DOI: 10.26565/2310-9513-2021-14-03 ISSN 2310-9513
УДК 65.012.8(613)

ПРОБЛЕМИ ПОБУДОВИ КОНСОЛІДОВАНИХ СТРАТЕГІЙ УПРАВЛІННЯ КОРПОРАТИВНОЮ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В РЕГІОНІ ЕМЕА*

Лубенець Сергій Васильович
кандидат технічних наук, доцент
кафедра міжнародних відносин, міжнародної інформації та безпеки
Харківський національний університет імені В.Н. Каразіна
майдан Свободи, 6, м. Харків, 61022
e-mail: s.lubenec@karazin.ua
ORCID: https://orcid.org/0000-0003-1061-8763
Харченко Ігор Михайлович
кандидат технічних наук, доцент
кафедра міжнародних відносин, міжнародної інформації та безпеки
Харківський національний університет імені В.Н. Каразіна
майдан Свободи, 6, м. Харків, 61022
e-mail: kharchenko@karazin.ua
ORCID: https://orcid.org/0000-0002-1372-0408
Новікова Людмила Вікторівна
кандидат юридичних наук, доцент
кафедра міжнародних відносин, міжнародної інформації та безпеки
Харківський національний університет імені В.Н. Каразіна
майдан Свободи, 6, м. Харків, 61022
e-mail: L.novikova@karazin.ua
ORCID: https://orcid.org/0000-0002-4640-2908

Розглянуто проблеми розробки та побудови універсальної консолідованої стратегії взаємодії служб ІТ та інформаційної безпеки, яка ґрунтується на вивченні та глибокому аналізі статистичних даних, що стосуються існуючої ситуації із взаємодією корпоративних служб ІТ і безпеки в різних міжнародних компаніях різних галузей і країн світу, з урахуванням досвіду відповідних фахівців, експертів та аналітиків. Предметом дослідження в статті є питання оптимальної взаємодії служб ІТ і безпеки у забезпеченні високого рівня корпоративної інформаційної безпеки в регіоні ЕМЕА**.** Мета – полягає в аналізі проблематики щодо побудови та реалізації консолідованих стратегій управління ІТ та безпекою з метою усунення неузгодженості та підвищення ефективності роботи відповідних служб для забезпечення дієвої інформаційної безпеки організацій на прикладі регіону ЕМЕА. Завдання**:** обробка та аналіз результатів онлайн-опитування, що стосується взаємодії служб ІТ і безпеки компаній і організацій різних галузей в різних країнах і регіонах світу, в тому числі в регіоні ЕМЕА; дослідження проблем та переваг побудови консолідованої стратегії управління ІТ та забезпечення інформаційної безпеки в регіоні ЕМЕА; розробка рекомендацій щодо вирішення існуючих проблем у виробленні і побудові корпоративних стратегій ефективного управління ІТ та забезпечення інформаційної безпеки. Використовується загальнонауковий метод системного аналізу – для визначення особливостей взаємодії служб ІТ і безпеки компаній і організацій різних галузей в різних регіонах світу, а також для досліджень проблем і переваг уніфікованої консолідованої стратегії управління ІТ та забезпечення інформаційної безпеки. Отримано такі результати: на основі кількісної та якісної оцінки, а також аналізу результатів опитування фахівців та експертів у сфері ІТ та безпеки в регіоні ЕМЕА визначено участь підрозділів компаній у розробці та реалізації стратегій у сфері інформаційної безпеки; визначено основні задачі ІТ-служб і служб безпеки в організації їх спільної роботи та узгодження дій між собою; досліджено основні перешкоди в організації спільної роботи ІТ-служб та служб безпеки компаній, серед яких суттєвими є істотна напруженість та конфлікти між співробітниками служб, глобальний та регіональний брак кваліфікованих кадрів, технічні складнощі. Висновки: встановлено, що консолідована стратегія управління ІТ та забезпечення інформаційної безпеки на основі досягнень в галузі безпеки і технологій здатна

* ***Cite as:*** Lubenets, S., Harchenko, I., Novikova, L. (2021). Problems of Building Consolidated Corporation Strategies for Corporate Information Security Management in the EMEA Region, *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism.* 14, 24-34. (in Ukrainian). https://doi.org/10.26565/2310-9513-2021-14-03

допомогти вирішити основні проблеми ефективної взаємодії відповідних служб компаній; розроблено ряд рекомендацій щодо вирішення існуючих проблем побудови корпоративних стратегій ефективного управління ІТ та забезпечення інформаційної безпеки, що покликані сприяти усуненню неузгодженості та підвищенню ефективності роботи відповідних служб для забезпечення дієвої інформаційної безпеки організацій у регіоні ЕМЕА в різних організаціях і компаніях, не залежно від сфери їх діяльності.

Ключові слова: інформаційні технології, інформаційна безпека, управління інформаційною безпекою, стратегії управління, консолідована стратегія управління, служба ІТ, служба безпеки.

Постановка проблеми. По всьому світу служби ІТ та безпеки щодня стикаються з серйозними ризиками і проблемами. Однак у багатьох випадках ці підрозділи розділені між собою і тільки заважають один одному, не виступаючи єдиним фронтом з консолідованою стратегією забезпечення інформаційної безпеки. Напруженість відносин між фахівцями в області ІТ і безпеки підсилює цей поділ і напруженість в сфері безпеки. У зв'язку з цим актуальним є пошук і розробка уніфікованої, консолідованої стратегії оптимальної взаємодії служб ІТ і безпеки з метою ефективного управління та забезпечення високого рівня корпоративної інформаційної безпеки в різних регіонах світу.

Аналіз останніх досліджень і публікацій. Питання взаємовідносин, налагодження взаємодії, вибудовування партнерства між службами ІТ і безпеки, пошук шляхів їх зближення і ефективної співпраці у забезпеченні ефективної інформаційної безпеки розглядалися в ряді робіт дослідників, аналітиків і профільних фахівців. Зокрема, в роботі [1] розглянуто основні причини виникнення конфліктних ситуацій у взаємодії та співпраці служб ІТ та інформаційної безпеки, розроблено ряд рекомендації щодо їх усунення. У статті [2] розглядаються проблеми узгодженості стратегічних цінностей компанії для ефективного управління інформаційною безпекою. Авторами побудована теоретична модель управління інформаційною безпекою на основі стратегічної узгодженості, з урахуванням основних факторів ефективного управління ІТ-безпекою. Результати показують, що при узгодженій роботі служб, підтримці вищого керівництва та обізнаності організації про ризики та інструменти безпеки можна розробити ефективні засоби контролю інформаційної безпеки, що призведе до успішного управління нею. В роботі [3] досліджуються проблемні питання щодо досягнення хороших стосунків, успішної співпраці вказаних служб та безпеки навколишнього середовище в кіберпросторі, забезпечення цілісного підходу до інформаційної безпеки на прикладі Латвії.

Однак важливою є проблема розробки універсальної консолідованої стратегії взаємодії служб ІТ та інформаційної безпеки, яка б ґрунтувалася не тільки на досвіді певних компаній або окремих фахівців і аналітиків, але й на вивченні та глибокому аналізі статистичних даних, що стосуються існуючої ситуації із взаємодією корпоративних служб ІТ і безпеки в різних компаніях різних галузей і країн світу. Для цього повинна бути зібрана, вивчена і проаналізована інформація про взаємини між службами ІТ і безпеки для порівняно великої кількості організацій, з урахуванням думок широкого кола експертів і провідних фахівців відповідних профілів з різних куточків планети.

Мета статті, завдання дослідження. Метою роботи є аналіз проблематики щодо побудови та реалізації консолідованих стратегій управління ІТ та безпекою з метою усунення неузгодженості та підвищення ефективності роботи відповідних служб для забезпечення дієвої інформаційної безпеки організацій на прикладі регіону ЕМЕА.

Відповідно до мети дослідження в роботі були поставлені та вирішувалися наступні *завдання*:

– обробити і проаналізувати результати онлайн-опитування, що стосується взаємодії служб ІТ і безпеки компаній і організацій різних галузей в різних країнах і регіонах світу, в тому числі в регіоні ЕМЕА;

– дослідити проблеми та переваги побудови консолідованої стратегії управління ІТ та забезпечення інформаційної безпеки в регіоні ЕМЕА;

– розробити рекомендації щодо вирішення існуючих проблем у виробленні і побудові корпоративних стратегій ефективного управління ІТ та забезпечення інформаційної безпеки.

Для вирішення вказаних завдань в даній роботі був проведений аналіз результатів оцінки взаємодії служб ІТ і безпеки компаній і організацій різних галузей в різних регіонах світу, в тому числі відносин між керівниками вищого рівня, рівня менеджерів і директорів зазначених структур, отриманих компанією Forrester Consulting [4] у 2020 році. У роботі також представлені результати досліджень проблем і переваг, які тягне за собою уніфікована консолідована стратегія управління ІТ та забезпечення інформаційної безпеки.

Основні результати дослідження. Компанією Forrester Consulting було проведено глобальне онлайн-опитування, в якому взяли участь 1451 респондент рівня менеджера і вище з ІТ-служб і служб безпеки міжнародних компаній, що працюють в різних галузях і країнах світу (рис. 1). Також були опитані вісім

директорів з інформаційних технологій та інформаційної безпеки. Кожен учасник опитування мав певний вплив на прийняття рішень, що стосуються стратегії забезпечення інформаційної безпеки організації, або це входило в його посадові обов'язки.

Із зазначених 1451 учасника опитування 665 перебували в регіоні EMEA (Європа, Близький Схід та Африка). Тому основна увага в даній роботі приділяється результатам опитування та їх аналізу саме в регіоні EMEA.

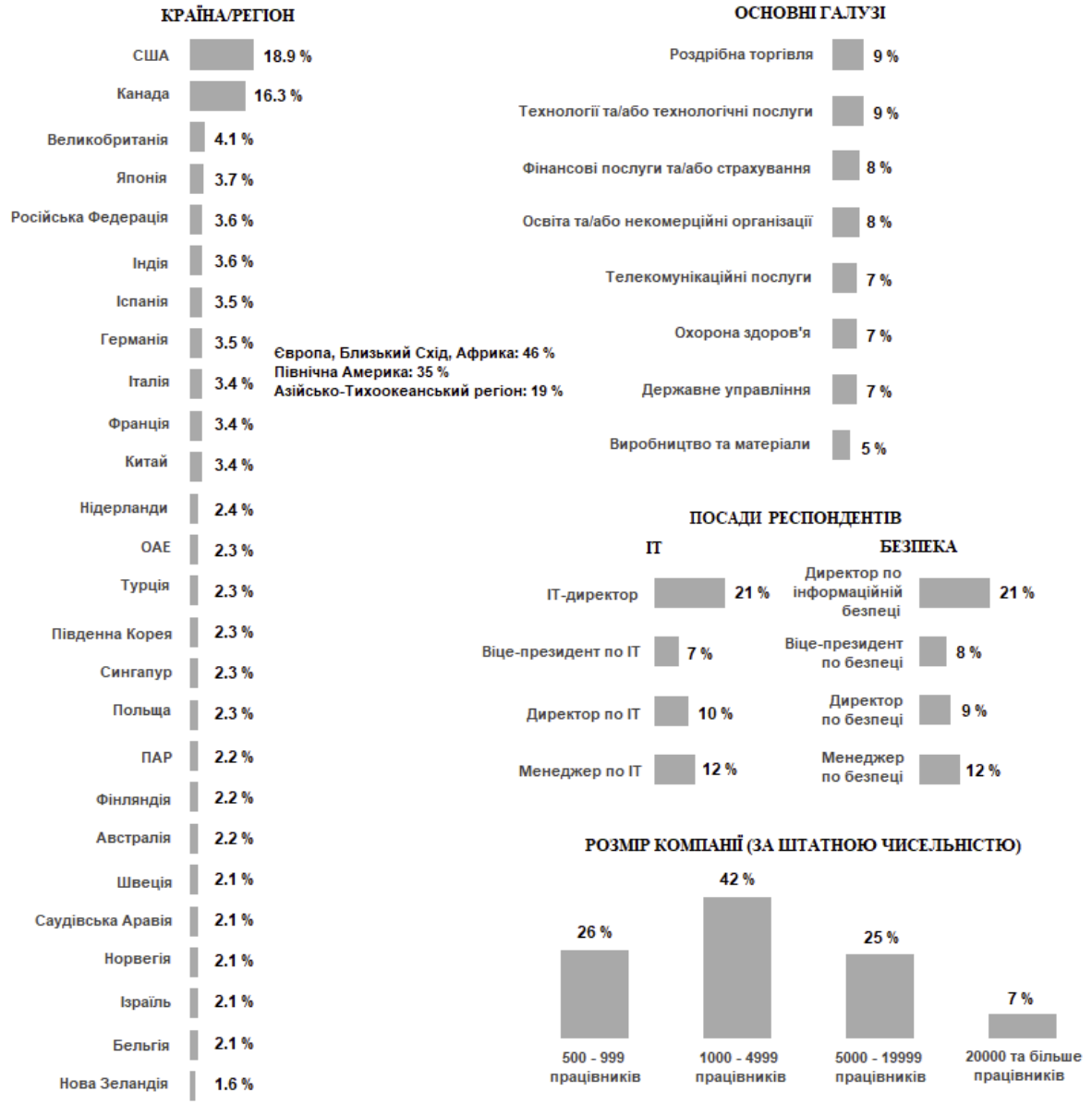

*Рис. 1. Країни, регіони, галузі та контингент онлайн-опитування**
**Розроблено авторами за матеріалами: [4]*

В ході досліджень було встановлено, що незважаючи на старання компаній усунути перешкоди між IT-службою та службою безпеки, певна напруженість між ними зберігається. На думку представників компаній, без єдиної стратегії в області IT і безпеки, що реалізується в рамках заснованої на застосуванні технологій спільної роботи з використанням загальних інструментів, домогтися успіхів у сфері інформаційної безпеки складно.

Результати проведеного опитування показали [4], що в регіоні EMEA спільна робота має першорядну важливість як для IT-служб, так і для служб безпеки. При цьому компанії називають організацію спільної роботи IT-служби та служби безпеки своїм першочерговим завданням на найближчий період часу і переходять на використання моделі загальних завдань.

Однак незважаючи на цілі організації щодо спільної роботи, погані відносини серйозно заважають відповідним службам. Колективи IT-служб і служб безпеки в регіоні EMEA стикаються з проблемами у всіх областях, будь

то кадри, процеси чи технології. При тому, що переважна більшість учасників опитування відзначають погані відносини між фахівцями відповідних служб, постійні труднощі з організацією спільної роботи не викликають подиву.

Учасники опитування приходять до спільної думки про те, що консолідовані стратегії є вирішенням основних проблем, з якими стикаються групи фахівців. Намагаючись протистояти цій напруженості у відносинах, організації з регіону EMEA намагаються реалізувати більш одноманітну і консолідовану стратегію управління IT та забезпечення інформаційної безпеки. Хоча така стратегія і була прийнята лише в третині організацій, найближчим часом заплановано прийняття відповідної стратегії з метою підвищення безпеки та прозорості і в інших організаціях.

Таким чином, незважаючи на наявні проблеми, служби IT та безпеки визначають налагодження спільної роботи як першочергове завдання. В даний час служби IT та безпеки набувають все більшої важливості для міжнародних організацій по всьому світу. Тепер, як ніколи раніше, життєво необхідно мати єдиний підхід до забезпечення інформаційної безпеки. Забезпечення такої безпеки більше не є завданням виключно фахівців служби безпеки. Стають абсолютно необхідними спільні з IT-службою (включаючи підрозділ, що обслуговує комп'ютерні мережі) зусилля.

В результаті виконання кількісної та якісної оцінки, а також аналізу проведеного опитування в регіоні EMEA, були отримані наступні результати:

1. *Забезпечення безпеки стає спільним завданням декількох підрозділів.* Міжнародні організації усвідомили, що забезпечення інформаційної безпеки має бути «командним спортом», і переносять велику частину пов'язаних із забезпеченням безпеки обов'язків у загальну модель, яка використовується декількома підрозділами. Наприклад, в розробці та реалізації стратегії забезпечення інформаційної безпеки беруть участь багато підрозділів, а не тільки служба безпеки (рис. 2).

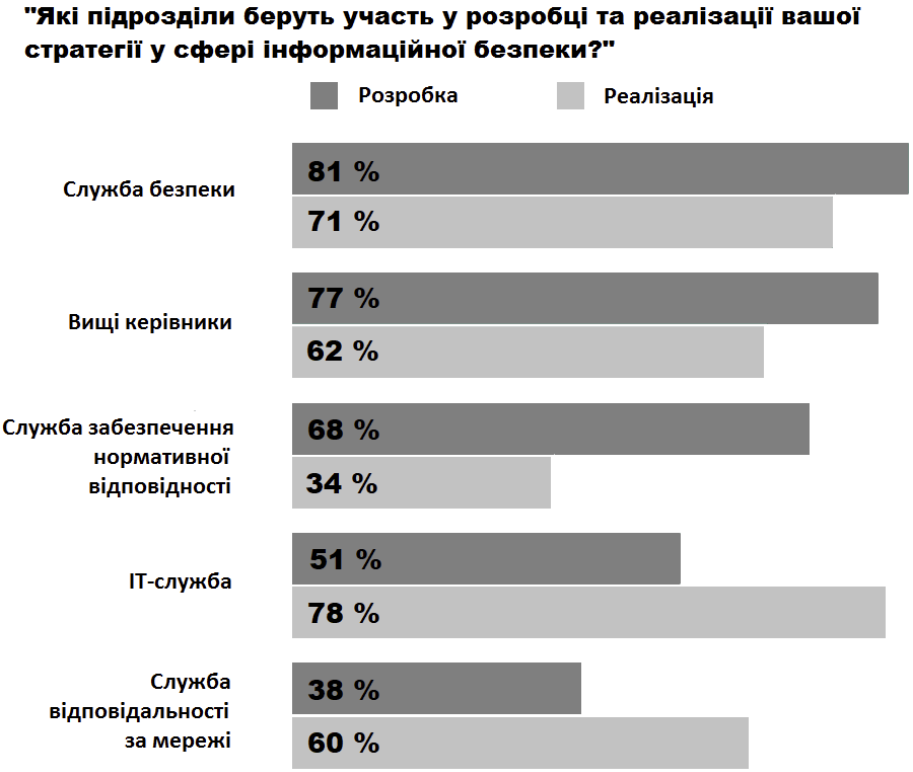

*Рис. 2. Участь підрозділів у розробці та реалізації стратегій у сфері інформаційної безпеки в регіоні EMEA**

**Розроблено авторами за матеріалами: [4]*

Хоча всього 51% учасників опитування з регіону EMEA відзначили, що їхні фахівці IT-служб беруть участь у розробці стратегії забезпечення інформаційної безпеки (зазвичай це завдання виконує служба безпеки і виконавче керівництво вищого рівня), 78% повідомили, що IT-служба відповідає за реалізацію такої стратегії. Однак ступінь участі виконавчого керівництва вищого рівня коливається в залежності від країни. У Російській Федерації (92%) та Іспанії (90%) особливо наголошується участь в розробці стратегії забезпечення інформаційної безпеки виконавчого керівництва вищого рівня, тоді як

у Великобританії цей показник падає до всього лише 50%. Згідно з відповідями респондентів з цієї країни, основна роль як при розробці (83%), так і при реалізації (82%) стратегії відводиться ІТ-службі. Незважаючи на розбіжності у відповідях, абсолютно очевидно, що розробка і реалізація стратегії забезпечення інформаційної безпеки більше не є обов'язком виключно служб безпеки.

2. *Спільна робота та узгодження дій є в регіоні EMEA найбільш важливими аспектами.* Вказуючи найбільш важливі завдання на наступні 12 місяців, фахівці ІТ-служб і служб безпеки відзначили, що основним пріоритетом для них буде організація спільної роботи і узгодження дій між собою (55%) (рис. 3).

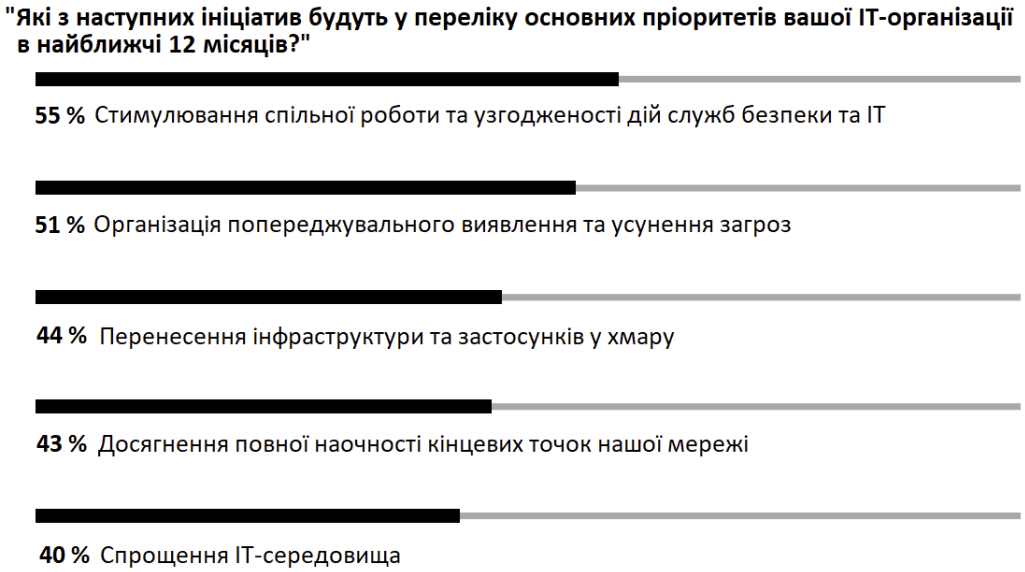

*Рис. 3. Основні задачі ІТ-служб в регіоні EMEA**
**Розроблено авторами за матеріалами: [4]*

У таких країнах як Іспанія (73%) і Російська Федерація (60%) цей показник ще вище. Однак у РФ в якості ще більш важливої відзначають іншу задачу: організацію попереджувального виявлення загроз і реагування на них (65%). Повний список пріоритетних завдань для регіону EMEA в повній мірі охоплює всі сфери бізнесу: кадри, процеси і технології. Для керівників вищого рівня очевидно, що між ІТ-службою та службою безпеки повинні бути встановлені позитивні відносини спільної роботи, які спираються на технології та процеси.

Результати аналізу ситуації показали, що незважаючи на загальну задачу організації спільної роботи, для її виконання існують значні перешкоди, які фахівці цих служб часто створюють самі собі. Досліджуючи ці перешкоди, було встановлено наступне:

1. *Не дивлячись на те, що метою є спільна робота, для регіону EMEA характерним є істотна напруженість між співробітниками ІТ-служб і служб безпеки.* При оцінці цих відносин встановлено, що найбільш негативні відносини існують між ІТ-службою та службою безпеки в цілому (рис. 4). Це в першу чергу продиктовано поганими відносинами між фахівцями з інформаційних технологій та безпеки (віце-президент і нижче).

2. *Служби ІТ і безпеки відчувають глобальний та регіональний брак кваліфікованих кадрів.* Хоча багато респондентів з регіону EMEA і відзначили брак кадрів, це не є проблемою одного регіону. Брак кваліфікованих кадрів спостерігається по всьому світу як в області ІТ (53% в регіоні EMEA, 52% в Північній Америці, 53% в Азійсько-Тихоокеанському регіоні), так і в області безпеки (59% в регіоні EMEA, 69% у Північній Америці , 65% в Азійсько-Тихоокеанському регіоні).

Наприклад, розмірковуючи про глобальну нестачу кваліфікованих кадрів у сфері безпеки, ІТ-директор однієї з організацій по створенню технічних рішень із США зазначив [4]: «Існує величезна нестача кадрів. Недостатність трудових ресурсів і знань у сфері безпеки очевидна. Думаю, ситуація поліпшується, але дуже повільно. На ринку Канади тепер існують університети, які спеціалізуються на програмах, пов'язаних з безпекою. В Онтаріо фактично створюється спеціальний університет або коледж для підготовки фахівців з кібербезпеки. У США ситуація виправляється, але все ще дуже складно найняти фахівців необхідної кваліфікації. В Австралії це практично неможливо. У Сполученому Королівстві це також складне завдання. Так що нестача фахівців у сфері безпеки безумовно існує по всьому світу».

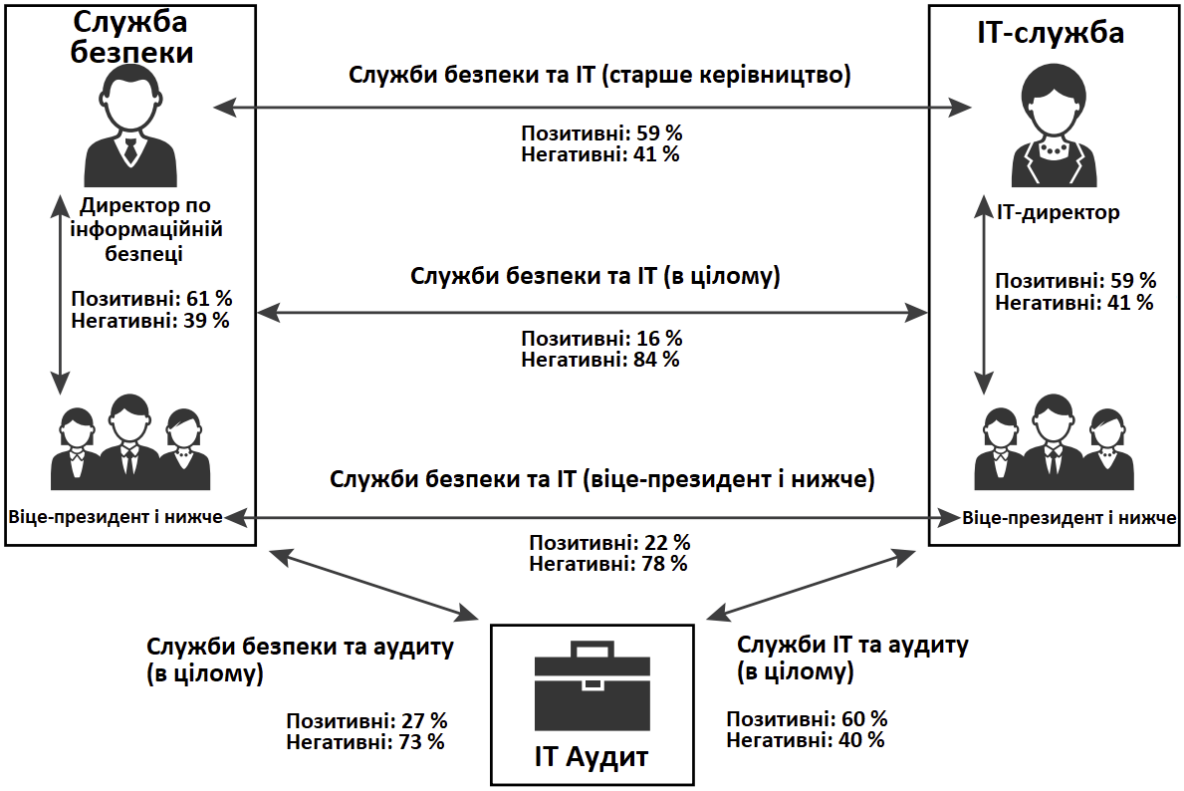

*Рис. 4. Особливості відносин між службами IT та безпеки в регіоні EMEA**
**Розроблено авторами за матеріалами: [4]*

Незважаючи на те, що респонденти з регіону EMEA відзначили, що їх організації вжили додаткових заходів щодо підвищення заробітних плат і пільг, що пропонуються для залучення хороших фахівців (73%), знайти відповідних фахівців все ще дуже складно. Респонденти з регіону EMEA також відзначали, що дуже або виключно складно знайти відповідного фахівця з безпеки (85%), виявлення загроз (72%) та IT (69%). У деяких країнах організації відзначають велику нестачу фахівців, ніж в інших. Наприклад, відсоток респондентів, які вважають, що дуже або виключно складно знайти відповідного фахівця з безпеки, вкрай високий у Німеччині (90%), Іспанії (92%) та Франції (96%).

3. *Зазначені проблеми додатково посилюються технічними складнощами.* На практиці технічні складнощі додатково погіршують і без того недостатню співпрацю, так як фахівці різних служб стикаються з величезною кількістю неузгоджених інструментів, неефективними продуктами для забезпечення інформаційної безпеки та іншими безпековими проблемами. В середньому компанії регіону EMEA використовують 28,2 продуктів для забезпечення інформаційної безпеки. Однак тільки 34% респондентів вказали, що ці рішення в основному або повністю інтегровані (рис. 5). Велика кількість розрізнених інструментів для забезпечення інформаційної безпеки і відсутність інтеграції призводять до високого ступеня незадоволеності. Навіть говорячи про корпоративні брандмауери – одних з найбільш поширених інструментів у сфері інформаційної безпеки на ринку, – тільки половина (53%) респондентів з регіону EMEA відзначили, що задоволені наявними рішеннями.

4. *Тільки третина респондентів з регіону EMEA задоволені стратегією в області IT та безпеки.* Ще більше ускладнює співпрацю те, що навіть коли служби в рамках існуючої моделі імовірно й повинні б гармонійно працювати разом, – це конфлікти між співробітниками служб. Це спостерігається по всьому світу, а не тільки в регіоні EMEA. При тому, що спільна робота є найважливішим завданням для респондентів, тільки 29% учасників опитування з регіону EMEA відмітили, що на сьогодні мають єдину і консолідовану стратегію управління IT та забезпечення інформаційної безпеки (30% у Північній Америці, 31% в Азійсько-Тихоокеанському регіоні). Незважаючи на те, що 40% респондентів у регіоні EMEA планують впровадити єдину стратегію в найближчі 12 місяців, організації займають наздоганяючу позицію і консолідують стратегії у вигляді запізнілою реакції на виникаючі проблеми, а не використовують консолідацію в якості основи для роботи обох служб.

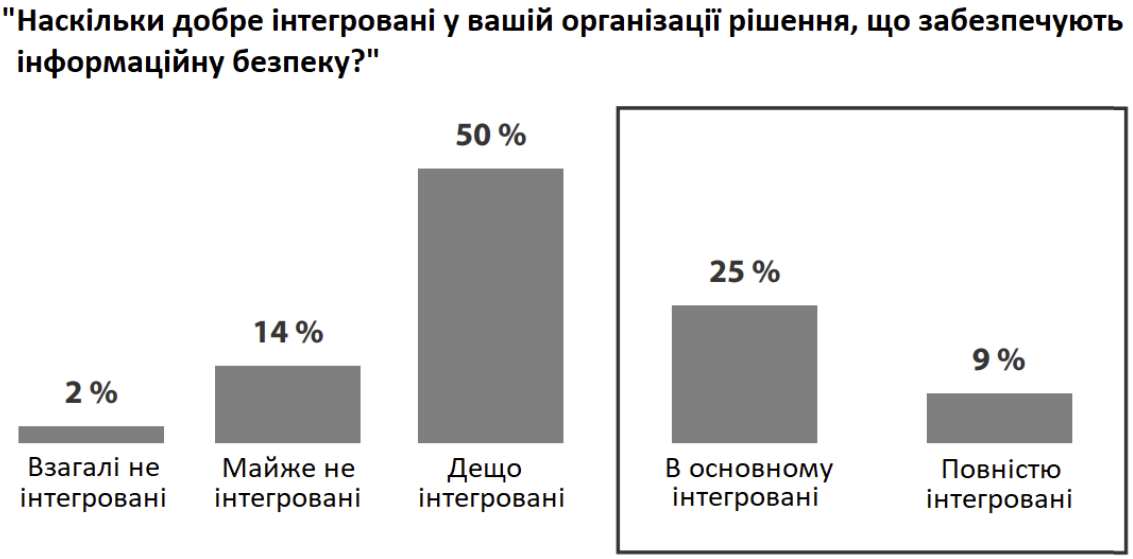

*Рис. 5. Рівень інтеграції рішень щодо забезпечення інформаційної безпеки в регіоні EMEA**
**Розроблено авторами за матеріалами: [4]*

Для вирішення зазначених вище проблем і створення єдиної стратегії забезпечення інформаційної безпеки організаціям необхідно враховувати всі основні внутрішні вектори підприємства: кадри, процеси і технології. Досліджуючи переваги єдиної стратегії забезпечення безпеки, були отримані наступні висновки:

1. *Служби знають про проблеми з співробітництвом і планують їх усунути в короткостроковій перспективі.* Незважаючи на перешкоди, організації сповнені рішучості вирішити проблеми взаємодії служб і пом'якшити наслідки майбутніх криз. В даний час 54% респондентів з регіону EMEA згодні з тим, що служби IT та безпеки хочуть бути уніфікованими, але вони стикаються з перешкодами, що заважають цьому. Хоча респонденти з Франції і не заявляють про існування на сьогоднішній день такої кількості перешкод (тільки 34%), учасники опитування з Іспанії відчувають великі труднощі і в 69% випадках заявляють про перешкоди для їх уніфікації. При цьому респонденти з Іспанії, як і з усіх інших країн регіону EMEA, розраховують, що в майбутньому перешкод стане менше. Тільки 17% організацій з регіону EMEA (18% в Іспанії) вважають, що існуючі перешкоди будуть продовжувати заважати уніфікації і через три-п'ять років. Це означає, що компанії посилено прагнуть вирішити ці критичні проблеми зі спільною роботою служб вже зараз, щоб закласти більш надійний фундамент на майбутнє.

2. *Консолідована стратегія управління IT та забезпечення інформаційної безпеки здатна допомогти вирішити основні проблеми.* Основною складовою вирішення наявних проблем фахівці з регіону EMEA вважають наявність консолідованої стратегії, яка охоплює кадри, процеси і технології. Компанії повинні шукати шляхи зняття напруженості у відносинах і усунення технологічних бар'єрів, які перешкоджають досягненню успіху. Створення уніфікованої і консолідованої стратегії забезпечить відповідних фахівців належними інструментами і придатними для виконання роботи процесами. Це дозволить організувати забезпечену технічними засобами і технологіями спільну роботу за допомогою застосування загальних інструментів, що стане дуже серйозним кроком у напрямку зниження кількості прогалин у системі інформаційної безпеки – ці два аспекти є найважливішими для організацій (рис. 6).

3. *Досягнення в галузі безпеки і технологій є основною рушійною силою для прийняття єдиної стратегії.* Організації регіону EMEA, що вже прийняли єдину стратегію, відзначають три основних стимули, які підштовхнули їх до цього:

– підвищена безпека (46%);
– вдосконалення технологій (45%);
– зручність відслідковування ресурсів (45%).

Характерно, що підвищену інформаційну безпеку назвали головним стимулом фахівці як IT-служб, так і служб безпеки організацій по всьому світу. Вони знають, що цю безпеку не може забезпечувати лише служба безпеки.

Таким чином, консолідовані стратегії є вирішенням основних проблем, з якими стикаються групи фахівців IT та безпеки.

Висновки та перспективи подальших розробок. Проведені в роботі дослідження показали, що в регіоні EMEA простежується велике бажання фахівців служб IT і безпеки працювати спільно, але результат спроб співпраці часто призводить до невдоволення служб одна одною. Розбіжні пріоритети, розрізнені технології, конкуренція за час, увагу,

бюджети може привести до провалу навіть самих продуманих стратегій.

Однак на основі проведеного компанією Forrester детального опитування осіб, які приймають рішення у сфері інформаційної безпеки, по єдиних стратегіях в області IT та безпеки, можна сформулювати кілька важливих рекомендацій, які покликані уникнути зазначених вище проблем:

1. *У регіоні EMEA служби вже бачать, що IT та інформаційна безпека стають завданням, що вимагає спільних зусиль, але їм необхідно працювати над безперешкодністю консолідації.*

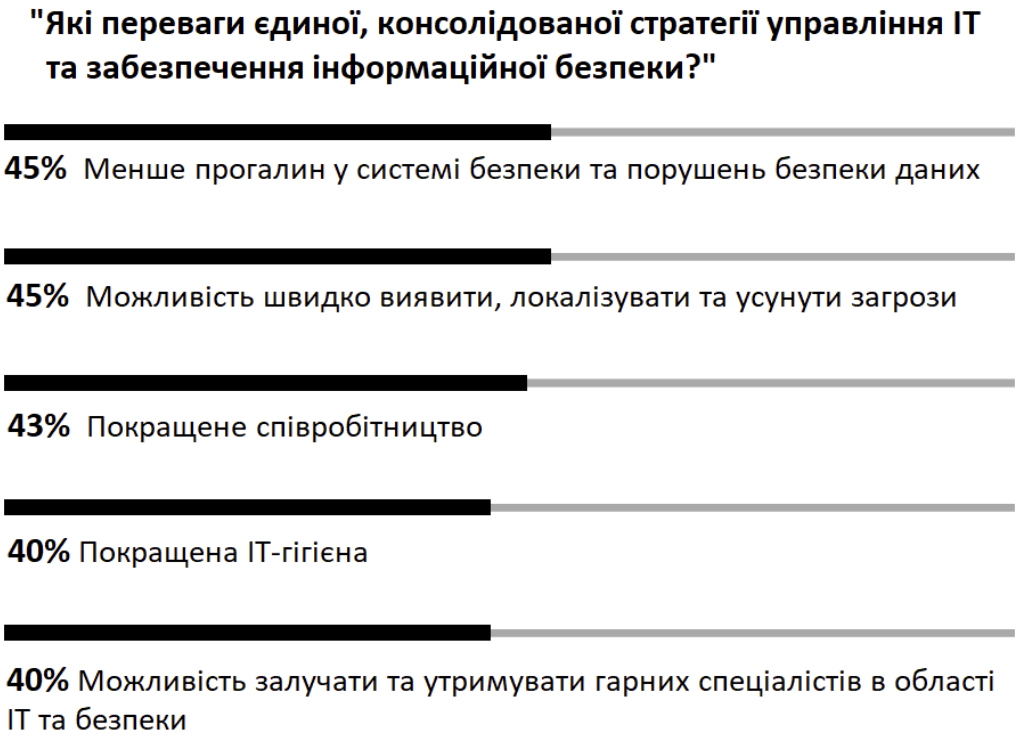

*Рис. 6. Основні переваги консолідованої стратегії управління інформаційною безпекою в регіоні EMEA**
**Розроблено авторами за матеріалами: [4]*

Сьогодні ця сфера стала вимагати компетентності в різних дисциплінах, що вимагає використання знань фахівців з дуже різних підрозділів. Це можуть бути окремі групи або підрозділи в одному департаменті. В будь-якому випадку керівники в області IT і безпеки повинні використовувати успішні приклади колег, щоб прийти до моделі загальної відповідальності, яка містить різні області спеціалізації, необхідні службам для успішного захисту ініціатив підприємства в області технологій, захисту користувачів і здатності захистити бренди і репутацію компанії від великого збитку. Необхідно зрозуміти, що найбільш успішні колективи мають відкриті канали зв'язку, працюють над доповнюючими одна одну (а не конкуруючими) цілями і спільно використовують консолідовані процеси і технології коли це можливо, щоб підвищити ефективність своїх зусиль.

2. *Для скорочення кількості прогалин і більш швидкого реагування стратегія управління IT та забезпечення інформаційної безпеки повинна бути консолідованою.*

Організації, які вважають, що вони успішно уніфікували свої стратегії, вказують на спрощення життя фахівців служби безпеки у вигляді більш швидкого отримання відповідей і усунення загроз. Ці переваги в поєднанні зі скороченням кількості прогалин у системі інформаційної безпеки приносять більшу вигоду службам IT і безпеки. Консолідація стратегії управління IT та забезпечення інформаційної безпеки може здаватися трудомістким завданням, але це окупається.

3. *Технології не повинні заважати ресурсам в регіоні EMEA в досягненні спільного успіху.*

На жаль, більшість учасників опитування вважають, що їм заважають застарілі підходи постачальників, з якими вони працюють. Незважаючи на прикладені для уніфікації стратегій і поліпшення співпраці зусилля, організації залишаються непідготовленими, недостатньо інтегрованими і незадоволеними результатами через інструменти і технології, які застаріли, але продовжують використовуватися. Для уніфікації служб IT і безпеки необхідно почати шукати технології, які б відповідали потребам обох груп зацікавлених осіб, підходили і IT-службі, і службі безпеки, і знімали напруженість через конкуренцію за обмежені ресурси.

Таким чином, розроблені в даній статті рекомендації, засновані на аналізі проблематики побудови і реалізації консолідованих стратегій управління IT та безпекою в регіоні EMEA, покликані сприяти усуненню неузгодженості та підвищенню ефективності роботи відповідних служб для забезпечення дієвої інформаційної безпеки організацій у даному регіоні. Крім того, на прикладі регіону EMEA ці рекомендації також можуть бути використані різними організаціями і компаніями, не залежно від сфери їх діяльності та місцезнаходження, для вирішення існуючих універсальних проблем у формуванні й реалізації корпоративних стратегій ефективного управління IT та забезпечення інформаційної безпеки.

Основними напрямками подальших досліджень розглянутої проблематики можуть бути розробки більш конкретних, детальних та універсальних підходів і рекомендацій, що стосуються:

– зближення служб IT та безпеки;

– налагодження їх спільної ефективної роботи та співпраці;

– вироблення, реалізації та безперервне вдосконалення консолідованих стратегій управління корпоративною інформаційною безпекою організацій та установ у різних країнах світу з урахуванням їх регіональної специфіки.

PROBLEMS OF BUILDING CONSOLIDATED CORPORATION STRATEGIES FOR CORPORATE INFORMATION SECURITY MANAGEMENT IN THE EMEA REGION

Serhii Lubenets, Candidate of Technical Sciences (Ph. D.), Docent, Department of International Relations, International Information and Security, V.N.Karazin Kharkiv National University, Freedom Square, 6, Kharkiv city, Ukraine, 61022, e-mail: s.lubenec@karazin.ua, ORCID: https://orcid.org/0000-0003-1061-8763
Igor Harchenko, Candidate of Technical Sciences (Ph. D.), Docent, Department of International Relations, International Information and Security, V.N.Karazin Kharkiv National University, Freedom Square, 6, Kharkiv city, Ukraine, 61022, E-mail: kharchenko@karazin.ua, ORCID: https://orcid.org/0000-0002-1372-0408
Ljudmyla Novikova, Candidate of Juridical Sciences (Ph. D.), Docent, Department of International Relations, International Information and Security, V.N.Karazin Kharkiv National University, Freedom Square, 6, Kharkiv city, Ukraine, 61022, E-mail: L.novikova@karazin.ua, ORCID: https://orcid.org/0000-0002-4640-2908

The problems of development and construction of a universal consolidated strategy of interaction of IT services and information security, which is based on the study and in-depth analysis of statistics on the current situation with the interaction of corporate IT services and security in different international companies in different industries and countries, are considered. specialists, experts and analysts. The subject of research in the article is the issue of optimal interaction of IT and security services in ensuring a high level of corporate information security in the EMEA region. The goal is to analyze the issues related to the construction and implementation of consolidated strategies for IT and security management in order to eliminate inconsistencies and increase the efficiency of the relevant services to ensure effective information security of organizations on the example of the EMEA region. Objectives: processing and analysis of the results of an online survey on the interaction of IT and security services of companies and organizations in various industries in different countries and regions of the world, including the EMEA region; research of problems and advantages of building a consolidated strategy of IT management and information security in the EMEA region; development of recommendations for solving existing problems in the development and construction of corporate strategies for effective IT management and information security. The general scientific method of systems analysis is used to determine the features of interaction between IT services and security of companies and organizations of different industries in different regions of the world, as well as to study the problems and benefits of a unified consolidated IT management strategy and information security. The following results were obtained: based on quantitative and qualitative assessment, as well as analysis of the results of the survey of IT and security specialists and experts in the EMEA region, the participation of companies in the development and implementation of information security strategies was determined; the main tasks of IT and security services in the organization of their joint work and coordination of actions among themselves are defined; the main obstacles in the organization of joint work of IT services and security services of companies are investigated, among which significant are tensions and conflicts between employees of services, global and regional shortage of qualified personnel, technical difficulties. Conclusions: it is established that the consolidated strategy of IT management and information security based on advances in security and technology can help solve the main problems of effective interaction of relevant company services; developed a number of recommendations to address existing problems of building corporate strategies for effective IT management and information security, designed to help eliminate inconsistencies and improve the efficiency of relevant services to ensure effective information security of organizations in the EMEA in various organizations and companies, regardless of their field of activity.

Keywords: information technologies, information security, information security management, management strategies, consolidated management strategy, IT service, security service.

ПРОБЛЕМЫ ПОСТРОЕНИЯ КОНСОЛИДИРОВАННЫХ СТРАТЕГИЙ УПРАВЛЕНИЯ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В РЕГИОНЕ EMEA

Лубенец Сергей Васильевич, канд. техн. наук, доцент, кафедра международных отношений, международной информации и безопасности, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы, 6, г. Харьков, 61022, e-mail: s.lubenec@karazin.ua, ORCID: https://orcid.org/0000-0003-1061-8763
Харченко Игорь Михайлович, канд. техн. наук, доцент, кафедра международных отношений, международной информации и безопасности, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы, 6, г. Харьков, 61022, e-mail: kharchenko@karazin.ua, ORCID: https://orcid.org/0000-0002-1372-0408
Новикова Людмила Викторовна, канд. юрид. наук, доцент, кафедра международных отношений, международной информации и безопасности, Харьковский национальный университет имени В. Н. Каразина, площадь Свободы, 6, г. Харьков, 61022, e-mail: L.novikova@karazin.ua, ORCID: https://orcid.org/0000-0002-4640-2908

Рассмотрены проблемы разработки и построения универсальной консолидированной стратегии взаимодействия служб ИТ и информационной безопасности, основанной на изучении и анализе статистических данных, касающихся существующей ситуации со взаимодействием корпоративных служб ИТ и безопасности в различных международных компаниях разных отраслей и стран мира, с учетом опыта соответствующих специалистов, экспертов и аналитиков. Предметом исследования в статье является вопрос об оптимальном взаимодействии служб ИТ и безопасности в обеспечении высокого уровня корпоративной информационной безопасности в регионе EMEA. Цель состоит в анализе проблематики построения и реализации консолидированных стратегий управления ИТ и безопасности с целью устранения несогласованности и повышения эффективности работы соответствующих служб для обеспечения действенной информационной безопасности организаций на примере региона EMEA. Задачи: обработка и анализ результатов онлайн-опроса, касающегося взаимодействия служб ИТ и безопасности компаний и организаций разных отраслей в разных странах и регионах мира, в том числе в регионе EMEA; исследование проблем и преимуществ построения консолидированной стратегии управления ИТ и обеспечения информационной безопасности в регионе EMEA; разработка рекомендаций по решению существующих проблем в выработке и построении корпоративных стратегий эффективного управления ИТ и обеспечении информационной безопасности. Используется общенаучный метод системного анализа – для определения особенностей взаимодействия служб ИТ и безопасности компаний и организаций разных отраслей в разных регионах мира, а также для исследований проблем и преимуществ унифицированной консолидированной стратегии управления ИТ и обеспечения информационной безопасности. Получены следующие результаты: на основе количественной и качественной оценки, а также анализа результатов опроса специалистов и экспертов в сфере ИТ и безопасности в регионе EMEA, определено участие подразделений компаний в разработке и реализации стратегий в сфере информационной безопасности; определены основные задачи ИТ-служб и служб безопасности в организации их совместной работы и согласования действий между собой; исследованы основные препятствия в организации совместной работы ИТ-служб и служб безопасности компаний, среди которых существенны существенная напряженность и конфликты между сотрудниками служб, глобальная и региональная нехватка квалифицированных кадров, технические сложности. Выводы: установлено, что консолидированная стратегия управления ИТ и обеспечения информационной безопасности на основе достижений в области безопасности и технологий способна помочь решить основные проблемы эффективного взаимодействия соответствующих служб компаний; разработан ряд рекомендаций по решению существующих проблем построения корпоративных стратегий эффективного управления ИТ и обеспечения информационной безопасности, призванных способствовать устранению несогласованности и повышению эффективности работы соответствующих служб для обеспечения действенной информационной безопасности организаций в регионе EMEA в различных организациях и компаниях, не зависимо от сферы их деятельности.

Ключевые слова: информационные технологии, информационная безопасность, управление информационной безопасностью, стратегия управления, консолидированная стратегия управления, служба ИТ, служба безопасности.

Література

1. Шойдин Ю. ИТ и СБ. Как выстроить партнерство : веб-сайт. URL: https://www.it-world.ru/cionews/security/115731.html (дата обращения: 13.11.2021).
2. Cindy Zhiling Tu, Yufei Yuan, Norm Archer, Catherine E. Connelly. Strategic value alignment for information security management: a critical success factor analysis. *Information and Computer Security*. 2018. Vol. 26, № 2. P. 150-170.
3. Deruma S. Problems and solutions of information security management in Latvia. *SHS Web of Conferences*. 2014. Vol. 10, № 7. P. 1-7.

4. Forrester Consulting – Implement modern, effective business strategies : web site. URL: https://www.forrester.com/consulting/ (date of the application: 10.11.2021).

References

1. Shojdin J. (2015) IT i CB. Kak vystroit' partnerstvo [IT and security service. How to build a partnership]. Available at: https://www.it-world.ru/cionews/security/115731.html (accessed 13.11.2021).
2. Cindy Zhiling Tu, Yufei Yuan, Norm Archer, Catherine E. Connelly (2018) Strategic value alignment for information security management: a critical success factor analysis. *Information and Computer Security*, vol. 26, no. 2. pp. 150-170.
3. Deruma S. (2014) Problems and solutions of information security management in Latvia. *SHS Web of Conferences*, vol. 10, no. 7. pp. 1-7.
4. Forrester Consulting – Implement modern, effective business strategies. Available at: https://www.forrester.com/consulting/ (accessed 10.11.2021).

Стаття надійшла до редакції 13 листопада 2021 р.
Стаття рекомендована до друку 12 грудня 2021 р.