DOI: https://doi.org/10.26642/jen-2022-3(101)-32-40
УДК 35.088.6:[004:007:351.86](477)

Л.А. Арсенович, доктор філософії
Департамент кадрової роботи та управління персоналом
Адміністрації Держспецзв'язку

Введення в органах публічної влади посад офіцерів із кіберзахисту як покращення стану кібербезпеки держави

Світ ІТ – досить великий і різноманітний. Він активно розвивається, підпорядковуючи собі чи не все навколо. Тенденція до розвитку сфери кібербезпеки вплинула і на навколишнє середовище, регулярно створюючи нові професії, пов'язані з ІТ-технологіями. Абсолютно точно, що в найближчі десятиліття сфера продовжить активно розвиватися, надаючи непогані можливості ІТ-фахівцям різних напрямів. ІТ-сфера зовсім не стоїть на місці і вже в найближчому майбутньому нас чекають абсолютно нові професії.

На сьогодні сфера кібербезпеки в Україні чи не найзатребуваніша в найближчому та віддаленому майбутньому. ІТ-індустрія вже потребує великої кількості web-розробників, програмістів, розробників ігор та аналітиків у сфері обчислювальної техніки, аналітиків з інформаційної безпеки. Проведений аналіз засвідчив, що інтенсивне зростання інформаційних технологій у майбутньому буде створювати як попит, так і пропозицію, у тому числі й на фахівців із кіберзахисту.

Впровадження в органах публічної влади посад офіцерів із кіберзахисту забезпечить подальше протистояння тим кіберзагрозам, що загрожують національній безпеці України, обмін досвідом, підходами, проведення спільних кібернавчань, а також мінімізацію можливостей для кібератак. Крім цього, введення в органах державної влади та на об'єктах критичної інфраструктури посад офіцерів із кіберзахисту стане дієвим «каталізатором» у подальшому створенні інструментів фінансового стимулювання працівників, які виконують завдання з адміністрування ІТ-систем, надасть змогу посилити відповідальність посадовців за невиконання вимог кіберзахисту, дозволить впроваджувати вимоги у «підрядних» організаціях, які працюють з органами державної влади, та усунути критичні вразливості в органах держвлади та на об'єктах критичної інфраструктури.

Ключові слова: *інформаційні технології; кібербезпека; кіберзахист; офіцер із кіберзахисту; цифровізація.*

Постановка проблеми у загальному вигляді та її зв'язок з важливими практичними завданнями. Світ не стоїть на місці та стає все більш технологічним. Змінюється і вид професій. Одна з особливостей найближчого майбутнього полягає в тісному проникненні інформаційних технологій в усі сфери життєдіяльності. Затребуваними стають спеціалісти, готові працювати з інформаційними технологіями та розвивати їх напрями. Підготуватися до таких реалій можна вже зараз, наприклад, вивчивши основи програмування або web-інженерії.

Ні для кого не секрет, що в майбутньому ринок праці чекають великі зміни. Підуть у минуле затребувані нині професії, а на їх місце прийдуть нові. Велика кількість перспективних професій на ринку праці зараз з'являється саме в ІТ-сфері. І на сьогодні це є загальноукраїнською тенденцією та загальносвітовим трендом. Багато нових професій зароджується і в психології, і в медицині, і в інших сферах діяльності.

Розвиток електронних пристроїв, потреба в знаннях комп'ютерних технологій, поява нових мов програмування дозволяє заглянути в майбутнє і зрозуміти, які професії в сфері інформаційних технологій можуть з'явитися в Україні у найближчі роки.

На сьогодні виникнення нових професій та посад не відображає появу нових технологій, а сигналізує про фундаментальні зрушення в галузі інформаційних технологій, особливо про їх еволюцію на всіх рівнях: від підрозділів та організацій з сервісної підтримки і технічного обслуговування до бізнес-лідерів та керівників державних органів.

Розпочата цифровізація державних та бізнес-процесів, за різними оцінками, ставить під ризик зникнення від 9 до 50 % всіх нині існуючих професій у найближче десятиліття. Зміст збережених «традиційних» професій істотно зміниться, інтегрувавши в себе нові технології. У найближчі 10–15 років відбудеться «поляризація кваліфікацій»: найбільш затребуваними будуть професії категорії «знання», а найменш затребуваними – категорії «уміння». У той же час кількість робочих місць середнього рівня кваліфікації буде відчувати найбільш сильний тиск нових технологій. До посад, які вже зараз зазнають скорочення у зв'язку з цифровізацією процесів, належать аналітики, бухгалтери, юристи, трейдери, рекрутери, адміністративний персонал та інші.

Зазначене потребує нормативно-правового забезпечення цієї сфери. При цьому майбутні зміни у законодавстві є передумовою ефективного формування інформаційної компетентності сучасного ІТ-фахівця, підвищення його ефективності та появи нових спеціальностей і професій у кібербезпеці.

Аналіз останніх досліджень та публікацій, на які спирається автор. Автоматизація вже наздогнала безліч професій, і темпи цієї експансії постійно наростають. Відповідно до дослідження Boston Consulting Group [1], до 2025 року з цієї причини по всьому світі незатребуваними будуть 10 млн чоловік. Щоб не опинитися «за бортом», майбутньому поколінню потрібно вчитися гнучкості і готуватися до безперервного підвищення кваліфікації протягом усього життя. Який же напрям вибрати? На думку аналітиків, сфера кібербезпеки стає все більш затребуваною. Ця професія вже зараз є однією з найбільш високооплачуваних. Спеціальності, які будуть найбільш популярними через п'ять років, вже існують. Щоб їх освоїти, досить зрозуміти, чого ти хочеш, і вибрати якісну та профільну освіту.

Дослідження проблематики потенціалу і тенденцій інноваційного розвитку високотехнологічних і традиційних секторів економіки України, в тому числі інформаційно-комунікаційних технологій, представлене в Національній доповіді «Інноваційна Україна 2020». Масштабні дослідження з цього питання здійснювалися Світовим банком, насамперед йдеться про «World Development Report 2016: Digital Dividends» [2] та «Reaping Digital Dividends: Leveraging the Internet for Development in Europe and Central Asia» [3].

У контексті нашого дослідження необхідно виокремити публікації О.Акіліної і Л.Ільїч [4], І.Діордіци [5], які розглядають питання конкурентоспроможності робочої сили ІТ-сфери через призму трансформацій ринку праці, вимоги роботодавців до майбутніх працівників сфери інформаційних технологій та характер репрезентації поняття «кваліфікаційні вимоги» до компетенцій фахівців із кібернетичної безпеки.

Водночас варто констатувати, що питання стосовно проблематики і стану наявних в Україні професій сфери інформаційно-комунікаційних технологій та подальших перспектив розвитку професій у сфері кібербезпеки залишилося поза увагою комплексних наукових досліджень галузі науки державного управління.

Метою статті є дослідження питання щодо введення в органах державної влади та на об'єктах критичної інфраструктури посад офіцерів із кіберзахисту із розробленням відповідних функцій та обов'язків.

Викладення основного матеріалу. В Україні зараз триває етап трансформації цифрового середовища. З'являється все більше цифрових послуг, які надають як державні інституції, так і приватні фірми та компанії. Наприклад, кількість користувачів додатка «Дія» вже перевищила 6 млн осіб. Такі поняття, як онлайн-покупки (банкінг, спілкування) відіграють все більшу роль у повсякденній діяльності.

Розвиток інформаційних технологій все більше потребує відповідних фахівців із кібербезпеки. Щоденно у світі відбуваються десятки тисяч кібератак, що здійснюються різними суб'єктами, знаходячи при цьому більш витончені методи для своїх злочинних дій. Міжнародний експерт Стів Морган з Cybersecurity Ventures зазначає, що втрати бізнесу в світі від кіберзлочинності сягнули до 2021 року 6 трлн доларів США, а витрати на кіберзахист з 2017 до 2023 року будуть становити 1 трлн.

В Україні стрімко зростає кількість кібератак на державні структури та приватні компанії. В розпал війни на сході країни (2016 рік) лише на органи державної влади здійснювалося близько 100 000 спроб кібератак щомісяця, які були спрямовані на критичну енергетичну, фінансову і транспортну інфраструктуру. У 2019 році Служба безпеки України нейтралізувала понад 480 кібератак на органи держвлади та об'єкти критичної інфраструктури, припинили функціонування більш ніж 1 000 вебресурсів.

З початком повномасштабного вторгнення росії під загрозою опинилися сайти українських військових і державних установ та об'єктів критичної інфраструктури. Згідно з дослідженням Держспецзв'язку, упродовж перших місяців війни в Україні зафіксовано 362 кібератаки (це утричі більше, ніж у такий самий період 2021 року). При цьому половина атак була спрямована на Уряд, органи державної влади, сектор безпеки й оборони України та комерційні організації. Саме тому підприємства потребують вироблення дієвих механізмів управління цими ризиками й у першу чергу механізмів кібер- та інформаційної безпеки [6, с. 29].

Питання власної кібербезпеки та захисту інформації стали предметом дослідження міжнародної некомерційної організації ISC, яка спеціалізується на сертифікації спеціалістів з інформаційної безпеки. У дослідженні взяли участь 1 500 представників ІТ-галузі з різних країн. Майже половина респондентів (49 %) планує у найближчий рік найняти більше фахівців для захисту своїх даних і мереж, тоді як 39 % планує залишити все як є. Опитування показало, що найбільший дефіцит фахівців з кібербезпеки – у Тихоокеанському регіоні, куди входять США і Китай (2,15 млн). У Європі – 498 000 вакансій у цій сфері, в Африці та на Близькому Сході – 142 000, у Латинській Америці – 136 000.

Дефіцит фахівців у сфері кібербезпеки призвів до зниження якості робочої сили. Згідно з результатами дослідження, 37 % роботодавців незадоволені низькою підготовкою фахівців у цій галузі.

Кого ж роботодавці хочуть бачити на посаді фахівця з кібербезпеки? Найціннішими для 49 % роботодавців є співробітники, які раніше вже працювали у сфері кібербезпеки. А 47 % дивиться в першу чергу на навички претендентів, для 43 % важлива наявність професійних сертифікатів, для 41 % – наявність диплома про релевантну вищу освіту.

Як показує аналіз у сфері кібербезпеки, працює 35 % молодих людей і 24 % жінок, що пов'язано перш за все з високими зарплатами. У середньому фахівець з інформаційної безпеки за кордоном може розраховувати на $85 000 на рік. При цьому визнані кіберзахисники отримують, як правило, більше за $88 000, тоді як новачки – щонайменше $67 000.

Знайти фахівця із кібербезпеки міжнародного рівня та з достатнім практичним досвідом роботи в Україні не просто. Як зазначає генеральний менеджер компанії Information Systems Security Partners (ISSP) Роман Сологуб, пошуки таких фахівців із кібербезпеки в Україні можуть тривати декілька місяців.

Список найбільш затребуваних IT-спеціальностей 2021 року за кордоном містить такі професії: системний архітектор, програміст, системний адміністратор, розробник програмного забезпечення, фахівець із кібербезпеки, web-інженер тощо. Так, за офіційними дослідженнями Бюро трудової статистики США (Bureau of Labor Statistics), прогнозується зростання потреби у фахівцях з кібербезпеки на 37 % на рік до 2023 року, і деякі експерти називають такі цифри доволі консервативними. На думку кандидатів на ці посади, ринок кібербезпеки також виглядає дуже перспективним – тут вже пропонують зарплатню на $10 000 вищу, аніж середня зарплата у США. Для працівників це хороші новини, але для світу не дуже. Кіберзагрози ставатимуть все масштабнішими та різноманітними. Отже, кібербезпека стосуватиметься усіх та усього – приватних осіб, корпорацій, інфраструктури та навіть урядів. Бо усе це все більше залежить від поєднаних мереж, систем та пристроїв.

За даними PricewaterhouseCoopers, в Україні в IT-сфері працює понад 90 тисяч програмістів (комп'ютерних аналітиків, різноманітних операторів, фахівців, інженерів сфери інформаційно-комунікаційних технологій). Експерти припускають, що до 2025 року пропозиція у таких фахівцях в країні буде найвищою, про що свідчать зазначені в таблиці 1.

Таблиця 1

Пропозиція робочої сили за кваліфікаційними групами

Кваліфікаційні групи	2020 рік	2025 рік	% зміни у 2020–2025 роках
Соціальні науки і науки про поведінку, соціальна робота	131,64	136,10	3,39
Право	123,68	131,40	6,23
Менеджмент і адміністрування	123,62	124,92	1,05
Електротехніка	121,60	118,28	-2,73
Сектор обслуговування	118,94	116,68	-1,89
Охорона здоров'я	120,57	116,08	-3,72
Інформаційні технології	97,91	108,62	10,93
Електроніка і телекомунікації	111,11	107,30	-3,43
Освіта	112,47	107,30	-4,60
Гуманітарні науки, культура і мистецтво, журналістика	99,71	99,98	0,27
Менеджмент і адміністрування	103,80	96,91	-6,63
Машинобудування	95,08	92,94	-2,25
Архітектура і будівництво	91,09	88,02	-3,37
Біологія, природничі науки, математика і статистика	71,72	70,63	-1,52
Транспорт	70,74	70,15	-0,84
Аграрні науки і продукти харчування, ветеринарна медицина	75,02	69,83	-6,93
Виробництво і технології	61,78	62,75	1,57
Хімічна промисловість і біотехнології	45,82	45,18	-1,40
Інше	84,25	88,88	5,49

Джерело: складено автором за даними [7]

Як видно з таблиці 1, зростання пропозиції робочої сили прогнозується для меншого числа кваліфікаційних груп. Найбільше зростання пропозиції очікується для груп «Інформаційні технології» –

на 10,93 %, «Право» – на 6,23 %, «Інші» – на 5,49 %, і «Соціальні науки і науки про поведінку, соціальна робота» – на 3,39 % [7]. Однак, згідно з інформацією з різноманітних інноваційних форумів, це не межа і кількість таких спеціалістів може бути ще вища.

Будь-яка передача цінностей – це фактично обмін даними, і якщо третя сторона зможе перехопити цю інформацію або видозмінити її, то тим самим людина або компанія зазнає цілком реальних матеріальних збитків. Щоб цього не сталося, і потрібні фахівці з безпеки інформаційних систем, які створюють надійну структуру обміну даними, передбачають дії зловмисників, знаходять і усувають уразливості в мережевих системах [8].

При цьому кількість кібератак зростає з кожним днем, як і стабільно збільшується кількість компаній, які переходять працювати в інтернет. За прогнозом Markets and Markets, ринок кібербезпеки до 2023 року виросте до $248,3 млрд. Тому проблем з пошуком високооплачуваних вакансій для фахівців з інформаційної безпеки в доступному для огляду майбутньому не передбачається [8].

Україна веде бойові дії на землі (повітрі, воді) та в кіберпросторі. Від російських хакерів страждають усі органи виконавчої влади. Кожен орган публічної влади знаходиться в зоні ризику будь-якої миті.

Саме керівник відповідальний за кіберзахист в установі. Як свідчать дослідження, переважна більшість керівників вважає, що кіберзахист – це зона відповідальності або офіцера із кіберзахисту (технічного директора), або CDTO. Але це не так. Керівники починають цікавитися питаннями кіберзахисту свого підприємства в кращому разі тільки після того, як «його зламають». При цьому багато керівників управляє своїми компаніями, виходячи зі свого особистого досвіду, бачення, інтуїції і неструктурованої інформованості про динаміку і стан розвитку ІКТ. Менеджери, які несуть відповідальність за діяльність організації в цілому, мають володіти більш широким баченням перспектив і проблем, що пов’язані з впровадженням інформаційно-комунікаційних технологій у різні сфери діяльності, і умінням управляти довгостроковим становленням інформаційно-комунікаційних систем у компанії [9, с. 10–11].

Головне завдання керівника в контексті кіберзахисту – це створення «культури кіберзахисту». Кіберзахист має стати основним підґрунтям кожної установи. А її керівник має зробити так, щоб всі службові процеси були вибудувані навколо цього. При цьому «крутим» спеціалістом з безпеки інформаційних систем бути не потрібно – це завдання інших фахівців. Проте варто бути в курсі усіх змін в законодавстві, розширяти знання про основи кібербезпеки, читати про кіберзагрози та застосовувати свою лідерську позицію для того, щоб стратегічно впливати на цей напрям.

Саме усвідомлення загрози та особистої відповідальності допомагає перейти безпосередньо до дій із забезпечення кіберзахисту установи. І перше завдання для керівників – це пов’язати місію установи з безпекою даних, активів і людей. Це має бути сформульований основоположний принцип, який визначає безпеку та конфіденційність як оперативні цілі.

Понад 90 % кібератак стали успішними саме через людський фактор. Тобто, якби на підприємстві була створена культура кіберзахисту, таких проблем вдалося би уникнути. Про це під час брифінгу за підсумками засідання РНБО України заявив голова Держспецзв’язку Юрій Щиголь. «З метою покращення стану кібербезпеки держави було прийнято рішення щодо введення в органах державної влади та на об’єктах критичної інфраструктури посад офіцерів із кіберзахисту з підпорядкуванням Службі захисту інформації та нормативного закріплення заробітної плати не нижче ринкової», – повідомив посадовець.

Необхідно зауважити, що на сьогодні потреба подальшого введення в органах державної влади нових посад, пов’язаних з ІТ-сферою, вже має правове підґрунтя, хоча такий процес і повільно рухається. Підтвердженням цього стало перше рішення Кабінету Міністрів України у 2019 році, а саме постанова Кабінету Міністрів України № 56 «Деякі питання цифрового розвитку», яка затвердила принципи державної політики цифрового розвитку для їх реалізації органами виконавчої влади. Однак деякі позиції цього рішення мають тільки рекомендаційний характер. Так пунктом 3 постанови міністерствам, іншим центральним органам виконавчої влади надано завдання тільки розглянути можливість утворення та забезпечення функціонування структурних підрозділів (спеціалістів) з питань цифрового розвитку, цифрових трансформацій і цифровізації, при чому тільки в межах граничної чисельності працівників апарату міністерств, інших центральних органів виконавчої влади.

Об’єкти критичної інфраструктури також повинні мати у своєму складі підрозділ або посадову особу з інформаційної безпеки, що відповідають за політику інформаційної безпеки, прийняту на об’єкті критичної інфраструктури, та контроль за її дотриманням. Як зазначено у Переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 19 червня 2019 року № 518, під час визначення відповідальних за інформаційну безпеку перевага повинна надаватися особам, які мають фахову освіту та досвід роботи у сфері технічного захисту інформації або інформаційної безпеки. Крім цього, підрозділ або посадова особа з інформаційної безпеки мають бути підпорядковані безпосередньо керівнику об’єкта критичної інфраструктури, а функції підрозділу або посадової особи з інформаційної безпеки можуть бути

покладені на службу захисту інформації підприємства, установи або організації. Проведений аналіз показує, що зазначена норма залишилася лише на папері.

Таке неоднозначне становище змінило Мінцифри у березні 2020 року, запропонувавши Кабінету Міністрів України ввести у міністерствах, інших центральних органах виконавчої влади посаду заступника керівника відповідного органу з питань цифрового розвитку, цифрових трансформацій і цифровізації (Chief Digital Transformation Officer). Відповідне рішення було ухвалено Урядом на засіданні 03 березня 2020 року (постанова Кабінету Міністрів України № 194). Залишається чекати, що такий важливий крок в умовах сьогодення дійсно дозволить просувати цифровізацію у всіх сферах економіки, як на загальнодержавному, так і на регіональному рівнях, у тому числі запроваджувати нові спеціальності, посади й професії у сфері кібербезпеки.

Основним завданням фахівця із кіберзахисту є забезпечення захисту інформації установи, країни або громадян. Фахівці цього напряму працюють в банках, у сфері оборони, урядових структурах, медицині, транспортних підрозділах (диспетчерські служби військової і цивільної авіації), комунальних службах та інших сферах. В СБ України – це Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, в Нацполіції – Департамент кіберполіції, в Держспецзв'язку – це Департамент кіберзахисту Адміністрації Держспецзв'язку та Державний центр кіберзахисту тощо. Але в переважній більшості в державних органах влади та на об'єктах критичної інфраструктури таких спеціалістів немає. Взагалі в Україні таку посаду можна зайти менш ніж в 5 % компаній.

Професійно підготовлений спеціаліст з кіберзахисту завжди зуміє відбити кібератаку, а дуже хороший спеціаліст ніколи її не допустить. Згідно з дослідженням PwC, лише 40 % підрозділів добре розуміють свої кіберризики у ланцюгу поставок. Тоді як кібератаки саме через ланцюжки постачань – актуальна проблема для всієї держави. Прикладом є кібератака 14 січня 2022 року на сайти Уряду, окремих міністерств і навіть сайт застосунку «Дія».

Робота офіцера із кіберзахисту полягає в організації та забезпеченні функціонування засобів програмного захисту інформації тієї чи іншої установи, налагодженні та підтримці роботи апаратної частини. Кажучи простою мовою, він повинен дуже добре розбиратися в роботі ПЕОМ, комп'ютерних мереж, вміти писати програмне забезпечення, а в разі потреби – створити дієвий антивірус. Більш детальніше зазначено на рисунку 1.

Введення в органах публічної влади посад офіцерів із кіберзахисту надасть змогу забезпечити:

- визначення принципів і побудову стратегії інформаційної безпеки. Моніторинг внутрішніх і зовнішніх загроз;
- використання системи інформаційної безпеки на основі оцінки ризиків для даних і встановлення достатніх вимог для їхнього захисту;
- управління кіберризиками у межах діяльності органів публічної влади;
- розробку, моніторинг і звітність за ключовими показниками інформаційної безпеки;
- впровадження системи контролю інформаційної безпеки для кожного структурного підрозділу органу публічної влади;
- розробку і моніторинг виконання процесів інформаційної безпеки для дотримання відповідного рівня конфіденційності даних;
- впровадження процесу управління інцидентами інформаційної безпеки для своєчасного виявлення і контролю порушень інформаційної безпеки;
- визначення та впровадження процесів безпеки ІТ, що забезпечують захист ІТ-активів;
- поінформованість про інформаційну безпеку співробітників органу публічної влади.

Крім цього, введення в органах державної влади та на об'єктах критичної інфраструктури відповідних фахівців із кіберзахисту зможе у подальшому впровадити:

- захист у кіберпросторі національних електронних інформаційних ресурсів, технологічних і комунікаційних систем, у тому числі тих, що використовуються для задоволення суспільних потреб;
- захист об'єктів критичної інформаційної інфраструктури;
- захист інтересів людини та суспільства у кіберпросторі;
- розроблення навчальних програм кібергігієни на державному, регіональному (місцевому) рівнях;
- заходи із формування культури кібербезпеки на підприємствах, на об'єктах критичної інфраструктури та інших установах;
- інформування громадян про кіберінциденти.

Функції офіцера із кіберзахисту	Обов'язки офіцера із кіберзахисту
Супроводження системи інцидент-менеджменту	Виявлення атак і розпізнавання вторгнень. Локалізація та усунення наслідків. Ідентифікація нападника (або джерела розповсюдження шкідливих програм). Оцінка і подальший аналіз процесу нападу
Супроводження системи управління вразливостями	Проведення зовнішніх і внутрішніх сканувань. Аналіз знайдених вразливостей і їхня категоризація за рівнями критичності. Контроль процесу усунення вразливостей
Супроводження систем захисту інформації	Системи антивірусного захисту. Аналітичної системи. Системи запобігання витоку конфіденційної інформації. PAM-системи
Контроль налаштувань мережевого обладнання	Визначення топології мережі та її проєктування. Підбір необхідного обладнання та його установка. Прокладка кабелю та налаштування активного мережевого обладнання. Тестування обладнання
Забезпечення безпеки інформації	Захист об'єктів інформаційної системи. Захист процесів, процедур і програм обробки інформації. Захист каналів зв'язку (акустичні, інфрачервоні, провідні оптичні, радіоканали тощо). Придушення побічних електромагнітних випромінювань і наведень. Управління системою захисту
Моніторинг працівників	Організація відеоспостереження. Моніторинг телефонних розмов. Використання GPS-технологій. Моніторинг працівників через ІТМ
Ведення ключів ЕЦП до інформаційної платформи	Забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у платформі, з використанням електронного цифрового підпису
Участь у розслідуваннях інцидентів інформаційної безпеки	Відновлення нормальної роботи служб у найкоротші терміни. Зведення до мінімуму впливу інцидентів на роботу організації. Забезпечення злагодженої обробки всіх інцидентів і запитів обслуговування. Зосередження ресурсів підтримки на найбільш важливіших напрямах. Надання відомостей, що дозволяють оптимізувати процеси підтримки, зменшити кількість інцидентів і спланувати управління
Кадрова безпека	Відбір і попередня перевірка персоналу, прийнятого на роботу (службу). Навчання співробітників. Досягнення взаєморозуміння керівників і співробітників у питаннях забезпечення інформаційної безпеки. Психологічна підготовка з метою протистояння методам «соціальної інженерії»
Технічний супровід управління інформаційними системами	Забезпечення доступу до актуальних легальних оновлень, програм і конфігурацій. Забезпечення можливості користування сервісами для відправки електронної документації. Отримання інформаційно-методичних матеріалів з налаштування і ефективного використання програм. Забезпечення цілодобового доступу до офіційних інтернет-ресурсів для оперативного отримання технологічної інформації. Організація безпечного доступу до офісних додатків з будь-якої точки світу в один клік. Організація консультаційної підтримки

Джерело: розробка автора

Рис. 1. Функції та обов'язки офіцера із кіберзахисту

Цифровізація створює значні кіберзагрози, для подолання яких необхідні радикальні зміни, у тому числі на рівні керівників органів публічної влади. В умовах, коли швидкість прийняття того чи іншого рішення є критично важливою, офіцери із кіберзахисту та їх керівники мають впровадити культуру безпеки на кожному рівні роботи з системами та даними. Створення такої культури надасть змогу офіцерам із кіберзахисту:

- міркувати та діяти як топменеджер. Керівники напряму кіберзахисту та кібербезпеки мають говорити мовою топменеджерів, знаходити спільні інтереси та загальну точку зору на питання кіберзахисту з керівниками організацій, добре розумітися на політиках організації. У подальшому, офіцери із кіберзахисту стануть тими особами, які завжди будуть обличчям підрозділу – це буде сприяти зміцненню відповідної довіри до них;
- розширювати перелік своїх повноважень. Обов'язки офіцера із кіберзахисту повинні розширюватися та включати безпеку інформації, запобігання кіберінцидентам та кіберподіям, взаємодію з іншими сторонами, дотримання законодавчих вимог та допомогу у протидії кіберзлочинності;
- інтегрувати кібербезпеку в організаційну ДНК. Зазначена інтеграція здійснюється шляхом впровадження безпеки у процеси управління, освіти, а також через встановлення правильного співвідношення корпоративних (особистих) показників ефективності;
- сформувати надійну команду із кібербезпеки та будувати партнерство. Офіцери із кіберзахисту мають залучати таланти з необхідними навичками та вибудовувати нові партнерські відносини із професіоналами у кібербезпеці;
- автоматизувати ручні процеси. Обсяги даних будуть продовжувати збільшуватися, тому автоматизація стає обов'язковим елементом роботи будь-якої команди з кіберзахисту. Автоматизація зменшує обсяг ручних операцій та скорочує дефіцит кадрів. Крім того, підвищує ефективність та допомагає досягти кращих результатів у відповідних процесах. Все це буде будувати безпеку у підрозділі і поліпшувати досвід користувачів;
- вивчати нові технології у сфері інтернету речей, штучного інтелекту, технологій 4G (5G), машинного навчання, аналітики тощо;
- зміцнити екосистему кібербезпеки. Оскільки головне завдання офіцера із кіберзахисту – це контролювати та пильнувати кіберзагрози, вони мають поєднувати багато ролей та обов'язків. Такі фахівці стають інфлуенсерами, тобто такими, які будуть сприяти підвищенню поінформованості про безпеку працівників, вибудовуючи при цьому культуру кібербезпеки та кібергігієну в установі.

Висновки та перспективи подальших досліджень. Кібербезпека – одне з пріоритетних завдань держави, що визначене в багатьох стратегічних документах. Майбутні спеціалісти повинні нестандартно мислити, добре володіти іноземною мовою, щоб спілкуватися зі своїми колегами з інших країн, розумітися на надсучасних технологіях і практиках. Професії сфери кібербезпеки та кіберзахисту існують зовсім нещодавно, але вже починають переформатовувати ринок праці і ставати привабливими не тільки для школярів, що визначаються із вибором майбутньої спеціальності, але й для професіоналів із інших галузей, які замислюються про перепрофілювання.

На теперішній час кількість сучасних кіберзагроз зростає у геометричній прогресії. Щоб захист був комплексним і надійним, в організації має бути співробітник, відповідальний за всі аспекти інформаційної безпеки, що організовує і супроводжує роботу всіх систем IT-захисту.

Усвідомлення кіберзагрози та відповідальності штовхає до певних дій із забезпечення кіберзахисту підприємства. При цьому організація кіберзахисту на підприємстві, на нашу думку, повинна базуватися на трьох базисних речах: на принципах, людях та відповідних пріоритетах.

Принципи. Одне із перших завдань для будь-якого керівника – це пов'язати місію (напрям) установи з безпекою даних, активів і людей. Це має бути чітко сформульований та конкретизований основоположний принцип, який визначає безпеку та конфіденційність в установі.

Люди. Серйозне ставлення до кіберзахисту починається з призначення відповідного фахівця з інформаційної безпеки та надання йому відповідних повноважень. При цьому керівник повинен навчати колектив певним навичкам і мисленню, які налаштують його на ризики кібербезпеки.

Пріоритети. Керівник має підвищити пріоритет кіберзахисту двома способами: переглянувши структуру підприємства та зробивши кібербезпеку складовою стратегії.

На сьогодні можна констатувати, що на сучасному етапі всі зазначені вище заходи кіберзахисту не набули системного характеру, немає напрацьованих дієвих механізмів державного управління цією сферою. Тотальна ж інформатизація суспільства ставить перед державою глобальні завдання подолання загроз, які вона несе з собою. І від їх вирішення сьогодні залежить не лише розвиток, а і в цілому існування держави як незалежної та конкурентоздатної. І саме професіонали можуть протистояти цим загрозам [10, с. 39].

Список використаної літератури:

1. A $2 Trillion Plan to Bring Two Billion More People into the Digital Age [Electronic resource]. – Access mode : https://www.bcg.com/publications/2020/plan-to-bring-high-speed-internet-access-to-two-billion-people.
2. World Development Report 2016: Digital Dividends [Electronic resource]. – Access mode : https://cutt.ly/8V7GllZ.
3. Reaping Digital Dividends: Leveraging the Internet for Development in Europe and Central Asia [Electronic resource]. – Access mode : https://www.worldbank.org/en/region/eca/publication/digital-dividends-in-eca.
4. *Акіліна О.В.* Конкурентоспроможність робочої сили ІТ-сфери через призму трансформацій ринку праці / *О.В. Акіліна, Л.М. Ільїч* // Науковий вісник Ужгородського національного університету. Сер. : Міжнародні економічні відносини та світове господарство. – 2018. – Вип. 18 (1). – С. 10–16.
5. *Діордіца І.* Кваліфікаційні вимоги до компетенцій фахівців із кібербезпеки / *І.Діордіца* // Підприємництво, господарство і право. – 2017. – № 2. – С. 215–219.
6. *Ткачук В.О.* Електронний бізнес: переваги та ризики в період цифрової трансформації / *В.О. Ткачук, Т.Ю. Мельник, Ю.В. Богоявленська* // Економіка, управління та адміністрування. – 2021. – № 4 (98). – С. 28–36.
7. Аналітичний звіт щодо професійно-кваліфікаційного прогнозування в Україні [Електронний ресурс]. – Режим доступу : https://cutt.ly/gVmvfiT.
8. Професії майбутнього: ТОП-7 напрямків, що будуть популярними до 2020 року // Сайт Національного університету харчових технологій [Електронний ресурс]. – Режим доступу : https://cutt.ly/7V7GQOt.
9. *Обіход С.В.* Імплементація інформаційно-комунікаційних технологій у систему управління бізнес-процесами вітчизняних підприємств у контексті розвитку цифрової економіки / *С.В. Обіход* // Економіка, управління та адміністрування. – 2021. – № 4 (98). – С. 10–17.
10. *Герасимюк К.Х.* Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення / *К.Х. Герасимюк* // Економіка, управління та адміністрування. – 2021. – № 3 (97). – С. 36–40.

References:

1. A $2 Trillion Plan to Bring Two Billion More People into the Digital Age, [Online], available at: https://www.bcg.com/publications/2020/plan-to-bring-high-speed-internet-access-to-two-billion-people
2. World Development Report 2016: Digital Dividends, [Online], available at: https://cutt.ly/8V7GllZ
3. Reaping Digital Dividends: Leveraging the Internet for Development in Europe and Central Asia, [Online], available at: https://www.worldbank.org/en/region/eca/publication/digital-dividends-in-eca
4. Akilina, O.V. and Il'i'ch, L.M. (2018), «Konkurentospromozhnist' robochoi' syly IT-sfery cherez pryzmu transformacij rynku praci», *Naukovyj visnyk Uzhgorods'kogo nacional'nogo universytetu*. Ser. *Mizhnarodni ekonomichni vidnosyny ta svitove gospodarstvo*, Issue 18 (1), pp. 10–16.
5. Diordica, I. (2017), «Kvalifikacijni vymogy do kompetencij fahivciv iz kiberbezpeky», *Pidpryjemnyctvo, gospodarstvo i pravo*, No. 2, pp. 215–219.
6. Tkachuk, V.O., Mel'nyk, T.Ju. and Bogojavlens'ka, Ju.V. (2021), «Elektronnyj biznes: perevagy ta ryzyky v period cyfrovoi' transformacii'», *Ekonomika, upravlinnja ta administruvannja*, No. 4 (98), pp. 28–36.
7. Analitychnyj zvit shhodo profesijno-kvalifikacijnogo prognozuvannja v Ukrai'ni, [Online], available at: https://cutt.ly/gVmvfiT
8. Nacional'nij universytetu harchovyh tehnologij, *Profesii' majbutn'ogo: TOP-7 naprjamkiv, shho budut' populjarnymy do 2020 roku*, [Online], available at: https://cutt.ly/7V7GQOt
9. Obihod, S.V. (2021), «Implementacija informacijno-komunikacijnyh tehnologij u systemu upravlinnja biznes-procesamy vitchyznjanyh pidpryjemstv u konteksti rozvytku cyfrovoi' ekonomiky», *Ekonomika, upravlinnja ta administruvannja*, No. 4 (98), pp. 10–17.
10. Gerasymjuk, K.H. (2021), «Mehanizmy derzhavnogo upravlinnja kiber- ta informacijnoju bezpekoju: problemy ta shljahy vyrishennja», *Ekonomika, upravlinnja ta administruvannja*, No. 3 (97), pp. 36–40.

Арсенович Леонід Антонович – доктор філософії, заступник начальника управління, начальник відділу Департаменту кадрової роботи та управління персоналом Адміністрації Держспецзв'язку.

https://orcid.org/0000-0001-7081-2838.

Наукові інтереси:

– публічне управління та адміністрування;
– кіберосвіта;
– цифрова трансформація.

E-mail: arsen-leon@ukr.net.

Arsenovych L.A.

Introduction of positions of cyber protection officers in public authorities as an improvement of state cyber security

The world of IT is quite large and diverse. It is actively developing, subordinating almost everything around. The trend towards the development of the field of cyber security has also affected the environment, regularly creating new professions related to IT technologies. It is absolutely certain that the field will continue to develop actively in the coming decades, providing good opportunities for IT specialists in various fields. The IT sphere does not stand still at all and completely new professions await us in the nearest future.

Today, the field of cyber security in Ukraine is perhaps the most in-demand in the near and distant future. The IT industry already needs a large number of web developers, programmers, game developers and analysts in the field of computing, information security analysts. The conducted analysis proved that the intensive growth of information technologies in the future will create both demand and supply, including for cyber security specialists.

The introduction of the positions of cyber protection officers in public authorities will ensure further resistance to those cyber threats that threaten the national security of Ukraine, exchange of experience, approaches, joint cyber training, as well as minimization of opportunities for cyber attacks. In addition, the introduction of cyber protection officer positions in state authorities and critical infrastructure facilities will be an effective «catalyst» in the further creation of tools for financial incentives for employees who perform IT system administration tasks, will make it possible to strengthen the responsibility of officials for non-compliance with cyber protection requirements , will make it possible to implement requirements in «contracted» organizations that work with state authorities, and to eliminate critical vulnerabilities in state authorities and critical infrastructure facilities.

Keywords: information technology; cyber security; cyber protection; cyber protection officer; digitalization.

Стаття надійшла до редакції 04.08.2022.