партнерств. ICS-CERT працює за чотирма напрямами: ситуаційна обізнаність заінтересованих сторін критичної інфраструктури та ключових ресурсів; системи управління реагуванням на інциденти та технічний аналіз; координація убезпечення вразливості систем управління; та зміцнення партнерства в царині кібербезпеки з урядовими відомствами.

NCC веде і координує надання, відновлення та забезпечення захисту телекомунікаційних послуг або об›єктів телекомунікацій NS / EP за будь-яких умов. NCC використовує партнерські відносини з урядовими, галузевими та міжнародними партнерами для формування ситуаційної обізнаності й визначення пріоритетів щодо захисту та реагування.

NCCIC багато в чому покладається на добровільну співпрацю з партнерами. NCCIC тісно співпрацює з федеральними міністерствами та відомствами й активно взаємодіє з компаніями та установами приватного сектора, а також із органами влади різних рівнів і міжнародними партнерами. Усі заінтересовані сторони формують практику спільноти, яка працює разом задля захисту тих критичних інформаційних технологій, якими володіє чи керує кожен із учасників. Оперативні ролі та обов'язки Агентства безпеки в галузі кібербезпеки реалізуються через Кіберкомандування США (USCYBERCOM)[169].

169 https://www.cybercom.mil/About/Mission-and-Vision/

Агентство із захисту інформаційних систем (DISA)

Агентство із захисту інформаційних систем (DISA)[170], до 1991 року відоме як Агентство із захисту комунікацій, є агентством бойового забезпечення Міністерства оборони США (DoD)

Зокрема, перед DISA було поставлено завдання забезпечення безпеки інформаційних технологій та комунікацій, підтримки та захист військових мереж.

В Агентстві працюють понад 8000 військових та цивільних службовців. Агентство забезпечує можливості командування, контролю та обміну інформацією, а також глобально доступну інформаційну інфраструктуру для безпосередньої підтримки військ, керівників держави та партнерів у здійсненні місій під час всього спектру військових операцій.

Розвідувальна спільнота США на чолі з Директором національної розвідки (DNI) нерозривно пов'язана з забезпеченням кібербезпеки через кількість інформації, яка проходить по всій інфраструктурі спільних інформаційних мереж світу. Управління директора національної розвідки координує 17 агентств та організацій, багато з яких підпорядковуються DHS та Міністерству оборони[171].

DNI встановлює цілі для Розвідувальної спільноти, але не має прямого контролю за персоналом різних відомств.

Агентство національної безпеки (ANB)

Агентство національної безпеки (ANB) є основним суб'єктом з кібербезпеки в секторі національної безпеки, хоча інші агентства також відіграють значну роль.

Відповідно до CNCI Федеральне бюро розслідувань (FBI) керує Національною спільною робочою групою з питань кіберрозслідування (NCIJTF), яка об'єднує представників контррозвідки, антитерористичногоих структур, розвідки та правоохоронних органів і опрацьовує інформацію та координує діяльність 19 федеральних відомств з метою прогнозування кібератак і запобігання їм.

На відміну від багатьох європейських країн, де власники та оператори критичної інфраструктури юридично зобов'язані повідомляти про великі інциденти з кібербезпекою визначеним державним органам, у США обмін інформацією щодо вразливостей та оцінки ризиків між федеральним урядом і приватним сектором є добровільним.

Відповідно, основна відповідальність за захист критичної інфраструктури, реагування на кібератаки та відновлення після них лежить на власниках та операторах цих потужностей.

---

170 https://www.disa.mil/About

171 https://www.defense.gov/Our-Story/Our-Forces/

Приватний сектор володіє значною кількістю об'єктів інфраструктури й накопичив потужні знання, тож управління кіберінцидентами та координація дій у цій галузі здійснюються у співпраці з приватними установами. Очолює цю співпрацю з приватним сектором NCCIC DHS, метою є забезпечення захисту критичної інфраструктури та основних ресурсів; особлива увага приділяється роботі з телекомунікаційною та інформаційною інфраструктурою.

У кожному секторі критичної інфраструктури створено власні центри обміну інформацією. Наприклад, в енергетичному секторі центр обміну інформацією та її аналізу було відкрито 1998 року. Програма обміну інформацією, започаткована 2013 року, забезпечує організації енергетичного сектора інформацією та аналітикою щодо кіберзагроз практично в режимі реального часу.

Міністерство торгівлі (DoC)

Міністерство торгівлі (DoC) та NIST керують Національною ініціативою з освіти з питань кібербезпеки (NICE), яка розширює можливості набору, навчання та утримання фахівців з кібербезпеки, підвищення обізнаності громадськості та сприяє поширенню знань з кібербезпеки в школах.

DoC також опікується контрактом з Інтернетом-корпорацією з присвоєння імен та номерів (ICANN), яка в силу своєї діяльності працює з багатьма заінтересованими сторонами, тож виступає ключовим чинником державно-приватного партнерства та взаємодії.

Серед численних ініціатив державно-приватного партнерства можна виділити кілька най ефективніших:

1. Рамковий для державно-приватного партнерства Національний план захисту інфраструктури (NIPP) визначає, як федеральний уряд та власники й оператори критичної інфраструктури можуть спільно працювати над управлінням ризиками та досягненням безпеки й стійкості.

2. Партнерство між DHS, DoD та Радою з оборонних іновацій, яка надає рекомендації міністру оборони та іншим вищим керівникам Міністерства оборони щодо нових технологій та інноваційних підходів, які Міністерство оборони має застосовувати для забезпечення технологічного та військового домінування США (DIB) має на меті підвищити рівень захисту конфіденційної інформації. Програма DIB з кібербезпеки та забезпечення інформації, запущена у 2012 році DoD та DHS, спрямована на підвищення стійкості критичної інфраструктури компаній оборонної промисловості шляхом посиленого обміну інформацією про кіберзагрози.

3 Вагомий приклад державно-приватного партнерства — Einstein[172], реалізована DHS система виявлення вторгнень, призначена для виявлення орієнтованого на цивільні мережі федерального уряду шкідливого трафіку, який передається через комерційні технології та за участю постачальників комерційних послуг. Програма передбачає автоматизований процес збору, співвіднесення, аналізу даних та обміну інформацією про комп'ютерну безпеку в межах федеральних урядових установ з метою посилення аналізу кібербезпеки, ситуаційної обізнаності та реагування на загрози. Наразі програма перебуває на третій фазі (Einstein 3) і забезпечує запобігання вторгненням до системи, здатна автоматично виявляти кіберзагрози та реагувати на них до заподіяння шкоди, таким чином не дозволяючи шкідливому трафіку зашкодити цивільним мережам федерального уряду.

Посилення державно-приватного партнерства є ключовим складником зусиль США, спрямованих на захист себе у кіберпросторі; утім, у царині обміну інформацією між державними й приватними структурами досі зберігається чимало проблем.

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ США

У вступному слові до Стратегії кібербезпеки Д.Трамп наголошує, що цифрова сфера є невід-дільною частиною життя держави й суспільства, що обумовлює необхідність її гарантованого захисту. У Вашингтоні відзначають значне зростання залежності країни від інформаційних технологій (IT), а також прагнення конкурентів і супротивників використовувати глобальну мережу «як арену, де військову, економічну і політичну перевагу Сполучених Штатів може бути нейтралізовано і де США, їхні союзники і партнери найбільш уразливі».

«Національна кіберстратегія США визначає, як ми (1) захищатимемо Батьківщину, захищаючи мережі, системи, функції та дані; (2) сприятимемо процвітанню США шляхом розвитку безпечної, процвітаючої цифрової економіки та сприятимемо сильним внутрішнім інноваціям; (3) зберігатимемо мир і безпеку шляхом посилення спроможності Сполучених Штатів у співпраці з союзниками та партнерами — стримуватимемо та, якщо потрібно, каратимемо тих, хто використовує кіберінструменти в зловмисних цілях; і (4) розширюватимемо американський вплив за кордон, щоб поширити основні принципи відкритого, сумісного, надійного та безпечного Інтернету»[173].

172 https://www.cisa.gov/publication/einstein-3-accelerated

173 Див посилання 153

ПОДОЛАННЯ ВРАЗЛИВОСТЕЙ У КІБЕРБЕЗПЕЦІ

Стратегію буде успішно реалізовано за умови ефективного подолання вразливостей у кібербезпеці. Це означає, що:

- мережі, системи, функції та дані забезпечені захистом;
- забезпечено виявлення інцидентів, протистояння їм, реагування на них та відновлення після них;
- деструктивні, руйнівні або інші дестабілізаційні шкідливі дії, спрямовані проти кібернетичних інтересів США, отримують відсіч або превентивно припиняються;
- діяльність, яка суперечить принципам відповідальної поведінки в кіберпросторі, стримується шляхом накладання санкцій за допомогою кібер- та інших засобів;
- США готові використовувати кіберможливості для досягнення цілей національної безпеки.

Національну кіберстратегію структуровано відповідно до засадничих елементів Стратегії національної безпеки. Рада національної безпеки США має узгодити з департаментами, агенціями та Адміністративно-бюджетним управлінням (OMB) відповідний план і ресурси для реалізації Стратегії. Департаменти та агенції виконують свої завдання, доносячи стратегічні рекомендації.

У документі зазначено, що низка зарубіжних держав не поділяє американські підходи до використання кіберпростору для взаємовигідної співпраці, обмежує і контролює доступ власного населення до глобальної мережі, підриваючи засади вільного Інтернету на міжнародних майданчиках.

Росію, Іран і Північну Корею звинувачено в «безвідповідальних кібератаках», які завдали шкоди американським і міжнародним діловим колам, союзникам і партнерам США. Китаю поставлено в провину економічне шпигунство і крадіжки інтелектуальної власності. Своєї чергою, недержавні суб'єкти, зокрема терористи і представники злочинних угруповань, використовують мережеве середовище для отримання прибутку, вербування прихильників, ведення пропаганди і організації атак на США, їхніх союзників і партнерів.

У Стратегії кібербезпеки США зазначено, що масштаби деструктивної мережевої діяльності в останні роки різко зросли. Кіберпростір перетворився на «середовище стратегічного міждержавного суперництва», де основні загрози походять від Росії та Китаю, які володіють «кіберпотенціалом», порівнянним з американським. При цьому підходи, що раніше застосовувалися до їх стримування і захисту національних інформаційних систем, фактично визнано малоефективними.

Для підвищення кібербезпеки США заплановано задіяти федеральні міністерства й відомства, приватний сектор, громадянське суспільство, а також союзників і партнерів.

Основну увагу приділено захисту інформаційних ресурсів, розвитку безпечної «цифрової економіки», стимулюванню інновацій, нарощування можливостей припинення ворожої кіберактивності, а також зовнішньополітичних заходів примусу третіх країн до «відповідальної поведінки» у кіберпросторі.

Стратегія кібербезпеки США передбачає забезпечення технічної переваги США і організацію ефективних адміністративних дій, сфера застосування яких повинна охопити й приватний сектор. Крім того, США визнає, що виключно технократичного підходу до протидії сучасним інформаційним загрозам недостатньо, а для ефективного стримування шкідливої активності і запобігання подальшій ескалації напруженості в кіберпросторі Білий дім повинен мати можливість вибору законодавчо закріплених варіантів реагування.

На думку президента США Д.Трампа, Стратегія кібербезпеки США є «першим за 15 років документом, де чітко сформульовані ключові напрями діяльності американських міністерств і відомств щодо мережевого середовища».

ОСНОВНІ ЗАВДАННЯ

- захист держави шляхом забезпечення безпеки інформаційних мереж, систем і даних;
- сприяння процвітанню США шляхом підвищення безпеки та розвитку цифрової економіки, а також стимулювання американських інновацій;
- збереження миру за допомогою нарощування можливостей США щодо стримування суб'єктів, які використовують кіберзасоби з деструктивною метою, і, в разі необхідності, здійснення на них впливу (спільно з союзниками і партнерами);
- розширення міжнародного впливу США для просування основоположних принципів відкритого, сумісного, надійного і безпечного Інтернету.

Структурно документ розділений на чотири частини, кожна з яких розкриває основні напрями діяльності центральних органів виконавчої влади щодо кіберпростору. У розділах, на які поділено частини, коротко описано обставини, що склалися в тій чи іншій сфері використання глобального мережевого середовища, визначено проблеми, виклики й загрози, а також наведено першочергові заходи на виконання головних завдань.

У кожній із частин, присвячених 4 основним елементам Стратегії кібезрбепеки США, визначено цілі та пріоритетні дії.

Основний елемент I: **Захистити американський народ, батьківщину і американський спосіб життя. Ключова мета: управляти ризиками кібербезпеки для підвищення захисту і стійкості персональної інформації громадян США та інформаційних систем. Частина складається з трьох розділів.**

Розділ I: забезпечення безпеки федеральних мереж та інформації. Передбачено такі пріоритетні дії: подальша централізація управління і нагляду за безпекою громадян на федеральному рівні; узгодження управління ризиками та діяльністю в сфері інформаційних технологій; вдосконалення управління ризиками у федеральній системі ланцюгів постачання; посилення кібербезпеки федеральних підрядників; забезпечення провідних позицій уряду в царині найкращих інноваційних практик.

Розділ II: захист критичної інфраструктури. Передбачено такі пріоритетні дії: вдосконалення розподілу функцій і сфер відповідальності; визначення пріоритетів дій залежно від характеру ідентифікованих національних ризиків; залучення провайдерів інформаційно-комунікаційних технологій як посередників у царині кібербезпеки; захист американської демократії; створення сприятливих умов для інвестицій у кібербезпеку; визначення пріоритетів національних досліджень і сприяння розвитку інвестицій; поліпшення транспортної, морської та космічної кібербезпеки.

Розділ III: боротьба з кіберзлочинністю й поліпшення звітності про інциденти. Передбачено такі пріоритетні дії: заходи щодо поліпшення звітності та реагування на інциденти; підвищення ефективності електронного нагляду, а також вдосконалення законодавства про комп'ютерні злочини; зниження загроз у кіберпросторі від транснаціональних злочинних організацій ; спрощення затримання злочинців, які перебувають за кордоном; зміцнення потенціалу правоохоронних органів країн-партнерів у боротьбі з кіберзлочинністю.

Основний елемент II: **Сприяння процвітанню США. Ключова мета: збереження впливу США в технологічній екосистемі, а також розвиток кіберпростору як відкритого рушія економічного зростання, інновацій та ефективності. Частина складається з трьох розділів.**

Розділ I: сприяння розвитку життєздатної та стійкої цифрової економіки. Передбачено такі пріоритетні дії: стимулювання гнучкої та захищеної технологічної торгівлі; визначення пріоритету інновацій; інвестування в інфраструктуру наступного покоління; сприяння вільному транскордонному потоку даних; підтримка лідерства США у передових технологіях; сприяння забезпеченню повного життєвого циклу кібербезпеки.

Розділ I: сприяння розвитку життєздатної та стійкої цифрової економіки. Передбачено такі пріоритетні дії: стимулювання гнучкої та захищеної технологічної торгівлі; визначення пріоритету інновацій; інвестування в інфраструктуру наступного покоління; сприяння вільному транскордонному потоку даних; підтримка лідерства США у передових технологіях; сприяння забезпеченню повного життєвого циклу кібербезпеки.

Розділ I: сприяння розвитку життєздатної та стійкої цифрової економіки. Передбачено такі пріоритетні дії: стимулювання гнучкої та захищеної технологічної торгівлі; визначення пріоритету інновацій; інвестування в інфраструктуру наступного покоління; сприяння вільному транскордонному потоку даних; підтримка лідерства США у передових технологіях; сприяння забезпеченню повного життєвого циклу кібербезпеки.

Розділ II: заохочення і забезпечення інноваційності США. Передбачено такі пріоритетні дії: оновлення механізмів обстеження іноземних інвестицій і діяльності в США; підтримка сильної і збалансованої системи захисту інтелектуальної власності; захист конфіденційності та цілісності американських ідей.

Розділ III: створення висококваліфікованого пулу працівників галузі кібербезпеки. Передбачено такі пріоритетні дії: створення і підтримка кадрового резерву; розширення можливостей перепідготовки та освіти для американських службовців і робітників; збільшення персоналу сфери кібербезпеки на федеральному рівні; використання виконавчих органів для виявлення і заохочення талановитих кадрів.

Основний елемент III: **Збереження миру за допомогою сили. Ключова мета: виявлення дій у кіберпросторі, які дестабілізують США і суперечать національним інтересам країни, протидія таким діям, припинення їх, ослаблення їхньої інтенсивності, а також стримування їх зі збереженням переваги США в кіберпросторі й за допомогою кіберпростору. Частина складається з двох розділів.**

Розділ I: підвищення кіберстабільності за допомогою впровадження принципів відповідальної поведінки держав. Передбачено такі пріоритетні дії: заохочення загальної прихильності до норм поведінки у кіберпросторі.

Розділ II: виявлення і стримування неприйнятної поведінки в кіберпросторі. Передбачено такі пріоритетні дії: керівництво досягненням заявлених цілей а також взаємодія з розвідувальними органами; реалізація відповідних заходів покарання за шкідливі дії в кіберпросторі; запуск ініціатив, спрямованих на стримування негативних дій у кіберпросторі; протидія шкідливому кібервпливу та інформаційним операціям.

Основний елемент IV: **Посилення американського впливу. Ключова мета: збереження довгострокової відкритості, функціональної сумісності, безпеки та надійності Інтернету, що підтримується і посилюється інтересами США. Частина складається з двох розділів.**

Розділ I: сприяння відкритому, функціонально сумісному надійному та безпечному Інтернету. Передбачено такі пріоритетні дії: захист свободи Інтернету і сприяння їй; співробітництво з країнами-однодумцями, бізнесом, науковими колами та громадянським суспільством; сприяння реалізації багатосторонньої моделі управління Інтернетом; сприяння багатосторонній, функціональній, спільній, надійній комунікаційній інфраструктурі й підключенню до Інтернету; підтримка ринків та інноваційних продуктів США по всьому світу.

Розділ II: створення міжнародного кіберпотенціалу. Передбачено пріоритетні дії, спрямовані на поліпшення заходів з мобілізації зусиль забезпечення кібербезпеки.

ВИСНОВКИ

Системи управління кібербезпекою в країнах, проаналізованих у цьому документі, мають спільні особливості й кардинальні відмінності. Цей досвід можна використати під час підготовки великої реформи державного регулювання у сфері кібербезпеки.

Так, країни з системами прецедентного права (Велика Британія та США) використовують ризик-орієнтований підхід і на підставі оцінки ризиків та загроз готують стратегічні документи, плани їх реалізації, уточнюють повноваження інституцій відповідно до тих завдань, які ставить національна стратегія. Ще одна особливість цих країн — відсутність на перших етапах регулювання окремого закону про кібербезпеку (наразі законодавство переглядаються). Велика роль відводиться самим суб'єктам кібербезпеки, їх свідомому підходу, а також системі стандартизації. Так, у США NIST останнім часом здобув підтримку на законодавчому рівні.

Найбільше від решти проаналізованих країн відрізняється підхід до кібербезпеки, застосовуваний в Ізраїлі. Ця країна постійно перебуває у ворожому середовищі, має високий відсоток виробництва високотехнологічної продукції, що залежить від сталості цифрових послуг, і експортує програмне забезпечення, тож вважає забезпечення кібербезпеки одним із завдань оборони країни, використовує мілітаризований підхід і досить обмежено інформує про заходи, що будуть вживатися; крім того, активно залучає науковий потенціал і широко співпрацює з бізнесом, але залученість громадськості до формування політики низька. Величезна роль відведена державно-приватному партнерству у форматі наукових парків, які виробляють політику, заходи і здійснюють аналіз ризиків.

Близькими до України за організацією управління кібербезпекою є країни колишнього СРСР (Литва, Естонія), які ухвалили відповідні закони про кібербезпеку, чітко визначили повноваження основних суб'єктів кібербезпеки та встановили відповідальність за невиконання заходів. Так, Закон про основи національної безпеки Литви визначає сектори національної економіки, які мають значення для національної безпеки: енергетика, транспорт, інформаційні технології та телекомунікації, інші високотехнологічні сфери, фінанси та кредит.

У Литві стратегічні цілі та пріоритети політики кібербезпеки, а також заходи, необхідні для їх досягнення, визначає уряд, а не законодавчий орган чи Президент.

Як найкращу практику регулювання в Україні можна адаптувати для застосування литовський закон про кібербезпеку, але з певними застереженнями, оскільки Литва як член ЄС визнає і без змін «переносить» Регламенти ЄС, що в Україні здійснити неможливо. Утім, нашій державі все одно слід імплементувати як Директиви, так і Регламенти ЄС у цій сфері.

Країни «старої» Європи — Нідерланди та Іспанія (обидві за формою правління — монархії) — відзначаються досить цікавою організацією управління та взаємодії інституцій.

І в Іспанії, і в Нідерландах до ухвалення рішень щодо формування та реалізації політики у сфері кібербезпеки залучені численні органи, а нормативно-правові акти вводяться в дію королівськими указами. У Нідерландах до системи забезпечення кібербезпеки включені також організації регіонального рівня.

Спільним для всіх країн (крім США, які наразі займаються цим питанням) є відведення великої ролі державно-приватному партнерству як складнику інституційного забезпечення управління кібербезпекою.

Державно-приватне партнерство реалізується за такими напрямами:

- підготовка пропозицій для розробки стратегічних документів у сфері кібербезпеки;
- участь у розробці стандартів, як національних, так і міжнародних;
- консультативно-дорадча функція;
- науково-технічне співробітництво (держава — наукові кола, наукові кола — бізнес);
- широкі консультації із заінтересованими сторонами в межах консультативно-дорадчих органів.

Більшість країн мають аналог української РНБО, але, на відміну від України, вони є радше органами міжвідомчої координації та взаємодії з урядом як єдиного джерела політики виконавчої гілки влади.

Міністерства оборони, що відповідають за захист національного суверенітету, відіграють значну роль у сфері кібербезпеки.

У Литві розробку політики кібербезпеки та її реалізацію організовує, контролює та координує Міністерство національної оборони Литовської Республіки. А Національний центр кібербезпеки бере участь у розробці політики кібербезпеки тією мірою, якою має бути встановлено правове регулювання діяльності суб'єктів кібербезпеки для виконання функцій, передбачених цим законом.

Політику кібербезпеки реалізують Національний центр кібербезпеки, Державна інспекція захисту даних, Литовська поліція та інші органи влади, функції яких пов'язані з кібербезпекою.

Слід зазначити, що в усіх країнах регулятори координують свою діяльність у сфері захисту персональних даних та у сфері кібербезпеки в частині інформування про інциденти, порушення цілісності систем, вироблення політики з метою уникнення дублювання повноважень тощо. Технічна частина системи захисту персональних даних регулюється законодавством у сфері кібербезпеки, а безпосередньо захист прав осіб — органом, що здійснює контроль у сфері захисту персональних даних.

Окремо варто наголосити, що підхід європейських країн до забезпечення захисту об'єктів критичної інфраструктури уніфікований відповідно до Директиви NIS.

Суб'єктами загроз визначені ворожі держави, злочинні або терористичні організації та особи, об'єктами нападу визначено не тільки кіберпростір як окремий об'єкт, а й як частину суверенної території держави (Стратегії кібербезпеки США, Великої Британії).

У Стратегії кібербезпеки Литви виклики та загрози, зокрема для кібербезпеки, як окрема частина не наведені — Стратегія містить посилання на окремий документ, в якому зазначені виклики й загрози національній безпеці. Тобто в цій країні кіберпростір також не розглядають окремо від держави.

У Стратегії кібербезпеки Іспанії запропоновано цікаву модель управління національною кібербезпекою, яку слід вивчити детальніше з метою можливої імплементації в інших країнах.

Фактично, виклики і загрози, за винятком певних особливостей, визначені майже у всіх стратегіях однаково.

Щодо відмінностей, то у Стратегіях кібербезпеки США, Великої Британії та Литви прямо вказані як загрози деякі країни (а не тільки угруповання, що походять чи перебувають у певних країнах); ці країни — Росія, Китай та Північна Корея.

Інші держави прямо не озвучують конкретні ворожі країни, але визначають ті виклики й загрози, що можуть походити із певних країн.

Інші виклики можна розділити на такі категорії:

- кіберзлочинність;
- нові технології;
- цифровізація у сукупності;
- недостатній рівень цифрових навичок і культури безпеки;
- неконтрольованість ситуації з розповсюдженням і використанням сервісів великою кількістю пристроїв;
- глобалізація і передача обслуговування сервісів третім особам (хмарні послуги як виклик зазначені у кількох стратегіях).

Загалом варто звернути увагу на підхід Литви: визначення загроз національній безпеці без розподілу на кіберзагрози і звичайні загрози. Не менш цікавий тут і підхід до оцінювання: Литви та Велика Британія, на відміну від решти проаналізованих країн, визначають певні ключові показники, яких необхідно досягнути.

У більшості стратегій визнано гібридний характер загроз.

Технології спричинять далекосяжні зміни протягом найближчих років. Роботизація, сенсорні технології, 3D-друк, великі дані та штучний інтелект — усе це приклади технологічного прогресу, який може змінити суспільство. Ми матимемо доступ до цифрових сервісів, які навряд можемо собі уявити, — послуг, доступних у будь-якій точці світу 24/7. Наше повсякденне життя ставатиме дедалі більш цифровим, що насамперед приноситиме вигоду приватним особам, компаніям та владі.

Цифровізація тягне за собою низку викликів. Суспільство стає дедалі вразливішим до кіберзагроз, і щораз важливіше максимально усвідомлювати цю цифрову залежність. Цифрові інфраструктури та системи набувають дедалі більшої складності, глобальності й інтегрованості. До Інтернету підключаються всі види пристроїв, розширюється використання хмарних рішень. Необхідність скорочення витрат і збільшення доступу до компетентних послуг призводить до того, що дедалі більше цифрових послуг передаються третім сторонам, особливо в країнах з низькими доходами.

Складні (гібридні) загрози розмивають традиційну лінію розмежування між миром та збройним конфліктом та ставлять під сумнів звичайний розподіл відповідальності між цивільним та військовим секторами. Через високу швидкість технологічної еволюції вкрай ускладнюється прогнозування майбутніх головних загроз. Утім, імовірно, конкретні види загроз на кшталт програм-вимагачів, промислового шпигунства, саботажу, шантажу, шахрайства та крадіжки особи протягом найближчих років залишатимуться помітним явищем. Це загрози, які можуть бути націлені як на приватних осіб, так і на компанії, і завдають потерпілим серйозної шкоди.

Спільна риса більшості проаналізованих стратегічних документів — визначення відповідальність усіх сторін за кібербезпеку держави з огляду на особливості побудови й регулювання електронних комунікацій, які є спільними для держави, бізнесу та громадян.

У нідерландських документах прямо зазначено, що в результаті кібернападу шкідливого програмного забезпечення NotPetya в Україні постраждали суб'єкти господарювання Нідерландів.

Також у документах наголошено на необхідності регулювання питання кібербезпеки на міжнародному рівні, зокрема на рівні ООН, у зв'язку з транскордонністю мережі Інтернет та сервісів, що наразі використовуються всіма учасниками кіберпростору.

У стратегічному документі Великої Британії визначено, що для ефективного захисту інтересів держави необхідний комплексний підхід, і уряд готовий виділити ще більше коштів на заходи, заплановані на основі оцінки виконаного за попередні роки:

- унаслідок масштабу й динамічної природи кіберзагроз, а також уразливості й залежності поточний підхід сам по собі не забезпечує достатнього рівня безпеки;
- ринковий підхід до просування елементарних правил кібербезпеки не забезпечив необхідних темпів і масштабу змін; тому уряд має виявити ініціативу й уживати активніших заходів, використовуючи свій вплив і ресурси для боротьби з кіберзагрозами;
- уряд сам по собі не в змозі охопити всі аспекти національної безпеки. Потрібно впроваджувати інтегрований і сталий підхід, який передбачає залучення громадян, представників галузі та інших партнерів у суспільстві й владі до повноцінної участі в забезпеченні безпеки мереж, послуг і даних;
- Великій Британії потрібен життєздатний сектор кібербезпеки і відповідний кадровий резерв, які допоможуть йти в ногу із загрозами, що еволюціонують, і випереджати їх розвиток.

Більшість європейських країн працюватимуть над імплементацією нового європейського законодавства у сфері кібербезпеки в частині поки що добровільної можливості для бізнесу засвідчувати, що його продукти відповідають стандартам кібербезпеки ЄС. Європейська Комісія регулярно проводитиме оцінку необхідності впровадження обов'язковості тієї чи іншої схеми сертифікації.

Застосовувана схема сертифікації може визначати один або кілька рівнів забезпечення безпеки: базовий, значний або високий. На базовому рівні виробники ІКТ або постачальники послуг зможуть самі здійснювати оцінку відповідності. У разі значного чи високого рівня оцінювання здійснюватимуться національними органами з сертифікації кібербезпеки.

Держави-члени ЄС розроблять правила щодо покарань за порушення Основ та схем сертифікації кібербезпеки ЄС та надаватимуть ширші компетенції органам, відповідальним за кібербезпеку, для забезпечення співпраці й застосування рекомендацій ENISA.