УДК 330.246.8

Сотниченко В.М.
кандидат педагогічних наук,
професор кафедри менеджменту
Державного університету телекомунікацій

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ТЕЛЕКОМУНІКАЦІЙНОГО ПІДПРИЄМСТВА

Стаття присвячена проблемам управління економічною безпекою телекомунікаційного підприємства. Процес управління розглядається через його методичне забезпечення. Це викликано тим, що запровадження сучасних технологій в ІТ-галузі не зменшує ризики для економічної безпеки, а, навпаки, збільшує їх. Створення організаційно-методичної бази дасть змогу оптимізувати бізнес-процеси і зменшити рівень загроз для економічної безпеки.

Ключові слова: методичне забезпечення, ІТ-технологія, бізнес-процес, віртуальна приватна мережа, ІТ-інфраструктура, управління послугами.

Сотниченко В.Н. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ ТЕЛЕКОММУНИКАЦИОННОГО ПРЕДПРИЯТИЯ

Статья посвящена проблемам управления экономической безопасностью телекоммуникационного предприятия. Процесс управления рассматривается через его методическое обеспечение. Это вызвано тем, что внедрение современных технологий в ІТ-сфере не уменьшает риски для экономической безопасности, а, наоборот, увеличивает их. Создание организационно-методической базы позволит оптимизировать бизнес-процессы и уменьшить уровень угроз для экономической безопасности.

Ключевые слова: методическое обеспечение, ІТ-технология, бизнес-процесс, виртуальная частная сеть, ІТ-инфраструктура, управление сервисом.

Sotnychenko V.N. METHODICAL SUPPORT OF MANAGING ECONOMIC SAFETY OF TELECOMMUNICATION SECURITY

The article is devoted to the problems of management by economic security of telecommunication enterprises. The management process is seen through its methodological support. This is due to the fact that the introduction of modern technologies in the IT sphere does not reduce risks for economic security, but rather enhances them. Creating organizational-methodical base enables you to optimize business processes and reduce threats to economic security.

Keywords: methodological support, it-technology, business process, virtual private networking (VPN), it infrastructure management services.

Постановка проблеми. Метод як спосіб, знаряддя, шлях до результату має завжди в класичному розумінні одну мету – отримати конкретний продукт діяльності. Результат представляється як форма, завершена і наповнена змістом. За строгого підходу до оцінки отриманого результату не можна обійтися без визначення кількісного та якісного параметрів виміру результату. Під кожний параметр підбирається відповідний прийом, спосіб або метод, який може дати саме той необхідний результат, який заплановано отримати. Тобто на початку операціоніст створює проект майбутнього необхідного результату у вигляді завершеного продукту.

Створення проекту необхідного результату починається з описування оптимальних вимог до нього, продовжується визначенням та добором методів, закінчується зведенням отриманих результатів у систему. Такою автору представляється організаційно-методична процедура створення системи управління економічною безпекою телекомунікаційного підприємства.

Аналіз останніх досліджень і публікацій. Економічна безпека як проблема на практиці і в теорії набуває актуальності зростаючими темпами практично кожного дня. Кожна нова технологія, продукт, сервіс або послуга в ІТ-галузі приносить нові ризики, які тримають економіку і суспільство у постійній напрузі. Стає очевидним, що проблеми безпеки стосуються всіх і вирішувати їх необхідно на державному рівні [1,2]. Такої позиції дотримується В.Л. Шевченко, який аналізує кращі світові практики зміцнення економічної стабільності держави шляхом оптимізації механізмів управління інформаційною безпекою. Дослідники Т.В. Альшанська, Є.А. Гур'янова, Ю.В. Королькова, розглядаючи проблеми інформаційної безпеки на підприємствах, доводять необхідність системних змін у напрямі створення ефективної системи управління економічною безпекою. Ці проблеми і шляхи їх розв–язання ілюструє також фахівець із кібербезпеки А. Янковський. Занепокоєння поглибленням проблем безпеки проявляється практично на всіх рівнях життєдіяльності людини, суспільства і держави [6; 7; 8]. Значну увагу вирішенню проблем дотримання безпеки в ІТ-галузі приділяє Міжнародний союз електрозв'язку [7], Верховна Рада України [6] та Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації [8]. Техніко-технологічне забезпечення бізнес-процесів на підприємствах телекомунікації базується на сучасних ІТ-технологія, сервісах, продуктах та мережах. Але при цьому захищеність ІТ-інфраструктур від зовнішніх та внутрішніх загроз залишається недостатньою, про що свідчать останні події у світовому кіберпросторі.

Постановка завдання. Основним завданням цієї статті є обґрунтування необхідності створення такої організаційно-методичної платформи, на основі якої буде організована продуктивна взаємодія всіх елементів бізнес-процесу.

Виклад основного матеріалу дослідження. Після кібератаки на Прикарпатобленерго значно підвищено вимоги до безпеки інформації, яка зберігається і обробляється в державних установах, силових відомствах, на підприємствах. Одним із найбільш небезпечних ризиків визнана загроза крадіжки або модифікації даних із використанням облікових записів користувачів із правами адміністратора.

Практично неможливо зберігати повну анонімність в Інтернеті, особливо коли все більша кількість пристроїв, якими ми користуємося щодня, підклю-

чається до мережі. Нашими даними зацікавлені не тільки зловмисники, а й (як показує справа «Сноудена») державні установи і компанії. Завдяки відстеженню поведінки користувачів в Інтернеті компанії заробляють, продаючи рекламодавцям інформацію про інтереси споживачів.

За даними дослідження, опублікованого компанією Microsoft в 2015 році, більшість інтернет-користувачів (у США до 77%) не знає, якого роду інформація збирається і зберігається в технологічних компаніях [7]. Простим і водночас ефективним способом обмеження ризиків відстеження є шифрування онлайн-спілкування за допомогою рішень типу VPN. Ця технологія сприяє значному зростанню рівня економічної безпеки підприємства.

VPN розшифровується як Virtual Private Network (віртуальна приватна мережа). Коли відбувається підключення до Інтернету, то на дистанції між користувачем і самим Інтернетом завжди є ймовірність втрати інформації. Таку загрозу потенційно представляє безпосередньо провайдер. Також це може бути громадська точка Wi-Fi. На цій дистанції інформація від користувача до провайдера або громадської точки доступу на шляху до Інтернету передається в незашифрованому вигляді. Це створює ризик втрати інформації як прецедент економічної небезпеки для підприємства. Підключення ж до VPN-сервера створює своєрідний тунель між комп'ютером і сервером, через який вся інформація проходить по спеціально створеному віртуальному каналу, але вже у зашифрованому вигляді. Провайдер не тільки не може розшифрувати інформацію, він навіть не може визначитися, до якого сайту звертається користувач.

Тенденція до використання програмного забезпечення VPN значно посилилася останніми роками. Сьогодні ця технологія дає змогу телекомунікаційному підприємству забезпечувати високий рівень економічної безпеки. Перевагою інструментів VPN є не тільки захист від стеження, а й можливість зміни інформації про місце розташування користувача. Відоме твердження про те, що той, хто володіє інформацією, – володіє світом, набуває все більшої актуальності. Ключовою умовою для успішного управління бізнесом є розвинена інформаційна корпоративна мережа, яка ефективно зв'язує всі підрозділи і об'єднує компанію в єдину систему.

Розглядаючи питання розроблення та застосування прийомів, методів, методик і технологій управління процесами забезпечення економічної безпеки підприємства, недостатньо лише декларувати наміри про досягнення успіхів у цьому напрямі. Треба враховувати технологічний аспект проблеми. Технології, темпи їх розвитку та сфери застосування безпосередньо впливають на зміст, форми та функціональне призначення методів управління.

Так, для компаній, що мають віддалені філії, нагальною проблемою є організація швидкого та надійного обміну інформацією, оперативного доступу до даних і впевненість у їх захищеності.

Єдине середовище, яке об'єднує інформаційні ресурси, офісну телефонну мережу і розширені функції обміну інформацією (наприклад, теле- і відеоконференції), забезпечується шляхом організації корпоративної мережі IP VPN.

Корпоративна мережа IP VPN відділена від публічних мереж. Трафік усередині мережі повністю захищений від несанкціонованого доступу і прослуховування ззовні. Інформаційні масиви, бази даних і телефонні розмови доступні тільки для внутрішніх користувачів корпоративної мережі. При цьому корпоративна телефонна мережа не має виходу в мережу загального користування.

Мережа легко конфігурується і масштабується до гігабітних швидкостей. Наявність каналу передачі даних має на увазі оперативне адміністрування мережі IP VPN. Є можливість самостійно встановлювати і регулювати пріоритетність трафіку того чи іншого бізнес-додатку.

Важливо розуміти і чітко уявляти собі, що технологія загроз розвивається і набуває, без перебільшення, планетарного масштабу. Кількість різновидів кіберзброї зростає. Кількість високо підготовлених фахівців-кіберзлочинців також зростає. І під усю цю даність треба мати величезну кількість методів на кожну комбінацію цих факторів. Тому, скоріше за все, треба дати характеристику всіх вже сьогодні відомих технологій і прийомів кібератак, а вже потім накреслити універсальні методичні рекомендації щодо захисту економічної безпеки телекомунікаційних підприємств.

Метод – це не одноактна дія, а складна процедура послідовних дій (прийомів) у межах його призначення і завдань, які належить вирішити. Так само і методика складається з кількох методів, об'єднаних єдиним завданням. Із результатів кожного методичного прийому складається результат методу загалом (див. рис. 1). Реалізація кожного прийому відбувається на основі певної технології.

Кожен метод в своїй основі має кілька технологій. Із цього логічно випливає висновок, що система управління економічною безпекою будь-якого підприємства, телекомунікаційного зокрема, не може бути побудована на основі однієї технології. Вона представляє собою складну високотехнологічну структуру.

Також важливо розуміти, що сьогодні вся наша економіка базується на єдиній телекомунікаційній платформі. Вона складається із сугубо телекомунікаційних підприємств та інформаційно-телекомунікаційних інфраструктур підприємств, орга-

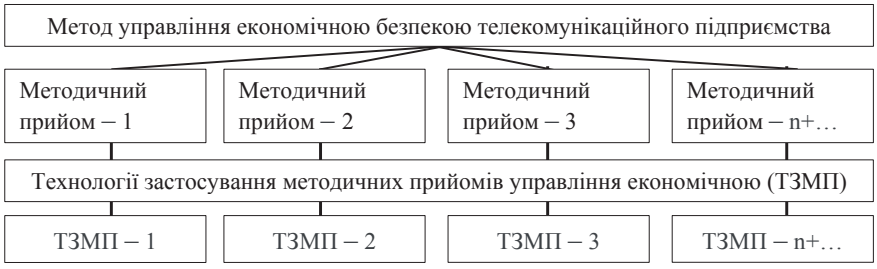

Рис. 1. Структура методу управління економічною безпекою телекомунікаційного підприємства

нізацій та установ. Кожне сучасне підприємство сьогодні не обходиться без телекомунікаційних послуг [3, с. 76–78]. Державне статистичне спостереження «Використання інформаційно-комунікаційних технологій на підприємствах України» показало, що у 2016 році 95,2% підприємств користувались комп'ютерами, з них 98% мають доступ до мережі Інтернет.

Але ця цифра має чисто фрагментарний характер, вона не дає повного уявлення про використання підприємствами інформаційно-комунікаційних технологій. Більш повною була б картина, якщо би було наведено дані про те, з якими цілями підприємства користувалися комп'ютерами й Інтернетом, до яких віртуальних джерел зверталися, які питання при цьому вирішувалися і з якими результатами, які завдання при цьому були пріоритетними.

Але з усією очевидністю можна стверджувати, що практично майже всі об'єкти інформації і послуг, цікаві для підприємств, відкриті для доступу в мережі. Крім традиційних каналів зв'язку, підприємства використовують програмно-апаратне забезпечення і телекомунікаційне обладнання та користуються сервісними послугами.

Послуги зв'язку виконують комунікаційні функції, завданням яких є отримання необхідної інформації та координація дій. Програмно-апаратне забезпечення та телекомунікаційне обладнання становлять основу інформаційно-телекомунікаційної структури підприємства. Сервісні послуги – установка обладнання, інсталяція та обслуговування програмного забезпечення, регламентні роботи – забезпечують коректне, безпечне та ефективне функціонування інформаційно-телекомунікаційної інфраструктури підприємства.

Цікавим для науково-практичної перспективи є IT-інфраструктура підприємства. Жодне підприємство не може обійтися без неї.

IT-інфраструктура підприємства – це свого роду конструкція, без якої компанія не зробить і кроку [4, с. 97–99]. Від того, наскільки ефективно будуть збудовані процеси всередині компанії і зовнішня комунікація з клієнтами та постачальниками, залежить успішність бізнесу.

В епоху глобалізації бізнес постійно піддається впливам ззовні. Інформаційно-телекомунікаційні технології, проекти і системи стають все більш складними, при цьому час на їх реалізацію скорочується. Прикладом є масштабні хакерські атаки на персональні комп'ютери державних і приватних підприємств України 27 червня 2017 року. За повідомленням Укрінформу постраждало близько 30 банківських установ. При цьому ступінь пошкоджень різний. Крім банків, постраждали підприємства торгівлі, транспорту, повністю припинив працювати сайт Кабінету Міністрів України. Ще й сьогодні немає точної інформації про спричинені збитки і втрати. Але навіть приблизні дані вражають, особливо порівняно з даними про втрати інших країн, на які також було здійснено хакерські атаки. Очевидним є одне – Україна має найбільші втрати від хакерських атак: постраждали майже всі сфери економіки, в тому числі і держсектор, транспорт, сільське господарство, металургія, засоби масової інформації, банки, торговельні підприємства.

Якщо взяти за 100% всі збитки, яких зазнали всі країни, що постраждали від хакерських атак, то частка України становила 75,24%, Німеччини – 9,06%, Польщі – 5,81%; Сербії – 2,87%, Греції – 1,39%, Румунії – 1,02%, Росії – 0,82%, Чеської республіки – 0,82% і решти світу – 2,97% (за даними ESET – міжнародного розробника антивірусного програмного забезпечення та рішень в галузі комп'ютерної безпеки для корпоративних та домашніх користувачів – http://internetua.com/ekspertinacsinauat-podscsitivat-poteri-ot-virusa).

Збитки, яких зазнав бізнес від вірусу, – це прибуток, який компанії не отримали. І причиною цього є те, що IT-інфраструктури підприємств України належним чином не захищені, а через те стан економічної безпеки підприємств виявився на відносно низькому рівні. Це є ризиком системного характеру, який негативно впливає на інвестиційну привабливість України.

Оптимальним напрямом вирішення проблем із захищеністю вітчизняного бізнесу повинна стати робота з організації резервування і зберігання даних та радикальний перегляд порядку і правил роботи в локальних мережах, розміщення в них конфіденційної інформації. Крім того, гостро небезпечним є питання користування програмно-апаратним забезпеченням, особливо імпортного виробництва [5; 6, с. 33–35; 8].

Тобто система захисту та збереження конфіденційної інформації виявилася не готовою протистояти зовнішнім загрозам як на професійному, так і на техніко-технологічному рівнях. Для оптимізації багатьох процесів існують відповідні IT-рішення, проте більшість із них підвищує вимоги до фахівців IT-служби. Такий підхід не тільки покращує якість сервісів, а і знижує витрати.

З метою вирішення питання управління IT-послугами у 2005 році було розроблено міжнародний стандарт для управління та обслуговування IT-сервісів ISO 20000. І з того часу він постійно вдосконалюється. Стандарт представляє собою докладний опис вимог до системи управління IT-сервісами. Таке управління передбачає сервісний підхід до роботи IT-служби, коли фахівці IT-департаменту надають іншим відділам компанії послуги відповідно до угоди про рівень послуг..

Принципово система управління IT-послугами (Information Technology Service Management, скорочено ITSM) схематично представлена на рисунку 2. Модуль оперативного контролю та звітності виконує сигнальні функції, сповіщає систему про появу та характер загроз. Модуль управління послугами готує організаційно-технічне рішення і проект вирішення питання щодо захисту економічної безпеки підприємства. У структурі цього модуля є база алгоритмів типових рішень, яка постійно оновлюється. І вже на рівні базових функціональних модулів і на основі розроблених рекомендацій реалізується підготовлений проект. Вся система управління IT-послугами базується на єдиній техніко-технологічній платформі, що забезпечує узгоджену взаємодію всіх її модулів.

Всі процесі і процедури в межах цієї системи управління описані в спеціально підготовленій бібліотеці (IT Infrastructure Library, скорочено ITIL), яка також постійно оновлюється і коригується. ITIL описує такі процеси, як управління проблемами й інцидентами; управління конфігураціями; управління змінами; управління релізами; управління рівнем сервісу; управління фінансами; управління потужністю; управління безперервністю; управління доступністю.

У бібліотеці ITIL зберігається набір документів, які використовуються для практичного впровадження принципів ITSM. Ідея бібліотеки ITIL з'явилася ще

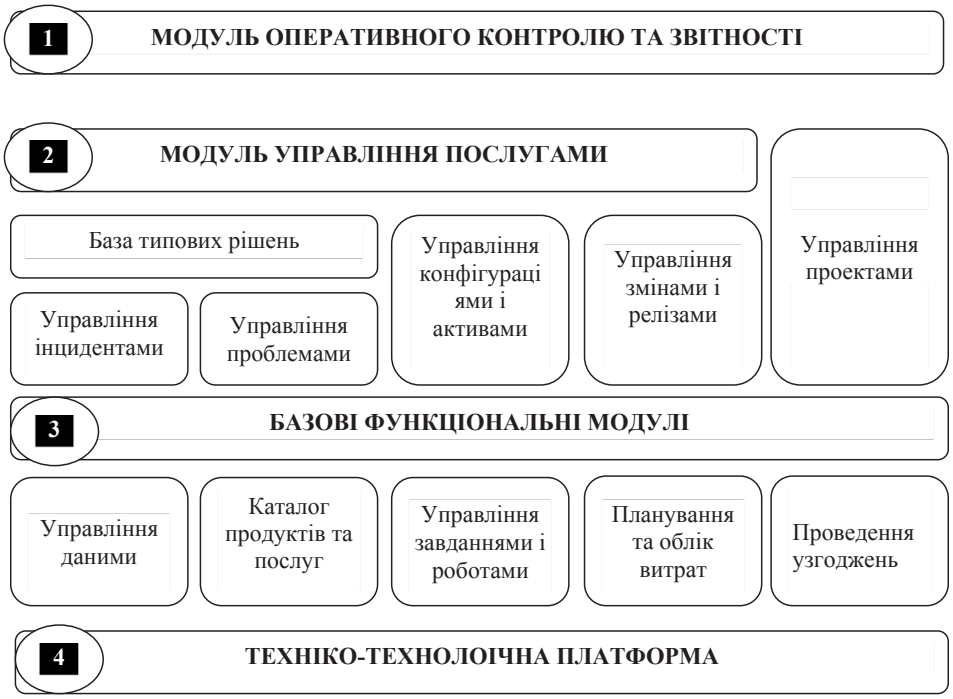

Рис. 2. Принципова схема системи управління IT-послугами (ITSM)

в 1980 році з ініціативи британського уряду. Робота над нею велася з 1986 по 1989 рік. Перша редакція була випущена у 1992 році. На основі ITIL був розроблений міжнародний стандарт ISO 20000 для управління та обслуговування IT-сервісів.

Для більш повного розуміння сутності окремих процесів в рамках ITSM варто коротко зупинитися на кожному з них.

Інциденти – будь-які ситуації, які вимагають реакції. Це можуть бути запити від користувачів, збої в системі. Для найбільш успішної реалізації цього процесу, завдання якого – виявити й усунути проблеми всередині компанії, мінімізувати ризик їх виникнення, організовується спеціальна служба підтримки – Service Desk.

Управління конфігураціями і змінами допомагає отримати достовірну та актуальну інформацію про IT-інфраструктуру та не допустити небажаних змін. Завданням управління рівнем сервісу є виявлення його оптимального рівня, недопущення падіння якості послуг, усунення неякісних послуг та решта процесів, таких як управління фінансовими бізнес-процесами, встановлення оптимальної потужності для реалізації завдань системи. Крім того, система забезпечує безперервність процесів, незважаючи на форс-мажорні обставини.

Відповідно до стандарту ISO / IEC 20000 «Інформаційна технологія. Менеджмент послуг» всі процеси зібрані в п'ять ключових груп, таких як надання сервісів (управління рівнем сервісу, управління доступністю і безперервністю, управління потужністю, а також управління інформаційною безпекою, бюджет і облік витрат); управління взаємодією (взаємодія з бізнесом, з постачальниками тощо); дозвільні процеси (управління проблемами і інцидентами); контроль (управління змінами та конфігураціями); управління релізами.

Упровадження ITSM-рішення можна розбити на кілька напрямків, таких як аудит системи управління та планування (обстеження IT-процесів, структури підприємства та IT-інфраструктури); визначення цільової моделі; оперативне усунення інцидентів і вирішення запитів користувачів (як внутрішніх, так і зовнішніх); моніторинг IT-інфраструктури (забезпечення контролю над змінами); управління процесами планування, розгортання та надання IT-послуг.

ITSM-проект завжди починається з аудиту. На цьому етапі відбувається аналіз усіх процесів і виявляється їх стан, виконується обстеження IT-інфраструктури. Проводиться аналіз продуктивності всіх підсистем, виявлення «вузьких місць» у бізнес-процесах, інвентаризація програмного забезпечення та ін. Під час аудиту всі IT-процеси оцінюються також і з позиції відповідності потребам організації. Для кожного процесу визначається поточний і цільовий рівень зрілості. На підставі цих висновків і опрацьовуються подальші поліпшення.

Розробляється індивідуальна концепція розвитку управління IT, описуються вимоги, яким кожен процес повинен відповідати в майбутньому. Це досить трудомістка процедура, проте вона дає змогу створити цілісну систему управління IT, яка зможе врахувати і нові можливості, і стратегію бізнесу.

Прогнозування результатів роботи дає змогу оптимізувати процеси управління. Концепція розвитку враховує не тільки процеси і технології, а й персонал, який буде брати участь у роботі. План щодо поліпшення послуг допомагає оцінити витрати і прийняти рішення про стратегію розвитку IT-служби.

Служба підтримки клієнтів компанії і внутрішніх користувачів допомагає домогтися чіткої регламентації процесу підтримки; автоматичної обробки всіх звернень; оцінки задоволеності користувачів.

Контроль над змінами в інфраструктурі – ще одне важливе завдання. Для цього проводиться інвентаризація програмно-апаратних засобів і забезпечується автоматизована підтримка актуальної інформації про інфраструктуру. Завдяки моніторингу відбувається оперативне виявлення збоїв, а процес внесення змін в інфраструктуру регламентований. Ще один

плюс – підготовка звітів про роботу відбувається автоматично.

Таким чином, керівництво підприємства постійно отримує інформацію, необхідну для поліпшення роботи та вдосконалення послуг. Управління процесами планування, розгортання і надання IT-послуг дає змогу створити надійний фундамент, розвивати взаємовигідні відносини із клієнтами, підтримувати високий рівень послуг.

Висновки. У роботі телекомунікаційних підприємств із забезпечення економічної безпеки використовуються сучасні IT-технології, сервіси і продукти, але при цьому залишаються недостатньо захищеними мережі. Однією із причин цього є організаційно-технічна та організаційно-економічна неузгодженість між собою IT-технологій, IT-послуг та IT-сервісів, що обслуговують бізнес-процеси. Виявляється недостатньо розробленою та організованою методична основа управління безпекою. Вирішення проблеми економічної безпеки підприємства буде більш ефективним і результативним, якщо взаємодія всіх елементів бізнес-процесів буде побудована на єдиній організаційно-методичній платформі.

Необхідно створити матрицю методичного забезпечення взаємодії технологій, послуг,сервісів, систем та мереж. Структурно така матриця має бути побудована за цілями, завданнями, формами організації взаємодії між елементами бізнес-процесу й орієнтована в часі і просторі. А предметом посиленої уваги вчених-дослідників і практиків повинні бути точки взаємодії всіх задіяних у процесі елементів.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Economics and National Security: Issues and Implications for U.S. Policy. URL: http://www.fas.org/sgp/crs/natsec/R41589.pdf
2. Hudson, W. Economic Security for All: How To End Poverty In The United States. URL: http://shults.org/wadehudson/esfa/
3. Шевченко В.Л. Кращі світові практики управління інформаційною безпекою та їх вплив на економічну стабільність держави / Шевченко В.Л. // Матеріали міжнародної науково-практичної конференції «Сучасні інформаційно-телекомунікаційні технології» (17–20 листопада 2015 р.). – К.: – ДУТ.– 2015. – т. 5. – С. 76–78.
4. Альшанская Т.В. Проблемы информационной безопасности на предприятиях / Т.В. Альшанская, Е.А. Гурьянова, Ю.В. Королькова / Развитие науки и образования в соврем. мире : сб. тр. Междунар. науч.-практ. конф. – Люберцы: АР-Консалт, 2014. – Ч. 3. – С. 97–99.
5. Янковский А. Проблемы в сфере кибербезопасности в Украине. [Електронный ресурс] // Украинская правда. – Режим доступа: http://www.pravda.com.ua/rus/columns/2017/02/15/7135442/
6. Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України: матеріали парламентських слухань у Верховній Раді України 3 лютого 2016 р. / Верховна Рада України, Комітет з питань інформатизації та звязку; ред. кол.: О.І. Данченко (голова), Г.О. Андрощук, О.Г. Старинець, О.А. Баранов [та ін.]. – К.: Парлам.вид-во, 2016. – 256 с.
7. Измерение информационного общества. Резюме // Международный союз электросвязи [Электронный ресурс]. – 2016. – Режим доступа: http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2014-SUM-PDF-R.pdf
8. Річний звіт про роботу Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації за 2016 рік.