ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

СТРАТЕГІЇ КІБЕРСТІЙКОСТІ: УПРАВЛІННЯ РИЗИКАМИ ТА БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ

Матеріали Всеукраїнської науково-практичної Інтернет-конференції

25 лютого 2021 року

КИЇВ

Рекомендовано до друку Вченою радою Навчально-наукового інституту захисту інформації Державного університету телекомунікацій

(протокол № 8 від 08.02.2021 р.)

Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: Матеріали Всеукраїнської науково-практичної Інтернет-конференції (м. Київ, 25 лютого 2021 року). Навчально-науковий інститут захисту інформації, Державний університет телекомунікацій. Київ, 2021. 113 с.

Збірник призначений для науковців, викладачів, докторантів, аспірантів і студентів закладів вищої освіти, фахівців з інформаційної та кібернетичної безпеки, працівників органів державної влади та місцевого самоврядування.

ЗМІСТ

СЕКЦІЯ 1. СУЧАСНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

СЕКЦІЯ 2. НОВІТНІ ТРЕНДИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ

СЕКЦІЯ 3. ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА

СЕКЦІЯ 7. ОСВІТА Й ОБІЗНАНІСТЬ, ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ

СЕКЦІЯ 8. ЗАКОНОДАВЧА Й НОРМАТИВНА ОСНОВА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

СЕКЦІЯ 1. СУЧАСНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ІТ-ТЕХНОЛОГІЙ У БІЗНЕС УКРАЇНИ

Воскобоєва О.В., к.е.н., доц., Ромащенко О.С., к.е.н.
Державний університет телекомунікацій
м. Київ, Україна

З кожним роком розвиток ІТ-технологій стає все стрімкіше і без технологій не обходиться вже не одна сфера діяльності. Особливо гостро інноваційних розробок потребує бізнес, оскільки йому складніше усього виживати, особливо в умовах кризи. Бізнес відіграє важливу роль в господарстві країни, оскільки підприємства сприяють розширенню сфери додатка праці, створенню можливості для реалізації підприємницької діяльності населення, додатку творчих сил. Бізнес допомагає зменшити соціальну напруженість і забезпечує ресурсозберігаюче економічне зростання. Бізнес є двигуном економіки, деяким драйвером, який життєво потрібний сучасній економіці. Достоїнства бізнесу значною мірою обумовлені можливостями його росту.

Ще зовсім нещодавно інформаційні ресурси і ІТ-технології не були такими значимими для розвитку бізнесу. Для ефективного управління було досить особистої участі керівника підприємства. Не було потрібне розгалужена мережа менеджерів і системне дослідження даних. Найбільш важливі рішення приймалися керівниками компаній виходячи з досвіду і інтуїції. Аналіз інформаційних даних про діяльність підприємства не грав вирішальної ролі. Тільки великі компанії вводили в штат центри аналітики, що готували узагальнені дані для ухвалення рішень. Швидкий розвиток, поліпшення якості, підвищення надійності обчислювальної техніки привели до того, що роль інформаційних технологій у бізнесі різко зросла [1, с. 1].

Сучасні фахівці в області маркетингу, бізнес-стратегій і в області інформаційних технологій згодні з тим, що основною тенденцією, на цьому етапі, вважається зміна ролі комп'ютерних технологій, оскільки автоматизації функціональних процесів вже стає мало і існує необхідність в тому, щоб розмилися межі між бізнес-процесами і інформаційними процесами та розробці програмного забезпечення і перспектив розвитку галузі інформаційних технологій на ринку [2, с. 2]. Відповідно до цього, представники малого і середнього бізнесу дуже зацікавлені не лише в нових інформаційних технологіях, але і в ІТ-фахівцях нового покоління, оскільки в їх обов'язки тепер входить пояснення результатів впровадження певної технології (зміна термінів випуску, фінансові наслідки від певних дій, вартість впровадження і можливі ризики). Згідно з даними аутсорсингової ІТ -компанії N - іХ, останнє десятиліття українська ІТ -сфера демонструє стабільний ріст. Політична криза в 2014 році спровокувала короткочасний спад із-за відтоку кадрів за кордон. Але інфляція, що послідувала за цим, і падіння цін стимулювали інтерес іноземних інвесторів до українських ІТ-послуг. Це стало початком нової активної фази розвитку ІТ -сфери.

Стрімкий розвиток інформаційних технологій породив бізнес нового типу - електронний. Перед ним стоять такі завдання: забезпечення інтеграції окремих компонентів інформаційних систем на підприємстві та взаємодія інформаційних систем різних підприємств.

Якщо порівнювати впровадження інформаційних технологій в малий і середній бізнес в Україні і в країнах Європи, то треба відмітити що Україна доки програє в цьому питанні. Так, до недавнього часу, керівники більшості малих і середніх підприємств в нашій країні були переконані в складності, недоступності і дорожнечі впровадження інформаційних технологій. При цьому, в країнах Європи впровадження інформаційних технологій в середній і малий бізнес складає 80-90 %. Проте, нині більшість керівників в нашій країні впевнені в необхідності ІТ-технологій із створення підприємства і в процесі

його розвитку. При цьому, хотілося б зазначити, що малий і середній бізнес не припускає спільного розвитку з інформаційними технологіями, а представники галузі інформаційних технологій не можуть донести до бізнесу, чим це може бути вигідно

Одна з гілок застосування інформаційних технологій у бізнесі- сучасний безперебійний зв'язок у будь-якій географічній точці світу. Можливість тримати ситуацію під контролем і оперативно вирішувати ключові управлінські питання - дуже цінна якість для будь-якого керівника.

Виходячи з вивченого матеріалу, можна сказати, що керівництво компаній малого і середнього бізнесу повинне відповісти на такі питання як:

1. У рішенні яких управлінських завдань доцільно використати інформаційні технології?

2. Які цілі і очікувані результати від впровадження інформаційних технологій в компанії?

У великих компаніях існують спеціальні відділи, які можуть допомогти відповісти на ці питання. У малому бізнесі, як правило, завдання і зараз лягає на плечі керівництва [3, с. 3].

Підводячи підсумок, можна сказати, що залежно від вибору моделі стосунків з інформаційно-технологічними структурами, а також способів підтримки таких стосунків безпосередньо залежатимуть як успішність і адекватність IT-підтримки сучасного бізнесу в недалекому майбутньому, так і якість роботи, і, швидкість функціонування підприємства в цілому. А перешкод цьому в Україні немає, оскільки за даними GlobalLogic, з 2015 по 2020 рік кількість IT-фахівців в країні подвоїлася з 90 000 до 180 000. За неофіційною статистикою, ця цифра перевищила 200 000. Україна займає 11 місце в ТОП 50 країн з кращими розробниками програмного забезпечення у світі, за даними HackerRank, і 6 місце в рейтингу кращих програмістів TopCoder.

Література

1. Сучасні інформаційно-комунікаційні технології для успішного ведення бізнесу URL: http://cyberleninka.ru/article/n/sovremennye-informatsionno-kommunikatsionnye-tehnologii-dlya-uspeshnogo-vedeniya-biznesa-uchebnoe-posobie

2. Скворцова Н. А., Лебедева О. А., Сотникова Е. А. Влияние информационных технологий на развитие бизнеса. *Теоретическая и прикладная экономика*. 2018. № 1. с. 42-50. URL: https://nbpublish.com/library_read_article.php?id=25189

3. Зміна ролі IT у бізнесі URL: http://dce.ifmo.ru/media/files/UMK/posob-upr-it-predp.pdf

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ В СИСТЕМАХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Долинський О.І.
Державний університет телекомунікацій
м. Київ, Україна

Розвиток безготівкових розрахунків, розширення сфери платіжної інфраструктури та оптимізація готівкового обороту не можливе без високого рівня надійності проведення міжбанківських переказів у національній валюті, обсяг яких зростатиме пропорційно до збільшення частки безготівкових розрахунків, що в результаті формує актуальність щодо забезпечення безпеки інформаційних ресурсів в системах електронних платежів.

Електронні перекази - це грошові операції, що відбуваються в електронному вигляді між споживачами та роздрібними продавцями. Мільйони користувачів по всьому світу регулярно здійснюють різні платежі через Інтернет. Ці обмінні операції є своєрідним

електронним грошовим інструментом. Згідно зі звітом Statista Fintech, у 2019 році загальний обсяг транзакцій у сегменті цифрових платежів оцінювався в 3670864 мільйони євро, а до 2023 року, за оцінками, він збільшиться до 5921831 мільйонів євро [1].

Електронна платіжна система - це спосіб оплати через електронну мережу, де фізична особа може оплачувати товари та послуги через Інтернет. Існує досить багато систем електронних платежів, які були створені у платіжному секторі по всьому світу, а також у посиланнях, автори класифікували електронні платіжні системи на різні категорії, а саме електронну готівку, електронний гаманець, онлайн-оплату, на основі карток тощо [1].

Властивості безпеки електронних платежів

Захист здійснення електронних платежів є перманентною проблемою, оскільки є певні ризики втрати персональних даних та грошових коштів під час здійснення електронних грошових операцій. Користувачі вимагають конфіденційності, автентифікації, цілісності даних, як основних вимог для здійснення безпечних розрахунків через Інтернет, або відмови від незахищених операцій. Системи електронних платежів повинні мати усі вищезазначені атрибути захисту, оскільки користувачі відмовлятиметься від системи електронних платежів, яка не захищена. Окрім цього, довіра є надзвичайно важливою, щоб гарантувати схвалення клієнтів [1].

Властивості захисту електронних платежів, адаптовані за [1], представлено на рис. 1.

Необхідні кроки для забезпечення безпеки електронних платежів

1. Відповідність PCI

Один із перших кроків - це переконатися, що ваша платіжна система відповідає галузі платіжних карток (Payment Card Industry Data Security Standard PCI DSS). Рада зі стандартів безпеки платіжних карток була створена в 2006 році для регулювання основних платіжних брендів та надання допомоги торговцям у збереженні фінансових даних своїх клієнтів. Їхня прерогатива - максимізувати інформаційну безпеку, реалізуючи 12 вимог безпеки [2].

Незалежно від того, великий чи малий ваш бізнес, це важливо, оскільки надає гарантії, що ви відповідаєте принаймні мінімальним вимогам безпеки для обробки транзакцій клієнтів. Рада PCI співпрацює з продавцями, щоб надати освіту про безпеку в Інтернеті, і вживатиме необхідних заходів для максимізації безпеки вашого веб-сайту. Конкретні вимоги, яким потрібно відповідати, залежать від багатьох факторів, включаючи розмір вашого бізнесу. Їхня робота - проаналізувати вашу систему транзакцій в Інтернеті, перевірити наявність вразливостей та виправити їх. Команда з дотримання вимог створює звіти та надсилає їх брендам карток та банкам, з якими пов’язаний ваш бізнес [2].

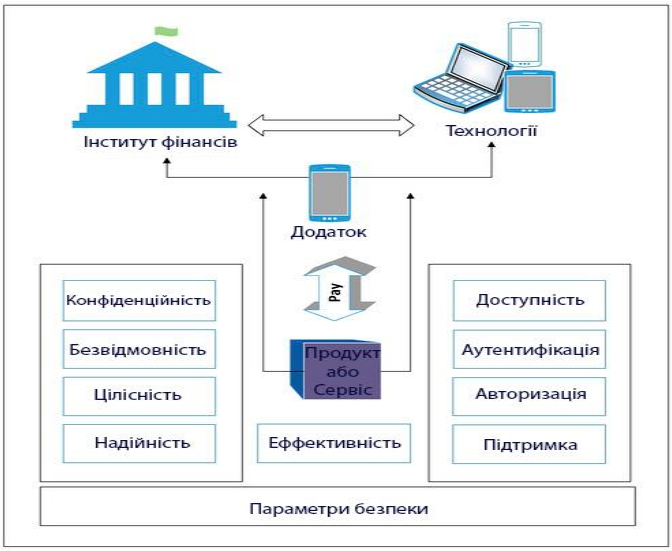


Рис. 1. Властивості безпеки електронних платежів

2. Шифрування даних

Іншим способом підвищення безпеки є використання технології шифрування, щоб приватна фінансова інформація залишалась приватною. Ця технологія підтверджує, що веб-сайти, які ваш бізнес використовує для транзакцій, є частиною діючих організацій та мають законних операторів, що мінімізує ризик втрати конфіденційної інформації. Це також значно зменшує шанси хакерів зламати паролі. Поєднання цих функцій створює додатковий рівень захисту для клієнтів протягом усього процесу транзакції. Шифрування даних є як ніколи важливим, особливо при використанні мереж Wi-Fi та відповідно проблемами викрадення особистих даних [2].

3. Екран безпечного входу

Коли клієнти входять, щоб отримати доступ до своїх облікових записів, важливо, щоб система входу була максимально безпечною. Ви відображаєте сайт HTTPS в адресному рядку? Якщо ні, то хакерам можна небезпечно проникнути та отримати доступ до конфіденційної інформації. У випадку, якщо клієнт забуде свій пароль, він повинен буде ввести ім'я користувача або адресу електронної пошти для його отримання. Потім система надішле йому електронний лист, де він зможе тимчасово увійти в систему або створити новий пароль. Дотримання цього типу протоколу безпеки є відносно простим, але може запобігти багатьом загрозам безпеки [2].

4. Оновлені операційні системи

Також розумно залишатися в курсі всіх оновлень безпеки, доступних для комп'ютерної мережі вашої компанії. Оскільки хакери постійно продукують нові методи, дуже важливо бути на крок попереду. Якщо ви цього ще не зробили, вам слід підписатись на автоматичне оновлення для всієї вашої мережі . Це не дозволить вам забути завантажити будь-які важливі запобіжні заходи, які можуть поставити під загрозу вашу безпеку онлайн-платежів. Окрім захисту транзакцій, це повинно значно зменшити шанси на зараження вірусом, який може негативно вплинути на здійснення грошових операцій [2].

5. Оцінка безпеки

Отже, ретельну оцінку вашої платіжної системи може здійснити компанія Security Metrics. Ця компанія за функціями схожа PCI, але дещо інша у своєму підході до проведення аналізу роботи систем. Однією з функцій, яку вони пропонують, є впровадження етичного злому, коли аналітики тесту на проникнення перевіряють вашу мережу так само, як і хакери. Вони роблять це вручну і шукають вади, які потенційно можуть бути використані. Згодом вони переглянуть свої висновки та проведуть консультації для підвищення безпеки. Додаткові функції включають виявлення місця витоку незашифрованих даних, конфігурацію мережі, захист бездротової мережі та захист зовнішньої / внутрішньої мережі. Якщо ви хочете дізнатись більше про техніку безпеки, вони можуть навіть забезпечити вам навчання з питань безпеки [2].

Отже, завдяки якісно побудованій системі захисту інформаційних ресурсів в системах електронних платежів можна значно зменшити кількість випадків витоку конфіденційної інформації про банки та їх клієнтів третіми особами, що в свою чергу дозволить мінімізувати фінансові та репутаційні втрати компанії.

Література

1. A Review on Electronic Payments Security. URL:: https://www.mdpi.com/2073-8994/12/8/1344/htm

2. Learn about The Payment Card Industry Data Security Standard requirements and the independent body, PCI Security Standards Council, that manages and enforces the PCI DSS. URL:: https://digitalguardian.com/blog/what-pci-compliance

ОСОБЛИВОСТІ ФІНАНСОВОГО, УПРАВЛІНСЬКОГО І ВИРОБНИЧОГО ОБЛІКУ В УПРАВЛІННІ ВИТРАТАМИ ПІДПРИЄМСТВА

Голобородько А.Ю., к.е.н.
Державний університет телекомунікацій
м. Київ, Україна

Фінансовий облік охоплює інформацію, яка використовується не лише для внутрішнього управління, але і повідомляється контрагентам. Ця інформація повинна задовольняти потребам як фіскальних державних органів, так і акціонерів компаній, утримувачів облігацій і інших цінних паперів, потенційних інвесторів. Норми і правила його ведення регулюються національними стандартами.

Для усебічного і повного розуміння суті управлінського обліку неможливо обійти увагою питання про взаємодію і співвідношення фінансового, управлінського і виробничого обліку.

Між управлінським і фінансовим обліком багато спільного, так і обоє вони використовують інформацію облікової системи підприємства. Одним з розділів цієї системи є облік витрат і доходів, необхідних як у фінансовому, так і в управлінському обліку.

Загальноприйняті принципи фінансового обліку можуть діяти також і в управлінському обліку, оскільки керівники підприємств у своїй діяльності не можуть керуватися оцінками, що виключно не перевіряють, суб'єктивними, і думками. Крім того, інформація обох підсистем використовується для ухвалення необхідних управлінських рішень.

Питання організації як фінансового, так і управлінського обліку на підприємствах придбавають особливу актуальність нині у зв'язку з переходом на міжнародні стандарти. Від чіткості представлення суті цих підсистем, їх цілей, функцій і завдань багато в чому залежить успіх економічної роботи підприємства.

Бухгалтерський облік разом з оперативним, статистичним і податковим входить в загальну систему підприємства і підрозділяється на дві частини:

1. Фінансовий;
2. Виробничий, об'єктом якого виступають витрати і доходи організації.

Такий підрозділ бухгалтерського обліку можна пояснити тим, що в принципі уся система бухгалтерського обліку є складовою частиною управлінської системи організації. Проте при використанні термінів “фінансовий облік” і “виробничий облік” основний упор робиться на облікові процедури. Управлінський же облік не обмежується тільки обліковими процедурами, а за рахунок інших функцій управління, по суті, перетворює виробничий облік на управлінський. Його дані містять комерційну таємницю, і на відміну від фінансового обліку використовуються виключно усередині організації.

Управлінський і виробничий облік ототожнювати не можна. Виробничий облік включає, в основному, обліково-розрахункові процедури, головною метою яких є визначення витрат на виробництво виручки на одиницю продукції.

Управлінський облік іноді називають внутрішнім обліком, який включає виробничий облік. Виробничий облік припускає систему збору, реєстрації, узагальнення і обробки систематизованої інформації про витрати на виробництво, контроль за їх станом і калькуляцію собівартості продукції. Формування показників виробничо-господарської діяльності підприємства в системі управлінського обліку є таємницею підприємства, секретом фірми.

Виробничий облік покликаний стежити за витратами виробництва і доходами підприємства і виявляти можливі резерви підвищення рентабельності виробничої діяльності. Він повинен чітко і детально відбивати усі процеси, пов'язані з виробництвом і реалізацією продукції на підприємстві.

Сучасний виробничий облік включає три основні розділи:

1. Облік витрат і доходів за їх видами.
2. Облік витрат і доходів за центрами відповідальності.
3. Облік витрат і доходів за їх носіями.

Облік витрат і доходів по центрах відповідальності повинен сприяти точному їх розподілу між окремими підрозділами підприємства для визначення результатів в розрізі кожного центру відповідальності.

Таким чином, тільки у рамках виробничого обліку вдається розрахувати собівартість і рентабельність одиниці продукції і виявити приховані резерви підвищення ефективності виробничої діяльності підприємства.

Управлінський облік по своєму складу, безумовно, ширше, ніж виробничий. Управлінський облік включає аналіз, прогнозування, планування, прийняття управлінських рішень, організація, облік і контроль, регулювання та стимулювання діяльності підприємства.

Предметом управлінського обліку є виробнича і комерційна діяльність організації в цілому і її окремих структур підрозділів в процесі усього циклу управління.

Господарські операції, що носять виключно фінансовий характер (операції з цінними паперами, орендні і лізингові), виходять за рамки предмета управлінського обліку.

Таким чином, управлінський облік можна визначити як інтегровану систему внутрішньогосподарського обліку, яка надає інформацію про витрати і результати діяльності як усієї організації, так і її окремих структурних підрозділів, призначену для ухвалення тактичних (оперативних) і стратегічних (прогнозних) управлінських рішень.

Література

1. Подолянчук О. А. Облік в системі управління витратами. *Електронне наукове фахове видання Ефективна економіка. 2018. Вип. 7. С.* URL: http://www.economy.nayka.com.ua/pdf/7_2018/47.pdf
2. Сахно Л. А. Еволюція управлінського обліку: від обліку витрат виробництва до стратегічного управління *Облік і фінанси АПК: бухгалтерський портал*. URL: http://magazine.faaf.org.ua/evolyuciya-upravlinskogo-obliku-vid-obliku-vitrat-virobnictva-do-strategichnogo-upravlinnya.html

СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ІТ – ГАЛУЗІ УКРАЇНИ

Сукурова Н.М., к.е.н., доц.
Державний університет телекомунікацій
м. Київ, Україна

За відносно короткий проміжок часу сфера інформаційних технологій зі звичайної, дещо другорядної галузі, перетворилась на один з головних драйверів світової економіки, ставши каталізатором для тектонічних змін і трансформацій у багатьох інших індустріях.

Для України ІТ-галузь має особливо важливе значення, адже в умовах загальної економічної та політичної кризи, вона здатна згладити ці явища за допомогою стрімкого розвитку, а також забезпечення функціонування багатьох суміжних галузей. Головні переваги ІТ-галузі полягають у тому, що для збільшення обсягів виробництва не потрібні значні інвестиції в основні засоби, оскільки головний актив тут – людський фактор, а також грамотно побудована стратегія підприємств технологічної галузі. Проте, на сьогоднішній день на розвиток ІТ галузі в Україні впливає чимало факторів, які його стримують.

Так, за індексом розвитку інформаційно-телекомунікаційних технологій (ІКТ) - The ICT Development Index що застосовується Міжнародним союзом електрозв'язку (ITU) для

виміру рівня й еволюції в часі змін у сфері ІКТ і порівняльного аналізу ситуації в різних регіонах і країнах, у 2019 році Україна посіла 77 місце із значенням 5,33 (табл. 1).

Таблиця 1

Позиції України та інших країн світу за індексом розвитку ІКТ (The ICT Development Index 2019, (IDI))

Місце	**Країна**	**Значення**
1	Південна Корея	8,84
2	Ісландія	8,83
3	Данія	8,74
4	Швейцарія	8,68
5	Великобританія	8,57
6	Гонконг	8,46
7	Швеція	8,45
8	Нідерланди	8,43
9	Норвегія	8,42
10	Японія	8,37
…		
76	Бруней	5,33
77	**Україна**	**5,33**
78	Венесуела	5,27

Джерело: [4].

Такий стан речей характеризує Україну як технологічно відсталу країну і свідчить про недостатню доступність та поширеність використання ІКТ, а також недостатність практичних навичок користування ІКТ населенням України.

Основними проблемами, які стримують розвиток ІТ-галузі в Україні та причинами досить низьких позицій у міжнародних рейтингах є:

- Несприятливий бізнес-клімат. Основна проблема ІТ-спеціалістів нашої країни полягає в тому, що більшість із них працює в тіні. Найбільша перепона - поганий економічний клімат, що визначається рівнем простоти ведення бізнесу, недосконаліть законодавчої бази, яка б підтримувала розвиток ІТ галузі.
- Применшення важливості галузі ІТ. Державні установи та підприємці все ще ігнорують можливість запровадження будь-яких інноваційних нововведень, що передбачають роботу із технікою.
- Відсутність якісної профільної освіти. Українські ВНЗ все ще працюють за застарілою програмою викладання, а сучасний ринок праці потребує спеціалістів, що розуміються на нових трендах. Для того, аби наздогнати інших, українську систему вищої освіти потрібно реформувати та покращувати до міжнародних стандартів.
- Нестача кваліфікованих кадрів. Якої б популярності не набула ця сфера, а спеціалістів із ІТ-технологій все ще не вистачає. Головною причиною цьому є система освіти, яка, на жаль, не може підготувати такої кількості кадрів, що відповідала би попиту. Також багато хто працює на іноземний ринок, а певна кількість айті-спеціалістів мігрувала.
- Проблема захисту прав індивідуальної власності. У 2017 році Україна все ще займала 4 місце у топ-10 країн за використанням піратських сайтів. Уряд намагається впровадити певні заходи, але поки українці все ще шукають альтернативні шляхи, аби не платити за контент та програм незабезпечення. Лише тоді, коли Україна вирішить проблему із захистом прав інтелектуальної власності, будуть отримуватися та зростати інвестиції в

інтелектуальномісткі сфери. Українські ІТ-спеціалісти, працюючи над своїми новими проектами, повинні бути впевненими у своїх правах на авторство [1; 2].

Тому, для розвитку ІТ- галузі в Україні, необхідно провести ряд заходів, зокрема:

- створити прозорі та стабільні правила ведення бізнесу;
- гарантувати безпеку бізнесу;
- сприяти розвитку внутрішнього ринку, зокрема продуктових компаній;
- забезпечити якісну підготовку професійних кадрів для ІТ-галузі;
- сформувати позитивний ІТ-імідж України;
- створити адекватну та здорову фіскальну систему тощо.

Важливим глобальним чинником, який впливає на розвиток ІТ в Україні, є підписання Угоди про Асоціацію з ЄС. У межах цієї угоди необхідно забезпечити реалізацію низки кроків, які стосуються ІТ-сфери, зокрема:

- імплементація Конвенції про кіберзлочини; визнання європейських цифрових підписів;
- визначення комп'ютерних послуг на основі Кодексу ООН CPC84;
- розробка законопроекту, спрямованого на адаптацію до норм європейського права у сфері IP (Internet Protocol);
- покращення трудового законодавства;
- залучення України в програму COSME (Competitiveness of enterprises and SMEs);
- запровадження е-уряду та окремих елементів (е-суд, е-закупівлі тощо) (у 2016 р., для прикладу, Україна займала 118 місце із 138 країн з Е-готовності уряду та 72 місце з використання урядом інформаційних комп'ютерних технологій [3];
- законодавче стимулювання науково-дослідних центрів та нових підприємств ІТ-сфери;
- скорочення кількості регулювальних та контролювальних органів, усунення дублювання їх функцій;
- розвиток співпраці у сфері інноваційної діяльності між державою, суб'єктами підприємництва, навчальними закладами та науково-дослідними інституціями;
- визначення на законодавчому рівні понять "бізнес-центр", "бізнес-інкубатор", "кластеризація", "субконстрактація";
- заохочення суб'єктів підприємництва до соціальної відповідальності бізнесу;
- реформування податкової політики (першим кроком є прийняті закони "Про державну підтримку розвитку індустрії програмної продукції" та внесення змін в Податковий кодекс України, що встановлюють особливий порядок оподаткування для ІТ-сфери тощо [3].

Таким чином, можна з впевненістю стверджувати, що тільки тісна співпраця та сприяння з боку держави може забезпечити сталий розвиток ІТ галузі України.

Література

1. ТОП-50 крупнейших IT-компаний Украины. DOU: *Сообщество программистов.* URL: https://jobs.dou.ua/top50/
2. 5 речей, які заважають розвитку ІТ в Україні. *Baker Tilly.* URL: http://www.bakertilly.ua/news/id1243
3. Седікова І. О. Сучасний стан розвитку телекомунікаційного простору України / І. О. Седікова, Д. В. Седіков // *Економіка харчової промисловості*. 2014. № 4. С. 74-78. URL: http://nbuv.gov.ua/j-pdf/echp_2014_4_13.pdf.
4. ICT Development Index 2019. International Telecommunication Union, ITU. URL: https://www.itu.int/net4/ITU-D/idi/2019/index.html

ВПЛИВ СТАДІЇ ЖИТТЄВОГО ЦИКЛУ ПІДПРИЄМСТВА НА ЙОГО ФІНАНСОВУ СТІЙКІСТЬ

Хлевицька Т.Б., к.е.н., доц., Іванова Г.М.
Державний університет телекомунікацій
м. Київ, Україна

У ході посилення процесів економічної глобалізації успішне функціонування підприємств значною мірою залежить від рівня стійкості їх фінансового стану. Тільки за цієї умови підприємство зможе генерувати чинники позитивних кількісних і якісних змін для нормального функціонування в теперішній час і зростання виробничого потенціалу в майбутньому, тому на нинішньому етапі ринкових реформ забезпечення фінансової стійкості підприємств є одним із пріоритетних завдань.

Питання забезпечення фінансової стійкості економічних суб'єктів, розробки системи аналітичних засобів та інструментів її оцінки досліджено в наукових працях вітчизняних і зарубіжних вчених, зокрема в працях І. А. БланкА [1], Є. Г. Рясних [2], П. В. Пузирьової [4], Н. М. Внукова [5] та інших, але ці проблеми залишаються ще не вирішеними й потребують подальшого розгляду. Метою дослідження є виявлення закономірностей управління фінансовими ресурсами відповідно до життєвого циклу підприємства.

Сутність стратегічного управління фінансовою стійкістю підприємства визначається ефективним формуванням, розподілом і використанням фінансових ресурсів на етапах його життєвого циклу. Так, для успішної діяльності підприємствам необхідно звертати увагу на стадії основних життєвих циклів, також слід враховувати те, що ситуація на ринку має тенденцію до зміни на кожній стадії. І як результат це вимагає відповідної зміни стратегії і тактики поведінки підприємства на ринку.

Розглянемо життєвий цикл ТОВ «ДІБК», використовуючи метод розрахунку показників стадій життєвого циклу розвитку підприємства О. М. Скрибицького [4, с.231]. Перш за все необхідно сформувати матрицю вихідних показників (3 групи показників – прибутковості, ділової активності, ліквідності та фінансової стійкості) репрезентативної групи підприємств.

З метою уникнення використання в розрахунках значних випадкових відхилень, виключень з типового діапазону значень, які можуть різко змінити результат дослідження розрахуємо середнє арифметичне значення (X), середнє квадратичне відхилення (σ) для показників підприємств і додатково відкидаємо значення, що менші, ніж $X - 2\sigma$ або більші, ніж $X + 2\sigma$.

На наступному етапі значення показників підприємств перетворюємо в індексну форму так, щоб діапазон цих індексів становив від 0 до 1, причому для всіх показників збільшення величини індексів свідчило б про кращий стан підприємства.

Потім розраховуємо інтегральні індекси за окремими групами показників (інтегральні індекси показників прибутковості І(п), ділової активності І(да), ліквідності І(л), фінансової стійкості І(фс):

$$І(п) = I_{(1.1)j}*K_{1.1} + I_{(1.2)j}*K_{1.2} + I_{(1.3)j}*K_{1.3} + ... + I_{(1.8)j}*K_{1.8}, \quad (1)$$

$$І(да) = I_{(2.1)j}*K_{2.1} + I_{(2.2)j}*K_{2.2} + I_{(2.3)j}*K_{2.3} + ... + I_{(2.14)j}*K_{2.14}, \quad (2)$$

$$І(л) = I_{(3.1)j}*K_{3.1} + I_{(3.2)j}*K_{3.2} + I_{(3.3)j}*K_{3.3} + ... + I_{(3.5)j}*K_{3.5}, \quad (3)$$

$$І(фс) = I_{(4.1)j}*K_{4.1} + I_{(4.2)j}*K_{4.2} + I_{(4.3)j}*K_{4.3} + ... + I_{(4.10)j}*K_{4.10}, \quad (4)$$

де К— коефіцієнт вагомості кожного з показників в межах групи.

Так, використовуючи вищенаведені формули (1-4) розрахуємо інтегральні індекси за групами показників ТОВ "КІБК":

І(п) = 0,9385

І(да) = 0,7892

I(л) = 0,9792

I(фс) = 0,8412

На основі формули середньої геометричної зі значень чотирьох інтегральних індексів розраховуємо загальний інтегральний індекс життєвого циклу підприємства:

$$(ЗІЖЦП)а = (1+I(1)j)*(1+I(2)j)*(1+I(3)j)*(1+I(4)j), \quad (5)$$

$$ЗІЖЦП = \sqrt[4]{(ЗІЖЦП)а} - 1, \quad (6)$$

Використовуючи формули 1.5 і 1.6 розраховуємо загальний інтегральний індекс життєвого циклу ТОВ «КІБК»:

$$(ЗІЖЦП)_{ТОВ\ «КІБК»} = (1+0,9385)*(1+0,7892)*(1+0,9792)*(1+0,8412) = 12,572$$

$$ЗІЖЦП_{ТОВ\ «КІБК»} = \sqrt[4]{12,572} - 1 = 0,88$$

Наближення значення $ЗІЖЦП_{КІБК}$ до одиниці свідчить про міцність фінансово-економічного становища підприємства і про можливість відображення його позиції у верхній частині кривої життєвого циклу підприємства.

Таким чином, виходячи з наявного потенціалу підприємства, вважаємо доцільним використання корпоративної стратегії прискореного зростання, якій відповідає стратегія фінансової підтримки прискореного росту, що передбачає зростання потенціалу формування фінансових ресурсів, які спрямовуються на приріст оборотних і основних активів підприємства.

Література

1. Бланк І. О. Фінансовий менеджмент. Київ: Ельга. 2008. 724 с.
2. Рясних Є. Г. Основи фінансового менеджменту. Київ: Академвидав. 2010. 336 с.
3. Скібіцький О. М. Антикризовий менеджмент. Київ: Центр навчальної літератури. 2017.
4. Пузирьова П. В. Матриця ключових стратегій в управлінні фінансовим потенціалом промислових підприємств. *Актуальні проблеми економіки.* 2018. №6 (108). С. 151- 156.
5. Внукова Н. М. Формування системи кількісних показників оцінки фінансового стану підприємств-емітентів. *Фінанси України*. 2016. №12. С.112-120.

АВС-АНАЛІЗ ЯК ІНСТРУМЕНТ СТРАТЕГІЧНОГО УПРАВЛІННЯ ТОВАРНИМ ЗАБЕЗПЕЧЕННЯМ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

Корнілова О.В., к.е.н., доц., Ященко А.В.
Донецький державний університет управління
м. Маріуполь, Україна

В умовах економічної нестабільності можливості виживання підприємства на ринку зумовлюються якістю сформованого стратегічного асортименту товарів та, відповідно, товарного забезпечення діяльності підприємства. Урізноманітнення вимог і потреб споживачів змушує підприємства гнучко підходити до формування власного асортименту. Одночасно посилення конкуренції серед постачальників та збільшення пропозиції товарів на ринку визначають необхідність ефективного управління товарним забезпеченням як одного з джерел конкурентних переваг торговельного підприємства. У зв'язку з цим обґрунтування

інструментарію стратегічного управління товарним забезпеченням набуває неабиякого значення.

Одним з універсальних методів структурного аналізу товарного портфелю підприємства є АВС-аналіз, який використовується для визначення ключових пріоритетів в діяльності підприємства загалом, і в управлінні товарним забезпеченням зокрема. Цей аналіз передбачає поділ об'єктів управління на 3 групи (найважливіші, середньої важливості, неважливі) за питомою вагою певного показника. Основна ідея АВС-аналізу ґрунтується на засадах принципу Парето: 20% усіх товарів дають 80% обороту. На основі цього методу визначається АВС-рейтинг усіх товарів з товарного портфелю підприємства, на основі чого розробляється стратегія розвитку і змін у товарному забезпеченні.

Отже, до групи А відносяться товари, сума накопичених вартостей яких складає 50% від сумарної вартості усіх реалізованих товарів за звітний період. Ця група є найбільш активною і тому має підлягати найщільнішому контролю і управлінню. Група В налічує товари, сума вартостей яких складає 80%. Дана група потребує менше управлінської уваги. Стосовно групи С, то ця група складається з товарних позицій, сумарна вартість яких – лише 20%. Ця група обслуговується найменш активно, тому що забезпечує малу частку обороту підприємства.

Варто зазначити, що АВС-аналіз доцільно проводити не тільки за одним вартісним показником, яким є товарооборот або прибуток, а й за реалізацією товарів у натуральних одиницях. Поєднання аналізу за вартісними й натуральними показниками дозволяє нівелювати вплив ціни товару. Тобто, якщо товар має низьку ціни, але продається добре, він може потрапити у групу В чи С. І навпаки, якщо дорогий, з високою надбавкою товар, продається рідко, але за рахунок високої вартості може потрапити у групу А, результатом чого будуть некоректні результати.

Однак, при значній кількості переваг АВС-аналіз має свої обмеження і недоліки [1, с. 172]:

Неточність вихідної інформації може суттєво вплинути на кінцевий результат і, як наслідок, привести до розробки неефективної помилкової стратегії управління товарним забезпеченням.

Нові товари в портфелі підприємства частіш за все потрапляють до групи С, тому що ще не вийшли на рівень повноцінних продажів, тож при проведенні аналізу доцільно враховувати стадію життєвого циклу товару, щоб співвідносити результати аналізу і час знаходження товару в асортименті підприємства.

Сезонні коливання і нестабільні продажі не враховуються при АВС-аналізі. Отже, для зменшення впливу цих факторів доцільно використовувати ще один метод – XYZ-аналіз.

Література

1. Комкова Е. Товарный портфель и управление закупками в рознице. СПб.: Питер. 2018. 376 с.

СЕКЦІЯ 2. НОВІТНІ ТРЕНДИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ

МЕТОДИКА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КРИТИЧНИХ КОМПОНЕНТІВ МЕРЕЖ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

Гуменюк І.В., к.т.н., Басараба М.С., Некрилов О.В.
Житомирський військовий інститут
імені С. П. Корольова,
м. Житомир, Україна

Інформаційний сектор завжди викликав великий інтерес у кіберзлочинної спільноти. За останніх п’ять років кібератаки здійснювалися на держустанови, сферу науки (освіти), фінансову, промислову та військову галузі. Прикладом тому є значна кількість атак, які сталися в світі. В Україні в умовах складної та недостатньо стабільної політико-економічної ситуації такі випадки також мають місце. Таким чином, в умовах, що склалися, актуальним є завдання розроблення нових дієвих, ефективних та удосконалення існуючих методів протидії кібернетичним атак та несанкціонованого доступу (НСД).

Виходячи з даних передумов, сформульовано **мету** даної доповіді, яка полягає у розробленні методики забезпечення кібербезпеки критичних компонентів мереж інформаційно-телекомунікаційної системи (ІТС).

Забезпечення надійного та дієвого захисту інформації, важливих компонентів ІТС є комплексним завданням, яке включає в себе сукупність взаємопов’язаних між собою задач. Саме тому, для досягнення мети завдання запропоновано методику, яка складається з таких кроків:

- постійний контроль стану мережевих вузлів та каналів зв’язку мереж ІТС;
- фіксування фактів здійснення кібернетичних атак з детальним описом рівня небезпеки загроз;
- постійний контроль доступу користувачів до мереж ІТС;
- своєчасне виявлення НСД до мереж ІТС та кіберзагроз, а також оперативна протидія цим спробам.

Детально розглянемо кожен із кроків.

Постійний контроль стану мережевих вузлів та каналів зв’язку мереж ІТС. Оскільки важливим завданням управління мереж є підтримання функціональності та надійності кожного мережевого компоненту, для ІТС необхідно використовувати ієрархічне управління, розподіливши мережу на окремі зони (кластери) з виділенням контролерів кластера, вузлів-шлюзів і внутрішніх вузлів кластера. Для постійної підтримки актуальності таблиць маршрутизації та цілісності топології мережі, контролери кластерів періодично розсилають вузлам інформацію про стани каналів. В умовах успішного проведення кібератаки на вузол кластера (він визначається як потенційно-небезпечний) проводиться його фізична ізоляція (рис. 1). Такий підхід ефективний для забезпечення кібербезпеки іншого кластера.

Фіксування фактів здійснення кібернетичних атак з детальним описом рівня небезпеки загроз. На даному кроці проводиться аналіз вхідного (вихідного) трафіка кластерів мережі, зокрема з використанням наявної системи виявлення вторгнень Intrusion Detection System (IDS). У результаті виконання поточного кроку визначається рівні безпеки мережі: допустимий (трафік містить певну загрозу, однак може фільтруватися) та небезпечний (вхідний трафік блокується для подальшого проходження в мережу).

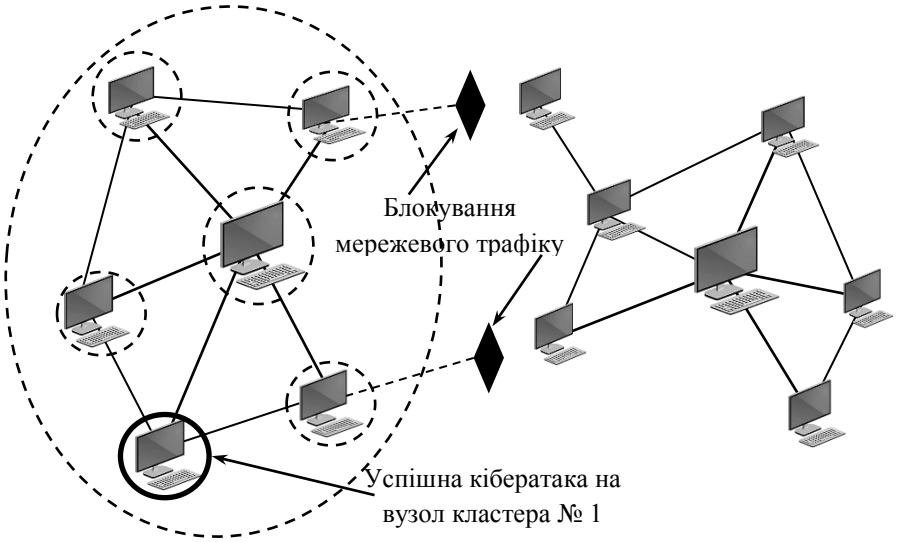


Рис. 1. Фізична ізоляція потенційно-небезпечного кластера

Постійний контроль доступу користувачів до мереж ІТС. Для забезпечення перевірки автентичності користувачів на даному етапі здійснюється:

Виявлення та локалізація геометрії обличчя користувача на зображені відеопотоку. Для пошуку форми (геометрії) обличчя на зображені систем відеоспостереження використано алгоритм Віоли-Джонса. При використанні даного методу відеозображення подається в інтегральному вигляді для підвищення оперативності аналітичних обчислень та розрахунків.

Обчислення набору базових ознак (характеристик) зображення. Основними принципами, на яких ґрунтується метод Віоли-Джонса є використання базових понять теорії розпізнавання об’єктів, зокрема ознак (примітивів) Хаара, застосування їх каскаду для аналізу результату ідентифікації.

Порівняння обчислених ознак з еталонними, які містяться у базі даних.

Структуру контролю доступу користувачів до мереж ІТС подано на рис. 2.

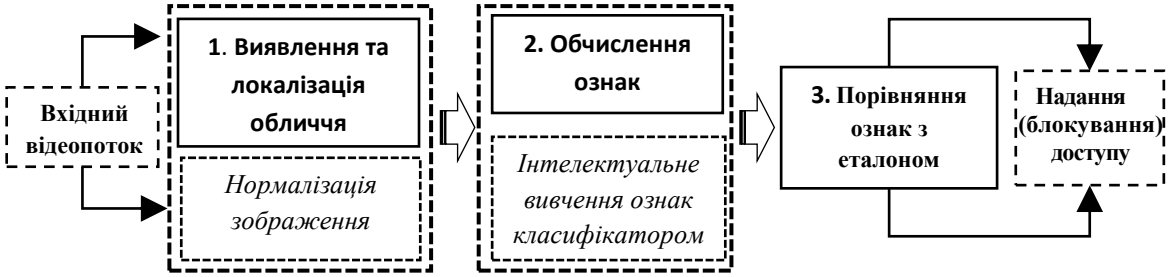


Рис. 2. Структура контролю доступу користувачів до мереж ІТС

За умови скоєння кібератак та/або НСД виконується ***своєчасне виявлення НСД до мереж ІТС та оперативна протидія цим спробам та кіберзагрозам.*** Виконання останнього етапу методики ґрунтується на узагальненні інформації про скоєння кіберзагрози або НСД, зокрема: власне сам факт здійснення кібернетичних атак (час, “компонент-жертва”, нова або повторна загроза тощо); деталізований опис рівня небезпеки загрози.

Отже, виконання завдання забезпечення захисту кібербезпеки критичних компонентів мереж ІТС, актуальність якого обумовлена збільшенням кількості кібератак Російської Федерації у кіберпросторі України та загроз національній безпеці держави, можливе з використання запропонованої методики.

БЕЗПЕКА ІНТЕРНЕТУ РЕЧЕЙ (IoT) ПРОТИ ПОШУКОВОГО АГРЕГАТОРА SHODAN

Гончаренко Н.А.
Київський національний університет імені Тараса Шевченка
м. Київ, Україна

З кожним днем ми стаємо все більш залежними від технологій, що зумовлено прискореним розвитком Інтернету речей (IoT) – складної мережі фізичних пристроїв та систем із доступом до мережевого підключення, яке дозволяє їм обмінюватися даними через Інтернет. Мабуть, таке явище вважалося б науково-фантастичним 20 років тому, однак сьогоднішня реальність доводить, що кіберфізичні системи пронизують усі аспекти нашого сучасного життя. Їх застосування включає моніторинг навколишнього середовища, управління інфраструктурою, охорону здоров'я, транспорт та ін.

У майбутньому кожен пристрій буде зв'язаний з сотнями таких же інших, але чи замислювався хтось про наслідки подібного симбіозу для інформаційної безпеки? Статистика на сьогоднішній день свідчить про те, що ні. Ідея створення механізмів безпеки в IoT залишилась лише задумом, своєрідним додатковим доповненням замість того, щоб бути інтегрованою в дизайн з самого початку життєвого циклу усіх його продуктів [1].

Як результат, ми отримуємо мережу взаємопов'язаних незахищених пристроїв, які є загальнодоступними з просторів Інтернету. Тут буде як ніколи доцільним згадати про існування проекту, основною метою якого є автоматизація виявлення та подальша каталогізація таких пристроїв.

Shodan – це пошукова система, що у деякому розумінні схожа до Google, проте на цьому уся її подібність закінчується. Замість того, щоб індексувати веб-вміст через порти 80 (HTTP) або 443 (HTTPS), як це робить Google, Shodan сканує в Інтернеті пристрої, що реагують на безліч інших портів, включаючи 21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 80, 443, 3389 (RDP) та 5900 (VNC). Як тільки Shodan виявляє хост, який відповів на запит через певний порт, він підключається до нього і отримує всю доступну сервісну інформацію про код стану системи, версію ПЗ, яку вона використовує, обслуговуючі сервіси і т.д. Потім ця інформація індексується разом із даними про геолокацію пристрою [1].

Рис.1. Результати пошуку за заданим фільтром у Shodan

З моменту запуску в 2009 році Shodan виявив та проіндексував досить широкий спектр підключених до Інтернету пристроїв, включаючи веб-камери, обладнання сигналізації дорожнього руху, маршрутизатори, брандмауери, системи відеоспостереження, промислові системи управління атомними електростанціями та електричними мережами, побутову техніку і т.п. Ці пристрої були підключені до Інтернету часто навіть без застосування базових засобів захисту, таких як надійні ім'я користувача та пароль.

Варто відмітити, що достатня частка знайдених пристроїв все ж таки має певний захист – наприклад, такий, що вимагає автентифікації, але навіть це не дає 100-відсоткової

гарантії захищеності від несанкціонованого доступу. У мінливому світі кібербезпеки ніщо не залишається статичним, тому список існуючих уразливостей поповнюється новими загрозами кожен день.

Вагомим прикладом для підтвердження вище висловленої думки може стати діяльність однієї з найбільш відомих компаній у галузі комп'ютерних мереж Juniper. У результатах свого недавнього публічного дослідження Juniper показала, що прошивка, яка працює на деяких їх пристроях, містить жорстко закодований пароль, який дозволить кожному, хто підключається до вразливого пристрою, просто поставити цей пароль у парі до дійсного облікового запису користувача, щоб отримати повний адміністративний доступ до жертви через Telnet або SSH [1].

Таким чином, використовуючи можливості Shodan, ми можемо переглядати список брандмауерів Juniper у пошуку тих, на яких запущена вразлива версія прошивки ScreenOS. Після підключення до панелі управління ми надаємо раніше відомий пароль для типового облікового запису користувача ScreenOS (*system*) і отримуємо змогу розпочати віддалене управління пристроями, що містять дану вразливість [2]. Якщо припустити, що лише 10% із проіндексованих 18 000 брандмауерів є вразливими (що є надзвичайно консервативною оцінкою), то це 1800 вразливих одиниць програмного забезпечення Juniper, яке наразі перебуває в мережі Інтернет.

Як кінцеві споживачі, ми повинні ретельно проектувати інфраструктуру розумних гаджетів і враховувати інформаційні загрози, які надходять до нас разом із придбанням цих пристроїв. Що стосується компаній, то вони зобов’язані переконатися, що володіють у своєму розпорядженні належним механізмом управління ризиками, який включатиме у себе не тільки можливість постачання корисного продукту, а і відповідні засоби для забезпечення його безпеки.

Література

1. M. Carthy. Shodan: The World’s Most Dangerous Search Engine. LinkedIn. February 28, 2016. URL: https://www.linkedin.com/pulse/shodan-worlds-most-dangerous-search-engine-michael-carthy.
2. CVE-2015-7755. Common Vulnerabilities and Exposures. August 10, 2015. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7755.

ФОРЕНЗІКА

Порохницький О.А.
Державний Університет телекомунікацій
м. Київ

Форензіка – це наука про дослідження доказів або ж по іншому комп’ютерна криміналістика.

На сьогоднішній день в світі спеціалісти в цій області є незамінними при необхідності знайти та проаналізувати інциденти в сфері Інформаційної безпеки, втрати конфіденційної інформації, злому серверів або ж робочих станцій. В своїй роботі спеціаліст в сфері форензіки притримуються наступним завданням:

1) Розібратися в реалізації злому
2) Побудувати сценарій атаки
3) Відновити хронологію атаки
4) Зібрати сліди атаки
5) Розробити необхідні міри захисту для попередження таких ситуацій в майбутньому

6) Зменшити пошкодження та відновити систему

Наприкінці експерт повинен зробити висновок стосовно інциденту ІБ цілком можливо що він знадобиться для державних органів. Тож все більше компаній з кожним днем впевнюються в потребі спеціального відділу, що буде займатися комп'ютерною криміналістикою. Також можна виділити окремо APT або ж цілеспрямовані атаки, їх метою є злом цільових систем нестандартними, а інколи досить специфічними методами та техніками невідомими до сьогодні.

Класифікація форензіки

Форензіку як і будь-яку науку можна поділити на деякі теми:

1) Computer forensics – відноситься до пошуку артефактів на локальних машинах.
2) Network forensics – розслідування в сфері мережевого стеку, дампу та парсингу мережевого трафіку.
3) Forensic data analysis – аналіз файлів та даних.
4) Mobile device forensics – відноситься до вилучення даних Android та iOS.
5) Hardware forensic – експертиза апаратного забезпечення та технічних пристроїв.

Також форензіку можна поділити на два основних підходи: статичний та динамічний аналіз.

Статичний аналіз – скопіювати образ жорсткого диску або дампу оперативної пам'яті, виявити та відновити видалені файли, аномальні файли в системних директоріях.

Динамічний аналіз – використовують нарізку з снапшотів системи, які запускаються в різних умовах для отримання повного бачення ситуації. Це дозволяє побачити як веде себе зловмисне ПЗ на зараженому комп'ютері.

В проведенні комп'ютерної криміналістики не обійтися без різного види спеціального ПЗ:

1. Створення образу диску, розділу або сектору.
1)FTK imager
2)dc3dd
2. Сбір даних з жорстких дисків.
1)DumpIt
2)Encrypted Disk Detector
3. Аналіз знайдених файлів.
1)Crowd Inspect
2)Memoryze
4. Обробка оперативної пам'яті
    1)Forensics, Memory Integrity & Assurance Tool by invtero
    2)Rekall
5. Пошук артефактів на HDD
    1)FastIR Collector
    2)FRED

Для форензіки існує достатня кількість дистрибутиві - CAINE, DEFT, Parrot OS, Sumuri PALADIN, Kali Linux – Forensic mode, Tsurugi. Окремо можна зазначити платні дистрибутиви та вузькопрофільні, а також можна використати Gentoo і зібрати свій власний дистрибутив для роботи.

Отже, можна зазначити що на сьогодні форензіка є досить важливою частиною кібербезпеки яка проводить аналіз заражених систем, дисків, мереж, детальний розбір атак на них та надає інформацію стосовно нових способів атаки та їх виявлення.

Література

1. https://spy-soft.net/computer-forensics/#_email

СЕКЦІЯ 3. ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА

УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА

Якименко Ю.М., к.в.н., доц.
Державний університет телекомунікацій
м.Київ, Україна

Завдання забезпечення національної стійкості останнім часом все частіше стає пріоритетом для для багатьох країн та міждержавних об'єднань світу, в тому числі і для України.

Аналіз застосування поняття «стійкість» свідчить про використання цього терміна в основному у вигляді інструменту формалізації діяльності системи забезпечення безпеки підприємства, а саме як вимоги до діяльності його керівництва, яка має враховувати різні типи загроз та спроможність реагувати протягом усього діапазону можливого розвитку ситуації – будь -якої події чи інциденту (передбачення – підготовка – запобігання – реагування – відновлення), що завжди формує запит на методологічний вимір впливу на рівень інформаційної та кібербезпеки підприємства.

В зарубіжній практиці використовується різна термінологічна база для опису діяльності у цій сфері забезпечення безпеки підприємства.Так директива президента США 2013 року (PPD-21) трактує поняття [1, с.15]:

• стійкість – «спроможність підготуватись та адаптуватися до змінних умов, а також протистояти загрозам порушень функціонування, шляхом вжиття фізичних заходів чи захисних кіберзаходів стосовно вторгнень та швидко відновлюватися від порушень. Стійкість включає спроможність протистояти загрозам та відновлюватися від цілеспрямованих атак, аварій, природних за-гроз та інцидентів»;

• забезпечення безпеки– «зменшення ризику критичної інфраструктури від втручання, атак або ефектів, спричинених природними катастрофами або людською діяльністю, за рахунок реалізації заходів із фізичного захисту або кіберзахисту».

В нормативних документах Великої Британії стійкість розглядається, як здатність активів, мереж та систем прогнозувати руйнівні події, переносити їх, адаптуватися до та швидко відновлюватися після них.

В українській практиці [1,с.17] необхідність усвідомлення діяльністного виміру в забезпеченні безпеки й стійкості та його формалізованого закріплення у документах додатково ускладнюється, так як безпека переважно розуміється як стан об'єкта, тобто як ціль та результат діяльності створеної системи безпеки і її можливості по запобіганню реалізації загроз та настання інцидентів будь-якого типу.

Таким чином в сучасних умовах зміст діяльності щодо безпеки зміщується на діяльність із недопущення пошкодження функціонування підприємства як об'єкта переважно внаслідок зловмисних дій (з поступовим розширенням також на загрози природного і техногенного характеру), а також із фокусуванням на створенні додаткового захисту від нових видів загроз.

Термін «стійкість» при цьому фокусується на діяльності зі створення можливостей для підготовки щодо запобігання та реагування на загрози і інциденти, адаптації до нових умов функціонування та відновлення нормального режиму роботи (хоча це також включає питання, які охоплені поняттям «захист»). Проте термін «стійкість» ще не визначений українським законодавством, а лише входить у практику використання. Робота провідних фахівців з кібербезпеки в Україні дозволила запропонувати визначення стійкості як «спроможність надійно функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після реалізації загроз будь-якого виду» [1,с.18].

Система безпеки стійкості кібербезпеки (БСК) підприємства має опікуватися питаннями інфраструктури забезпечення реалізації життєво важливої функції (фізичний, організаційний, структурний виміри). З позицій системного підходу сфера відповідальності системи БСК підприємства стосується переважно організаційно-функціональної структури його життєдіяльності, яка забезпечує взаємодію, обмін ресурсами та інформацією між підрозділами, як її елементами.Україна перебуває на початковому етапі створення державної системи БСК , тому при розгляді зарубіжного досвіду важливо виокремити загальні підходи до створення національних систем, в тому числі і на рівні підприємств, їх основні цілі, структурні особливості та базові елементи, механізми та інструменти, які забезпечують їхнє функціонування, урахування специфіки та реалії українського сьогодення.

Система БСК, що створюється, повинна:

- забезпечувати безпеку та стійкість щодо всіх видів фізичних загроз та кіберзагроз;
- удосконалювати механізми та процедури взаємодії та обміну інформацією на всіх рівнях управління кібербезпекою;
- функціонувати на основі ризик-орієнтованих підходів, чіткого розподілу повноважень і відповідальності щодо налагоджування ефективного обміну інформацією між усіма суб'єктами процесу забезпечення БСК;
- забезпечувати виконання функцій інтегрування та аналізу даних по загрозам і інцидентам для підтримки процесів планування та прийняття рішень стосовно кібербезпеки;
- проводити підготовку кадрів для забезпечення функціонування БСК;
- постійно перевіряти готовність сил і засобів, планів і процедур взаємодії та обміну інформацією про загрози і інциденти під час регулярних навчань на всіх рівнях управління.

В системі БСК повинні також бути створені наступні спеціальні механізми: «раннього попередження», «координації та обміну інформацією», «планування, запобігання, реагування та функціонування у кризових ситуаціях», « виявлення та реєстрації загроз інформаційної безпеки».

З огляду на важливість виявлення інцидентів процедури збору інформації можуть забезпечуватися як технічними, так і організаційними заходами. Інформація про виявлені інциденти фіксується у спеціальних журналах (в паперовому і електронному вигляді). Результати аналізу, розслідувань і профілактичних заходів зазвичай оформляються у вигляді довідок, звітів і аналітичних записок та зберігаються в підрозділі ІБ. Ще більшою проблемою стає підготовка і аналіз статистики, тоді як вона є одним з ключових показників ефективності діючої системи БСК підприємства. Ефективність процесу управління інцидентами залежить від:

1. координації і узгодженості дій всіх залучених осіб;
2. наявних можливостей з отримання і аналізу інформації, пов'язаної з інцидентом;
3. оперативності і коректності отриманих результатів.

Управління інцидентами можливе тільки тоді, коли буде на підприємстві створена і постійно використана СМІБ (система менеджменту інциндентів інформаційної безпеки).

Далі приводяться задачі і можливості СМІБ.

Таким чином, система БСК підприємства фактично буде системою колективної роботи, яка автоматизує процеси з УІБ, за допомогою інтеграції людей і апаратно-програмного забезпечення моніторингу і захисту, а також інформаційної інфраструктури організації.

Література

1. Бобро Д. Г. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / / Д. Г. Бобро та інші / за заг. ред. О. М. Суходолі. – Київ : НІСД, 2019. 224 с. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf#page=8&zoom=auto,-75,489

КОНЦЕПЦІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА

Мужанова Т.М., к.держ.упр, доц.
Державний університет телекомунікацій
м. Київ, Україна

Поняття «кіберстійкість» з'явилося на стику кібербезпеки та неперервності, стійкості бізнесу. Кібербезпека використовує технології, процеси і заходи, які призначені для захисту систем, мереж і даних від кіберзлочинів. Ефективне забезпечення кібербезпеки знижує ризик кібератак і захищає організації, підприємства й окремих осіб від навмисного деструктивного використання систем, мереж і технологій.

Кіберстійкість розглядається в більш широкому контексті і допомагає компаніям усвідомити наявні переваги зловмисників у використанні інноваційних інструментів, ефекті несподіванки і реально оцінити їхні шанси на успіх. Концепція кіберстійкості має на меті навчити бізнес, як підготуватися, запобігти, відреагувати і успішно відновитися після деструктивних кіберподій до передбачуваного безпечного стану. Це культурне зрушення, оскільки кіберстійкість вимагає від бізнесу не тільки постійної роботи із забезпечення кіберзахисту і впровадження передових методів безпеки в повсякденні операції, але іншого мислення і більшої гнучкості в боротьбі з кібератаками [4].

Досягти кіберстійкості не так легко, як може здатися на перший погляд. Дослідження «Business Risk & Cyber Resilience» свідчать, що лише 36% організацій із шести ключових галузей у США, Великобританії, Німеччині, Франції та Японії можна вважати кіберстійкими [3]. Однак, на нинішньому етапі забезпечення кіберстійкості є життєво важливим завданням кожної сучасної організації чи підприємства.

На думку фахівців-практиків, забезпечення кіберстійкості означає процес підготовки компанії до потенційних збоїв бізнесу, спричинених кібератаками, здатність відновлюватися після цих порушень і системні можливості адаптуватися й розвиватися після кожної пережитої атаки.

Успіх стратегій кіберстійкості підприємства базується на дотриманні комплексу принципів, серед яких:

- ініціативність і вирішення проблем безпеки;
- вчасне прийняття рішень з питань безпеки;
- застосування різноманітних кіберзасобів;
- організаційна готовність і вирішення бізнес-проблем;
- технічна гнучкість і адаптивність;
- ситуаційна обізнаність Рис.1 [1].

Рис.1. Принципи кіберстійкості.

Відповідно до бачення Національного інституту стандартів і технологій США (NIST) [2] кіберстійкість передбачає здатність компанії досягти таких основних *цілей*:

–Anticipate - передбачати, тобто підтримувати стан поінформованої готовності до кібератак.

–Withstand – протистояти, продовжувати основні місії або ділові функції, незважаючи на кіберзагрози.

–Recover - відновлювати місії або виконання ділових функцій під час і після кіберінцидентів;

–Adapt - пристосовуватися – модифікувати місію, ділові функції та допоміжні можливості відповідно до передбачуваних змін у технічному, експлуатаційному середовищах чи середовищі загроз.

Досягнення зазначених цілей може стосуватися системи; механізму, компонента або елемента системи; розподіленого сервісу, загальної інфраструктури або системи систем, що ідентифікуються з місією чи бізнес-функцією; організації; сектору критичної інфраструктури або регіону; системи систем у секторі критичної інфраструктури або підгалузі; і до держави (нації). Кіберстійкість має стати ключовим елементом будь-якої ефективної стратегії забезпечення операційної стійкості, окремої місії компанії або розвитку бізнесу загалом.

На думку дослідників NIST, основними *завданнями* забезпечення кіберстійкості є:

Prevent or Avoid. Запобігати або уникати кібератак, щоб виключити успішне виконання нападу або реалізацію несприятливих умов.

Prepare. Бути готовим до атак, дотримуючись реалістичних напрямів дій, що враховують передбачувані або неочікувані загрози.

Continue. Забезпечити неперервність, максимізувати тривалість і життєздатність основних місій або ділових функцій організації під час інцидентів.

Constrain. Обмежити обсяги збитків внаслідок кіберінцидентів.

Reconstitute. Відновлювати місії або ділові функціональності після атак.

Understand. Зрозуміти, усвідомити наміри порушника, стан захищеності активів та наявні вразливості, оцінити ефективність засобів кібербезпеки.

Transform. Трансформувати місію, ділові функції та допоміжні процеси організації, щоб ефективніше справлятися з труднощами та враховувати зміни середовища.

Re-Architect. Змінювати архітектуру систем, щоб ефективніше справлятися з труднощами та враховувати зміни оточуючого середовища.

Для досягнення кіберстійкості NIST рекомендує використовувати низку *методів (технік)*, перелік яких подано у таблиці 1 [2].

Таблиця 1

Методи (техніки) кіберстійкості

Техніка	Мета
Adaptive response Адаптивна відповідь	Оптимізація здатності реагувати своєчасно і належним чином, забезпечуючи безперервність функціонування організації та надання послуг
Analytic monitoring Аналітичний моніторинг	Постійне відстеження ситуації з метою своєчасного виявлення несприятливих дій і умов. Забезпечення ситуаційної обізнаності
Coordinated protection Скоординований захист	Впровадження стратегії глибокоешелонованого захисту, зменшуючи шанси нападника досягти критичних активів
Deception Введення порушника в оману	Надання хибної інформації щодо активів, захист критично важливих активів, перешкоджання й заплутування нападника з метою його виявлення
Diversity Забезпечення різноманітності	Використання різноманітних засобів захисту для мінімізації атак, що використовують загальні вразливості

Dynamic positioning Динамічне позиціонування	Розподіл і динамічне переміщення функціональних можливостей або системних ресурсів у залежності від ситуації
Dynamic representation Динамічне представлення	Створення й підтримка ситуативної обізнаності про стан місій або ділових функцій організації з урахуванням впливу кіберподій та заходів кіберзахисту
Non-persistence Недовговічність	Створення та зберігання активів за потреби або протягом обмеженого часу, щоб не дати можливості порушнику їм зашкодити
Privilege restriction Обмеження привілеїв	Обмеження привілеїв на основі характеристик користувачів, елементів системи, зовнішніх чинників, щоб зменшити ймовірність ненавмисних деструктивних дій авторизованих осіб
Realignment Перегрупування	Зведення до мінімуму зв'язку між критично важливими і некритичними сервісами, тим самим зменшуючи ймовірність впливу відмови останніх на критичні сервіси
Redundancy Резервне копіювання	Створення кількох захищених примірників критично важливих активів, зводячи до мінімуму шанси їх втрати
Segmentation Сегментація	Ідентифікація і розмежування елементів системи відповідно до їх критичності та надійності
Substantiated integrity Підсилена цілісність	Постійна перевірка справності і неушкодженості критичних елементів системи для своєчасного виявлення деструктивних спроб зловмисника
Unpredictability Непередбачува-ність	Внесення змін у системи захисту позапланово і в випадковому порядку для перешкоджання потенційним діям нападника

Крім цього, у своїй концепції кіберстійкості експерти NIST розглядають дії, необхідні для розробки систем, здатних захистити себе і зберегти працездатність, а також складові компоненти і сервіси, які залежать від цих систем.

Таким чином, незважаючи на відносну новизну поняття «кіберстійкість», концепції кіберстійкості вже досить ґрунтовно розробляються в науці і широко використовуються на практиці. Встановлено науково обґрунтовані й апробовані на практиці принципи, цілі, завдання і методи досягнення кіберстійкості, які можуть бути використані підприємствами й організаціями різних галузей по всьому світу.

Література

1. Cyber Resilience: Part Three What is Cyber Resilience? URL: https://blog.blackswansecurity.com/ 2016/02/part-three-what-is-cyber-resilience/
2. NIST Special Publication 800-160 Volume 2. Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. URL: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf
3. The path to cyber resilience URL: https://www.greenbone.net/en/the-path-to-cyber-resilience/
4. Киберустойчивость - Cyber_resilience. URL: https://ru.qaz.wiki/wiki/ Cyber_resilience

ІНСТРУМЕНТИ ТЕСТУВАННЯ СИСТЕМ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

Андрущенко К.Ю.
Державний університет телекомунікацій
м. Київ, Україна

На сьогоднішній день ринок пропонує численні системи забезпечення інформаційної безпеки, і перед бізнесом постає проблема їх порівняння і вибору. Звичайні офісні програми можна оцінити тільки за функціоналом та зручністю використання, так як вони обираються безпосередньо для потреб бізнесу. В той же час рішення безпеки використовуються не для заробітку, а для мінімізації збитків при реалізації загрози, і ефективність обраного рішення виявляється під час інциденту. Якщо засоби захисту не нейтралізували зловмисні дії – бізнес понесе збитки.

Саме тому важливо оцінити ефективність засобу перед впровадженням в організації. Фактично всі рішення інформаційної безпеки надають можливість тестування перед придбанням – пілотний проект, що проводиться за допомогою компанії-інтегратора або дистриб'ютора. Остаточне рішення залишається за організацією, і саме спеціалісти організації займаються тестуванням рішення.

Постає питання, як спеціалістам інформаційної безпеки протестувати численні системи, коли це не є їх профільним напрямом і вони також мають інші обов'язки?

В першу чергу існують комерційні програмні продукти, розроблені для тестування комплексної системи захисту, але їх придбання доцільне тільки для великих організацій з окремим відділом інформаційної безпеки, можливо власним центром реагування. При цьому їх ефективність також необхідно обґрунтувати.

На противагу, в мережі існують загальнодоступні засоби тестування. Зупинимося на тестуванні захисту кінцевих точок, адже з часом межі мереж усе більше розмиваються, і актуальності набуває саме захист пристроїв користувачів. До найбільш відомих рішень можна віднести MITRE CALDERA, Atomic Red Team та APT Simulator. Усі наведені засоби доступні на платформі GitHub.

CALDERA – відкритий проект MITRE, розроблений переважно для автоматизації дій Red Team [1]. Для запуску атак необхідно налаштувати сервер та ініціювати агент на кінцевій точці. Далі у веб-інтерфейсі створюються профілі зловмисників шляхом комбінування наявних команд, і обрані операції запускаються агентом на кінцевій точці. Результат виводу команд також можна переглянути в консолі.

CALDERA є досить гнучким інструментом, надає можливість створювати власні операції, розробляти агенти, налаштовувати передачу інформації між операціями. Але загалом стандартного функціоналу достатньо для базового тестування, особливо коли спеціаліст організації не володіє глибокими знаннями в даному напрямку.

Atomic Red Team - це бібліотека простих тестів, які кожен спеціаліст інформаційної безпеки може виконати для перевірки засобів захисту [2]. Atomic Red Team пропонує схожий функціонал, в деяких моментах більш зручний, порівняно з CALDERA. Встановлюється система безпосередньо на комп'ютер для тестування і запускається з PowerShell. Основною перевагою є можливість автоматичної перевірки передумов виконання операцій (часто необхідно створити певний тестовий файл, деяким технікам необхідний адміністративний доступ). І навіть за відсутності веб-інтерфейсу, користуватись Atomic Red Team зручно.

APT Simulator менш масштабний у порівнянні з попередньо розглянутими засобами, але в той же час більш простий. APT Simulator - це скрипт Windows Batch, який використовує набір інструментів та вихідних файлів, щоб компрометувати систему. Немає необхідності налаштовувати сервер, достатньо завантажити підготовлений архів, розпакувати та запусти файл від імені адміністратора [3].

Звичайно поверхневе тестування загальнодоступними засобами не допоможе повністю і безпомилково оцінити систему захисту. Але грамотне використання наведених

систем висвітлить різницю між різними рішеннями безпеки, надасть можливість протестувати реакцію систем на дії зловмисника та зробити усвідомлений вибір. Правильно підібране рішення захисту кінцевих точок збереже фінансові ресурси організації та її репутацію.

Література

1. mitre / caldera. URL: https://github.com/mitre/caldera
2. redcanaryco / atomic-red-team. URL: https://github.com/redcanaryco/atomic-red-team
3. NextronSystems / APTSimulator. URL: https://github.com/NextronSystems/APTSimulator

РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ПІДПРИЄМСТВА ВІД ДИСКРЕДИТАЦІЇ ТА КОМПРОМЕТАЦІЇ

Єрмак М.В.
Державний університет телекомунікацій
м. Київ, Україна

Нині, в час коли весь світ потерпає від бурхливого розвитку, а доступ через інтернет до будь-якої інформації стає надлегким, стрімко розвиваються різноманітні форми впливу. Будь-яке підприємство піддається впливу негативних факторів внутрішнього та зовнішнього середовища, що в подальшому переростає в кризові ситуації й становить серйозну небезпеку. А тепер, коли в інтернеті можна не тільки знайти будь-яку компроментивну інформацію, але й написати про товар чи послуги нісенітниці. Так і виникає конкуренція. Оскільки вона є рушійною силою ринкової економіки, через своє стимулювання виробництва товарів, яких потребує споживач, то питання захисту підприємства від конкуренції, дискредитації, компрометації та похідних є досить актуальним.

Ділова репутація – невеличкий, але дуже важливий висновок про професійні та управлінські здібності. Але, на жаль, у бізнес-середовищу часто вдаються до нечесних методів конкурентної боротьби, задля того, щоб зіпсувати репутацію. Саме метод дискредитації для цього використовують найчастіше. Взагалі, дискредитація тлумачиться як умисні дії, спрямовані на підрив авторитету, іміджу й довіри [1]. А як відомо, основу репутації підприємства складає саме позитивний імідж. Аналіз досвіду багатьох успішних компаній свідчить, що підвищення іміджу дозволяє забезпечити не тільки високу ефективність виробництва й зайнятості, а й підвищити конкурентоспроможність підприємства. Щодо України, де умови економіки, з мають специфічні особливості, історичне минуле та сучасні проблеми, то навіть в такій ситуації ідеї авторитету й іміджу знаходять широкого практичного впровадження [1]. Тому невипадково конкуренти використовують метод дискредитації, щоб перешкоджати іншому суб’єкту господарювання та досягнення неправомірних переваг.

В такій ситуації, звичайно, постає питання: «Як же захиститися від такого впливу». Існує декілька рекомендацій, які варто врахувати, щоб знизити ризик потерпання від дискредитації:

- по перше, варто досить точно розуміти імідж підприємства як елемента конкурентної переваги та передбачати зміну його місця й ролі серед ресурсів підприємства;
- по друге, повинно бути розуміння, що свобода слова має свої межі та відрізняти свободу слова від образ та наклепу. Наприклад, поширена інформація повинна стосуватися конкретної особи; інформація повинна бути недостовірною; повинен бути факт заподіяння шкоди цією інформацією.

- по третє, необхідно вдосконалити методику управління діловою репутацією, через поглиблення теоретичних досліджень ділової репутації, її складових елементів, та факторів, що впливають на неї та як результат - це сприятиме підвищенню конкурентоспроможності підприємства та принесе йому значний комерційний ефект [2].

Компрометація – Ще один метод конкурентної боротьби. Це так званий факт доступу сторонньої особи до інформації, що захищається. Захистити своє підприємство від такого втручання трохи складнішу, оскільки розвиток технологій не стоїть на місці. Але декілька способів є:

- варто звернути увагу на підвищення ІТ-грамотності бухгалтерів підприємства, дасть можливість суттєво посилити систему безпеки захисту даних;
- також не потрібно забувати про захищеність сучасними та якісними антивірусами і мережевим екраном.
- оскільки найбільш поширеним способом впливу зловмисників на корпоративні мережі з метою копіювання важливої інформації є використання шкідливих посилань, необхідно встановити на браузері комп'ютерів підприємства заборону переходити на неперевірені чи шкідливі посилання.

Таким чином, прості рекомендації, які слід дотримуватися, допоможуть підприємству залишатися не тільки конкурентоспроможнім, а й підвищити комерційну ефективність.

Література

1. Ксьондз С., Яскал І., Мадей І. Концептуальні підходи до кількісного визначення іміджу підприємства. *Ефективна економіка*. 2013. № 3. С. 26-32.
2. Сизоненко В. О. Сучасне підприємництво: довідник. Київ: Знання-Прес, 2007. 440 с.
3. Міцура, О.О. Управління онлайн-репутацією: теоретичні засади та методичні підходи. *Маркетинг і менеджмент інновацій*. 2012. № 4. С. 47 – 48. URL: http://mmi.fem.sumdu.edu.ua.

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ ІНФОРМАЦІЙНИХ СИСТЕМ ПЕРСОНАЛЬНИХ ДАНИХ В ЗАХИЩЕНОМУ ВИКОНАННІ

Лисенко А.В.
Державний університет телекомунікацій,
м. Київ, Україна

Розвиток міжнародно-економічної, фінансової, банківської, культурної, правоохоронної, правової та інших форм співробітництва, що передбачає вільний рух інформаційних ресурсів щодо товарів, капіталів і послуг за умов використання інформаційно-телекомунікаційних технологій, збільшення потоків персональних даних і підтримання суверенітету держави визначають об’єктивну необхідність захисту персональних даних. Без дослідження всесвітніх міжнародних та європейських стандартів, вивчення особливостей національних регулятивних підходів окремих країн Європи, Сполучених Штатів Америки (США) та інших демократичних держав, що мають теоретичні напрацювання, розвинуте законодавство і багаторічний досвід з питань захисту прав і свобод людини, у тому числі права на захист персональних даних, украй ускладнюється розуміння сучасних проблем забезпечення відносин із захисту відомостей про особу взагалі та персональних даних громадянина зокрема.

Головною передумовою появи законодавства про захист персональних даних у європейських країнах на початку 1970-х роках було виникнення автоматизованих баз даних, розвиток телекомунікацій та потреба у забезпеченні приватного життя людини відповідно до принципів Європейської Конвенції “Про захист прав людини і основоположних свобод”

(Рим, 04. 11. 1950 р.). Більшість зарубіжних законів у сфері захисту персональних даних мають типову назву - “Закон про захист даних”.

Під захистом даних розуміють будь-які правові, організаційні, технічні (технологічні, криптографічні, програмні) засоби щодо захисту інформації персонального змісту. Для комплексного захисту даних на міжнародному рівні використовується термін “безпека даних”.

Історично відомими є дотримання двох класичних підходів при укладанні правових систем захисту персональних даних (рис. 1.), що передбачають .

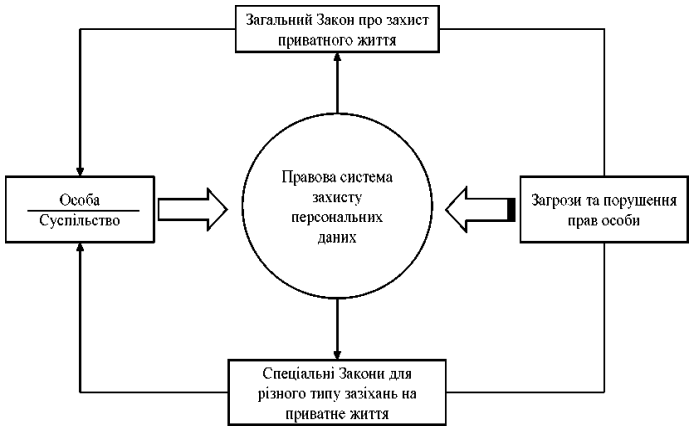


Рис. 1. Класична схема правової системи захисту персональних даних

• створення всеохоплюючого закону про захист приватного життя, що спрямований на впорядкування суспільних інформаційних відносин, пов’язаних з визначеними даними. Цей підхід веде до необхідності коригування положень закону при появі нових загроз;

• створення спеціальних законів для кожного типу зазіхань на приватне життя або для кожної сфери, що є потенційним джерелом загрози та порушень (наприклад, для засобів масової інформації, банків, телекомунікацій та ін.). У даному випадку, при виникненні нових загроз, такий підхід призводить до безсистемності, дублювання та суперечливості окремих норм права.

У практичному застосуванні обидва підходи виявили свою низьку ефективність. На даний час набутий досвід ураховується законодавцями і при створенні національних правових систем застосовують змішаний підхід, що полягає у створенні механізму забезпечення захисту персональних даних на підставі базового закону про захист персональних даних (рис. 2), а вже на його основі розробляються галузеві нормативно-правові акти.

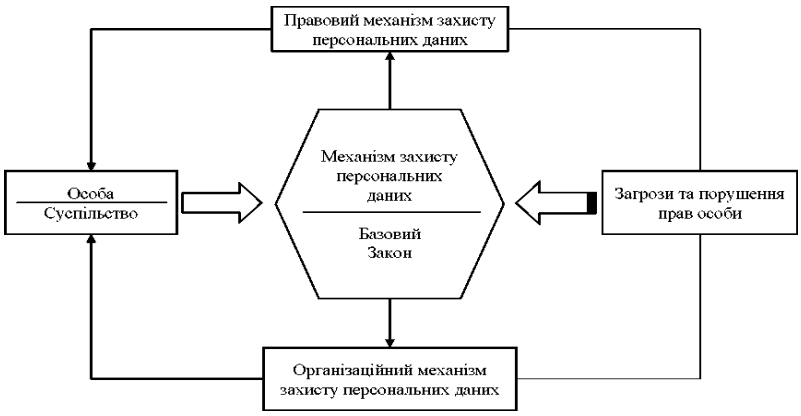


Рис. 2. Схема створення механізму забезпечення захисту персональних даних

При виникненні нових загроз та видів порушень прав особи на її персональні дані система захисту залишається незмінною, а до галузевої нормативно-правової бази вносяться необхідні доповнення та зміни. При цьому створення зазначених національних базових законів обов'язково ґрунтується на принципах захисту персональних даних, що були розроблені різними міжнародними організаціями, що представляють політико-економічні союзи та співтовариства держав, зокрема Організацію з економічного співробітництва і розвитку, Раду Європи.

ПРОВЕДЕННЯ ОЦІНКИ ЕФЕКТИВНОСТІ СУІБ

Самко В.В.
Державний Університет Телекомунікацій
м.Київ, Україна

Для підтримки достойного рівня інформаційної безпеки організації необхідно здійснювати постійне покращення системи управління інформаційною безпекою. Отже з моменту впровадження СУІБ одним з основних завдань організації є проведення оцінки ефективності її функціонування. Визначення результативності роботи СУІБ стає необхідною умовою для забезпечення та подальшого розвитку інформаційної безпеки організації.

Для оцінювання ефективності системи управління інформаційною безпекою(СУІБ) потрібно провести вимірювання ефективності використаних, діючих методів та засобів контролю і керування інформаційною безпекою(ІБ).

Але для здійснення такого оцінювання спочатку потрібно обрати метрику. Підходяща метрика повинна бути однозначною, простою в оцінюванні, зрозумілою усі учасникам процесу оцінювання та зокрема приймаючому рішення керівнику.

Для правильного визначення метрик потрібно обрати цілі, ступінь досягнення яких планується оцінювати. Обрані метрики можна за необхідності переводити в інші метрики для розуміння усіма учасниками процесу. Як правило кінцеві метрики представлені у звітах мають кількісний характер і направлені на визначення фінансової вигоди отриманої від функціонування СУІБ. Такий підхід до обрання метрик особливо ефективний у разі участі в оцінці СУІБ вищого керівництва організації. Також обрані метрики можуть бути якісними(суб'єктивними) з метою розуміння усіма учасниками процесу оцінки, або використані у поєднанні з кількісними[1, с. 10].

Після обрання метрики починається оцінка ефективності СУІБ яка є неперервним процесом, що повинен здійснюватися постійно під час її функціонування. Здійснення неперервного моніторингу ефективності СУІБ дозволяє вчасно реагувати на зміни та проблеми і вирішувати їх забезпечуючи, ще один невід'ємний процес функціонування СУІБ - постійне покращення.

Отже для оцінювання СУІБ потрібно у процесі її функціонування здійснювати збір та аналіз даних. Основними джерелами даних для оцінювання ефективності СУІБ вважають:[2, с. 22].

- результати аналізу та оцінювання ризиків;
- результати внутрішніх чи зовнішніх аудитів;
- документована інформація про події у системі;
- дані про інциденти ІБ;
- результати тестувань на проникнення;
- дані про процедури та процеси ІБ організації.

Дані з цих джерел повинні бути проаналізовані, зведені разом для отримання відповідної оцінки ефективності роботи СУІБ та надання інформації для планування

майбутнього розвитку СУІБ. У результаті аналізу організація визначає різницю між очікуваними та отриманими результатами. Знайдені невідповідності вказують на необхідність покращення реалізованої СУІБ[3]

Згідно ISO/IEC 27001 керівництво організації повинно приймати участь в оцінюванні ефективності СУІБ і здійснювати керуючу функцію тобто: затверджувати метрики, строки здійснення оцінювань, методи проведення робіт. Залежно від аналізу отриманих даних керівництво може прийняти рішення про необхідність введення змін в СУІБ. У разі виявлення невідповідностей або суттєвих ризиків ІБ керівництво визначає рішення щодо виправлення ситуації та при можливості покращення СУІБ[3].

У результаті проведення аналізу ефективності СУІБ очікується: перегляд отриманих результатів керівництвом, визначення рівня ефективності управління ІБ в організації та результативності роботи СУІБ, аналіз ризиків ІБ та переоцінка існуючих, прийняття рішень щодо подальшого розвитку СУІБ.

Література

1. Метрики оцінювання ефективності СУІБ С. 1-26, URL:https://docplayer.ru/34817016-Ocenka-effektivnosti-sistemy-upravleniya-ib.html
2. Atsec information security. Проведення оцінки ефективності ІБ, С. 20-23 URL: http://www.atsec.cn/downloads/documents/ISMS-Implementation-Guide-and-Examples.pdf
3. ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement.

ОЦІНЮВАННЯ СТАНУ ЗАХИЩЕНОСТІ ПІДПРИЄМСТВА ВІД ЗАГРОЗ КІБЕРБЕЗПЕЦІ

Кукшин Д.В.
Державний університет телекомунікацій
м. Київ, Україна

Інформаційна безпека підприємства (ІБП) є одним з видів безпеки, яка забезпечується за допомогою організаційно-технічної підсистеми захисту інформації (СЗІ), що входить до складу системи комплексної безпеки (СКБ) підприємства. Інформаційна безпека (за визначенням) - це стан захищеності інформаційного середовища підприємства від зовнішніх і внутрішніх загроз, що забезпечує її формування, використання і розвиток в інтересах як підприємства окремо, так і суспільства в цілому [2].

Під забезпеченням інформаційної безпеки підприємства в статті мається на увазі взаємозалежне вирішення двоєдиного завдання: з одного боку, захист інформації від її руйнування і несанкціонованого поводження з нею, з іншого - захист людей і інформаційно-керуючих систем від руйнівного впливу інформації.

На практиці основна увага в плані забезпечення інформаційної безпеки підтриємства приділяється переважно першої зі згаданих на початку складових проблем, тобто захисту інформації, квалифицируемой її власником (державою, юридичною особою, групою фізичних осіб або окремим фізичною особою) як об'єкт захисту від зовнішніх і внутрішніх загроз безпеки. В окремих випадках до об'єкта захисту можуть бути віднесені також носій інформації або інформаційні технології.

Технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації [2].

Обов'язкова умова вирішення проблеми забезпечення інфорамційної безпеки підприємства - централізоване управління, яке передбачає:

- координацію дій структурних підрозділів підприємства з реалізації наміченого плану забезпечення безперебійного живлення,
- зосередження сукупності корпоративних ресурсів підприємства на вирішенні завдань, передбачених зазначеним планом;
- контроль за своєчасністю та повнотою виконання плану.

Перелік завдань, що підлягають вирішенню для забезпечення інформаційної безпеки, можна визначити наступним чином:

- захист законних прав та інтересів підприємства юридичними, інноваційними та іншими методами;
- моніторинг стану обстановки (зовнішнього оточення підприємства) на основі довідкових, статистичних та інших матеріалів, а також вивчення партнерів і конкурентів підприємства;
- ідентифікація потенційних загроз ІБП і вироблення превентивних заходів щодо попередження інформаційних та інших ризиків;
- захист інформації обмеженого доступу, а також інформації, що становить комерційну, службову, професійну та інші види таємниці;
- охорона матеріальних носіїв, які містять захищається інформацію, а також технічних засобів її обробки та зберігання;
- профілактика і припинення можливої протиправної діяльності персоналу підприємства в збиток джерела безперебійного живлення,
- підготовка і проведення акцій, що поліпшують імідж і підвищують ділову репутацію підприємства в очах партнерів, органів державної влади та місцевого самоврядування [3].

Оцінка (оцінювання) стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі – оцінка стану захищеності) – сукупність заходів, спрямованих на виявлення загроз державним інформаційним ресурсам та запобігання несанкціонованим діям щодо інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;

Оцінка стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності проводиться згідно з річним планом, який затверджується наказом Адміністрації Держспецзв'язку, або позапланово.

Планова оцінка стану захищеності проводиться в державних органах, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності не частіше ніж один раз на п'ять років.

Витяги з річного плану надсилаються до вказаних у ньому державних органів, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності щороку до 01 лютого.

Позапланова оцінка стану захищеності проводиться в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності за їх безпосередніми зверненнями та рішенням Голови Держспецзв'язку або його заступника за напрямом діяльності згідно з розподілом функціональних обов'язків [1].

Отже, інформаційна безпека функціонально небезпечного підприємства, що забезпечується підсистемою захисту інформації в складі системи комплексної безпеки, досягається на основі здійснення наступного комплексу заходів:

- формування організаційно-технічної структури інформаційної безпеки підприємтва, орієнтованої на проведення правових, організаційних, технічних та програмно апаратних засобів захисту інформації та прав на неї;

- орієнтація на переважне використання сучасних методичних підходів і технологічних рішень для захисту інформації;
- централізована координація заходів щодо вдосконалення структури інформаційної безпеки підприємтсва та послідовне зосередження зусиль на їх вирішенні;
- дотримання принципів законності, розумної достатності і адаптивності до змін обстановки.

Ігнорування з тих чи інших кон'юнктурних міркувань будь-якого із зазначених положень призводить до зростання ймовірності того, що підприємство втратить почуття перспективи і не досягне бажаних результатів в стабільності свого розвитку.

Література

1. Закон України «Про захист інформаціїї в інформаційно-телекомунікаційних системах» URL https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
2. Наказ «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в іноформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» URL: https://zakon.rada.gov.ua/laws/show/z0090-15#Text
3. Журавель М. Ю., Полозова Т. В., Стороженко О. В. Формування системи показників оцінки рівня інформаційної безпеки підприємства. *Вісник економіки транспорту і промисловості.* 2011. № 33. С. 171-177.

АНАЛІЗ ТЕХНОЛОГІЙ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ВЕБ-РЕСУРСІВ ПІДПРИЄМСТВА

Самосюк В.В.
Державний університет телекомунікацій
м. Київ, Україна

Веб-сайти містять велику кількість конфіденційну інформацію. На веб сайтах можливо знайти персональні дані такі як адреси електронної пошти, імена, дата народжень, номері кредитних карт тощо. Сьогодні, захист інформаційного приватного життя є в більшості інформаційних інструкцій яких потрібно дотримуватись. У сучасному бізнесі веб-технології набули величезну популярності. Більшість сайтів великих компаній являють собою набір додатків, які інтерактивні, на веб сайтах є засоби персоналізації, засоби взаємодії із клієнтами: інтернет-магазини, дистанційне банківське обслуговування, засоби інтеграції із внутрішніми корпоративними додатками компанії, тому для зберігання в цілісності цих активів, щорічно компанії витрачають величезні гроші на пошук і усунення вразливостей у своїх веб-проектах.

Безпека веб-сайту дуже важлива, тому що хакери нападають принаймні на 50000 веб-сайтів щодня. Напади на веб сайти відбуваються на компанії будь-якого розміру. Приблизно 43% нападів відзначають підприємства малого бізнесу.

Деякі уразливості веб сайтів відомі тільки теоретично, інші ж можуть активно використовуватися при наявності програмного коду, який використовує уразливість сайту й застосовується для проведення атаки на систему. Уразливості веб-додатків набагато простіше виявити, ефективніше використовувати й при цьому сховати свою присутність. Уразливості можуть експлуатуватися не тільки з інтернету, але й зсередини (внутрішній порушник). Веб-уразливості сьогодні перевершують по кількості й зв'язаним ризикам будь-які інші проблеми інформаційної безпеки. Більшість зовнішніх атак на корпоративні інформаційні системи націлені саме на уразливості веб-додатків. Якщо усередині мережі веб сайт є доступним зловмисникові, йому набагато простіше втілити свої наміри.

Щоб переконатися, що веб-додаток є безпечним, необхідно визначити всі проблеми безпеки й уразливості в самому веб-додатку, перш ніж зловмисник ідентифікує й використовує їх. Дуже важливо регулярно виконувати процес виявлення вразливостей веб-додатка протягом життєвого циклу розробки програмного забезпечення, а не тільки в процесі експлуатації. Тестування на ранніх стадіях розробки має першорядне значення, оскільки надалі може бути дуже складно або зовсім неможливо забезпечити безпеку додатка, а потрібно буде переписати його. Чим раніше безпека веб-додатка буде включена в проект, тим більше безпечним буде веб-додаток і тем дешевше й простіше буде усунути виявлені проблеми на більш пізньому етапі. Існує кілька технологій виявлення вразливостей у веб-додатках: автоматичне сканування й ручний пошук вразливостей. Кращого з них не існує — кожний має свої плюси й мінуси. Автоматичний сканер виявить технічні уразливості, але не ідентифікує логічні уразливості, які можна визначити тільки за допомогою ручного аудиті. Ці типи вразливостей не можуть бути ідентифіковані за допомогою автоматичного інструмента. Автоматичне сканування завжди повинне супроводжуватися ручним аудитом. Також при ручному аудиті завжди залишаються незнайдені уразливості, є ймовірність людської помилки й появи нових вразливостей у процесі аудита. Інформація про слабкі місця веб-сайту у відповідності стандартам OWASP, може бути, знайдена в вразливостях внесених у Базу даних. Користувачі можуть управляти цією базою даних додаючи нові уразливості, обновляючи або виключаючи їх з бази даних.

Література

1. George Mutune. Top 10 Website Security Practices for 2021. - URL: - https://cyberexperts.com/website-security-practices/
2. Nguyen Duc Thai, Nguyen Huu Hieu. An Improving Way for Website Security Assessment. REV Journal on Electronics and Communications, Vol. 10, No. 1–2, January–June, 2020. – URL: - An Improving Way For Website Security Assessment | Nguyen | REV Journal on Electronics and Communications (rev-jec.org)
3. Top 10 Web Anplication Security Risks. - URL: https://owasp.org/www-project-top-ten/

ПОМСТА ЧИ ВИПАДКОВІСТЬ: ЧОМУ СПІВРОБІТНИКИ “ЗЛИВАЮТЬ” КОНФІДЕНЦІЙНУ ІНФОРМАЦІЮ КОМПАНІЇ

Вовк Н.І.
Державний університет телекомунікацій
м. Київ, Україна

Розвиток і успішне функціонування підприємництва передбачає забезпечення ефективної системи інформаційної безпеки. Безпека, пов'язана з персоналом, вважається домінуючою по відношенню до інших елементів системи безпеки підприємства, оскільки саме персонал має безпосередній доступ до конфіденційної і критично важливої інформації, яка забезпечує конкурентоспроможність підприємства [1]. У зв'язку з цим аналіз загроз і розробка заходів щодо зниження рівня впливу персоналу на інформаційну безпеку підприємства є надзвичайно актуальними напрямами в сучасних умовах.

На сьогоднішній день більша частина загроз інформаційної безпеки підприємства виходить від працівників, підрядників або ділових партнерів, які мають легітимний доступ до даних, інформаційних систем і баз даних підприємства. Теоретично, кожна з перерахованих вище груп користувачів може використовувати наданий доступ для фальсифікації, знищення або крадіжки секретної інформації, що в результаті призведе до серйозних негативних наслідків і послабить поточний стан підприємства по відношеню до конкурентів.

Як свідчать результати дослідження, яке провели Ponemon Institute і компанія Fasoo, недбалість співробітників - головна причина витоку конфіденційної інформації підприємства. Саме вона - причина більше ніж половини інцидентів (56%). У 37% випадків витік відбувається в результаті втрати або крадіжки пристрою. 35% інцидентів пояснюється помилкою третьої сторони. Лише в 22% випадків витік конфіденційної інформації відбувається з вини зловмисників, які не пов'язані з компанією[2].

До найбільш поширених внутрішніх загроз відносяться крадіжка, зараження інформації вірусами, або псування файлів персоналом компанії. До причин внутрішніх загроз відносяться:

– чинники психологічного характеру у зв'язку з відносинами між співробітниками підприємства, що не склалися;

– незадоволення рівнем заробітної плати;

– неблагополучні відносини між співробітником та керівництвом компанії;

Психологи стверджують, що близько 25 % всіх працівників підприємств розголошують інформацію, продають або передають її конкуруючим компаніям задля додаткового заробітку.

Інсайдерські загрози можна розділити на дві категорії: зловмисні та ненавмисні.

Зловмисні загрози можуть бути викликані негативними емоціями: якщо інсайдер пригнічений, розчарований або злий через ситуацію, що стосується підприємства чи робочого місцях [3].

Також причиною злого умислу працівників часто стають матеріальні чинники. Фінансова вигода є, мабуть, найпоширенішою мотивацією для зловмисного інсайдера. Співробітники всіх рівнів усвідомлюють, що корпоративні дані та конфіденційна інформація мають цінність. Ця загроза, ймовірно, є найбільш високим ризиком у нинішніх умовах[4]. Пандемія коронавірусу спричинила фінансовий тиск на мільйони людей.

Причинами ненавмисних загроз є відсутність знань у професійній сфері, тобто коли інсайдер є технічно не обізнаним, а також халатність, безвідповідальне ставлення до виконання своїх обов'язків. Халатність є дуже поширеною причиною інсайдерських загроз, що коштує компаніям у середньому 4,58 млн доларів на рік. Така загроза, як правило, виникає внаслідок того, що співробітники нехтують правилами інформаційної безпеки: невдалого входу / виходу з корпоративних систем, запису чи повторного використання паролів, використання несанкціонованих пристроїв чи програм.

Таким чином, потрібно пам'ятати, що сьогодні без належного захисту інформації витік корпоративних даних з вини співробітників компанії є значно легшим способом скомпрометувати інформацію, аніж з вини зовнішніх порушників. Оскільки персонал підприємства, як правило, має більші можливості доступу до важливих даних, обізнаний у процесах, які відбуваються на підприємстві та в його інформаційній політиці, а також може знати всі прогалини захисту інформаційно-комунікаційного забезпечення діяльності підприємства.

Література

1. Морозова А. М. Кадровая безопасность в системе обеспечения экономической безопасности предприятия. Международный журнал гуманитарных и естественных наук. 2018. № 3. С. 213–216. URL: http://intjournal.ru/kadrovaya-bezopasnost-v-sisteme-obespecheniya-ekonomicheskoj-bezopasnosti-predpriyatiya/

2. Эволюция угроз и стратегии защиты. URL: https://habr.com/ru/company/smart_soft/blog/304764/

3. The Primary Factors Motivating Insider Threats. URL: https://www.observeit.com/blog/primary-factors-motivating-insider-threats/

4. Mapping the motives of insider threats. URL: https://www.helpnetsecurity.com/2020/09/08/mapping-the-motives-of-insider-threats/

СЕРТИФІКАЦІЙНІ ПРОГРАМИ ДЛЯ ФАХІВЦІВ З УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Мужанова Т.М., к.держ.упр., доц., Шафаренко М.І.
Державний університет телекомунікацій
м. Київ, Україна

Сучасний ринок праці у сфері IT та інформаційної безпеки потребує висококваліфікованих фахівців, які мають володіти відповідним набором вмінь та навичок, а не тільки теоретичними знаннями. Сьогодні роботодавці часто вимагають від фахівця з інформаційної безпеки наявність сертифікатів про закінчення курсів практичного спрямування, серед яких найбільш популярними і затребуваними є сертифікати CISSP, CISM та CISA.

Сертифікований професіонал з безпеки інформаційних систем - Certified Information Systems Security Professional (CISSP) - це незалежна сертифікація з інформаційної безпеки від некомерційної організації International Information Systems Security Certifications Consortium (ISC). Перші сертифікати за цією програмою були видані у 1991 році, і на сьогодні в усьому світі понад 147 тис. спеціалістів є діючими CISSP [3].

Фахівець з безпеки IT, який володіє сертифікатом CISSP, повинен дуже добре орієнтуватися в усіх сучасних течіях інформаційної безпеки і, в першу чергу, в галузі менеджменту інформаційної безпеки. Здобувач повинен вміти мислити категоріями «вразливість», «ризик», «контрзахід». Корисним буде досвід адміністрування засобів захисту інформації або злому комп'ютерних мереж. Здобувачу сертифікату потрібно розуміти, що стоїть за абревіатурами RFID, NIPS, RBAC, DIAMETER, IKE, ESP, LLC, MTPD, IDM, XSS, які використовують алгоритми шифрування, хешування тощо.

Обсяг знань CISSP відповідає обсягу знань молодого фахівця, який з хорошими оцінками закінчив профільну кафедру і має кілька років реального досвіду в інформаційній безпеці в серйозній організації.

Дві інші сертифікаційні програми CISM та CISA **були розроблені Асоціацією аудиту і контролю інформаційних систем (Information Systems Audit and Control Association – ISACA). ISACA** є всесвітньовідомою організацією з розробки методологій та стандартів у галузі управління, аудиту і безпеки IT. Асоціація об'єднує понад 165 тис. членів у 180-ти країнах, є співавтором поширеного у всьому світі стандарту з IT-управління CobiT, а також учасником багатьох інших методологічних проектів у сфері IT [1].

Сертифікація CISA (Сертифікований аудитор з інформаційної безпеки) досить високо цінується в усьому світі, однак не так поширена на пострадянському просторі. У лінійці сертифікації ISACA сертифікат CISA є першою сходинкою на шляху до CISM, який вже є визнаною і часто обов’язковою вимогою для серйозних керівників підрозділів IT або інформаційної безпеки.

Володар сертифікату CISA повинен не тільки добре орієнтуватися в галузі інформаційної безпеки, але і в IT-менеджменті, життєвому циклі інформаційних систем, і в тому, як це все перевіряти на відповідність кращим світовим практикам. В ідеалі здобувачеві даного сертифікату треба мати досвід роботи в одній з компаній великої четвірки (BIG4: EY, PWC, KPMG, Deloitte) або у великій компанії, в якій є повноцінна група або відділ IT-аудиту.

CISM (Сертифікований менеджер з інформаційної безпеки) – це незалежна і найпрестижніша сертифікація управлінців у сфері інформаційної безпеки, яка визнана на державному рівні у багатьох країнах світу. Якщо володарем CISSP може бути недавній випускник вищого навчального закладу, який уміє працювати з апаратним та програмним забезпеченням, і лише уявляє, що таке менеджмент, то сертифікат CISM призначений для фахівців, що займаються менеджментом в галузі інформаційної безпеки не один рік.

Поява сертифіката CISM викликана потребою у вузько направленому навчанні фахівців-управлінців і дозволяє пов'язати інформаційну безпеку зі стратегією розвитку бізнесу компанії. Програма CISM включає чотири тематичні управлінські блоки: управління інформаційною безпекою, управління ризиками інформаційної безпеки, управління програмою інформаційної безпеки, управління програмою управління інцидентами інформаційної безпеки.

Варто відзначити, що сертифікацію CISM необхідно підтверджувати за допомогою постійного професійного навчання (не менше 120 годин навчання кожні 3 роки і не менше 20 годин на рік) за схваленими ISACA програмами. Загалом сертифікація CISM оцінюється як одна з кращих для управлінців, які працюють в галузі забезпечення інформаційної безпеки.

Відповідно до статистики ISACA сьогодні понад 151 тис. осіб є сертифікованими аудиторами з інформаційної безпеки (CISA) і понад 56 тис. фахівців пройшли сертифікацію як менеджери з інформаційної безпеки (CISM) [2].

Отже, фахівці з управління інформаційною безпекою для підтвердження своєї професійної кваліфікації можуть пройти незалежну сертифікацію від визнаних міжнародних експертних організацій. Найбільш популярними і затребуваними є сертифікати CISSP, CISM та CISA, які забезпечують здобувачам оволодіння необхідним набором знань, умінь та навичок у сфері управління інформаційною безпекою.

Література

1. About ISACA. URL: http://www.isaca.org.ua/index.php/homepage/about
2. CISM certification holders URL: https://www.isaca.org/ credentialing/ certifications CISSP Member Counts. URL: https://www.isc2.org/About/Member-Counts
3. Дорофеев А. Сертификаты CISSP, CISA, CISM. URL: https://habr.com/ru/ company/ npoechelon/blog/320748/

СПОСОБИ ВИКОРИСТАННЯ КІБЕРПРОСТОРУ ДЛЯ ШАХРАЙСТВА ТА ВІДПОВІДНІ МЕХАНІЗМИ ЗАХИСТУ

Дудко В.В.
Державний університет телекомунікацій
м. Київ, Україна

Кіберполіція повідомлює що:

«Повідомлення про шахрайські дії в інтернеті становлять 80 % від усіх звернень громадян. Найбільш розповсюдженими видами шахрайства у віртуальному просторі є продаж неіснуючих товарів, а також фішингові онлайн-магазини. Загалом із початку цього року кіберполіція зареєструвала понад 32 тисячі звернень громадян. Найчастіше злодії ошукують громадян, продаючи неіснуючі товари на майданчиках оголошень або у соцмережах. Як правило, у таких випадках головна умова купівлі – повна переплата за товар. Ще одна поширена схема шахраїв – створення фішингових ресурсів, які ззовні схожі на популярні інтернет-магазини. Сплачуючи на таких сайтах, покупець не лише залишається без бажаного товару, а й «передає» дані банківської картки аферисту», – йдеться в повідомленні.

Об’єктом кіберзлочинів може стати будь-який користувач інтернету.

Найпоширенішими видами таких злочинів є:

1. Кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»).

2. Фішинг – вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі.

3. Вішинг – вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки.

4. Онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

5. Піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті.

6. Кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного TV.

7. Соціальна інженерія – технологія управління людьми в Інтернет-просторі.

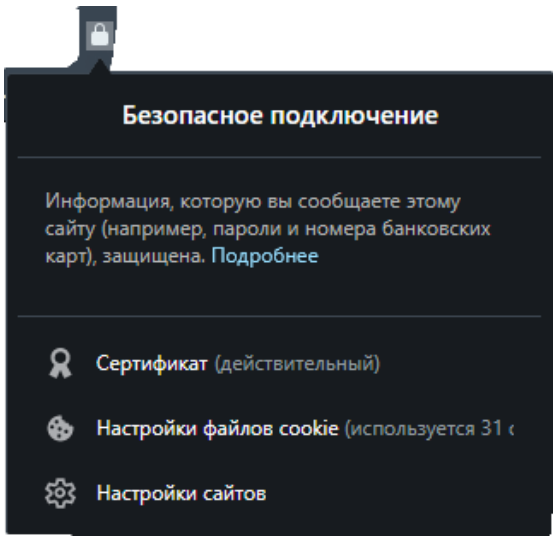
8. Мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення.

9. Протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

10. Рефайлінг – незаконна підміна телефонного трафіку.

Основні способи як захистити себе від інтернет шахрайства:

1. В першу чергу створення надійних паролів в сервісах якими ви користуєтесь і періодично їх змінювати (також пароль не повинен бути простим наприклад дата вашого народження і не повторювати однотипні паролі на всіх сайтах якими ви користуєтесь);
2. захист пристроїв, встановлення антивірусних програм;
3. використання захищених мереж;
4. не завантажувати файли з невідомих інтернет ресурсів



Література

1. https://uk.wikipedia.org/wiki/Безпека_мережі
2. https://cybercalm.org/novyny/yak-bezpechno-zavantazhuvaty-fajly-z-internetu-porady-korystuvacham/
3. https://www.gurt.org.ua/articles/34602/
4. https://uk.wikipedia.org/wiki/Комп’ютерне_шахрайство

ЗАВДАННЯ СЛУЖБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗАБЕЗПЕЧЕННІ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА

Матюх В.Ю.
Державний Університет Телекомунікацій
м. Київ, Україна

В умовах постійної зміни умов діяльності підприємств, інформаційного середовища, впливу внутрішніх і зовнішніх факторів необхідним є формування ефективної системи забезпечення інформаційної та кібербезпеки підприємства, удосконалення методів запобігання і протидії кібератакам, формування кіберстійкого бізнес-середовища.

Завдання щодо забезпечення кіберстійкості, яка допомагає бізнесу підготуватися, запобігти, відреагувати і успішно відновитися після кібератак і, таким чином гарантувати безперервність своєї бізнес-діяльності, покладаються на службу інформаційної (кібер) безпеки.

Метою створення служби інформаційної безпеки є організаційне забезпечення інформаційної та кібербезпеки підприємства та здійснення контролю за функціонуванням його інформаційно-телекомунікаційних систем.

Основними завданнями служби інформаційної безпеки є:

- управління інформаційною безпекою та забезпечення відповідності нормативним вимогам;
- оцінка операційних ризиків інформаційній безпеці підприємства;
- стратегічне планування розвитку інформаційної безпеки підприємства;
- вибір групових рішень у сфері інформаційної безпеки;
- забезпечення класифікації критичних інформаційних активів;
- контроль за безпекою корпоративної мережі підприємства;
- централізований моніторинг і запобігання несанкціонованого доступу до критичних інформаційних активів;
- управління доступом до корпоративних ІТКС;
- контроль виконання стратегічної програми розвитку інформаційної безпеки бізнес-підрозділами підприємства;
- розробка політик і стандартів інформаційної безпеки підприємства;
- моніторинг подій безпеки та реагування на інциденти та інші.

Сьогодні за умов пандемії, зростання обсягів дистанційної роботи та появи нових видів кіберзагроз завдання служби інформаційної безпеки постійно трансформуються і включають такі нові напрями:

- моніторинг кібератак та нових вірусів в світі, які можуть бути використані проти підприємства, аналіз загроз та визначення рівня критичності внутрішніх активів;
- встановлення та налаштування програм або засобів на виявлення загроз або швидшого реагування на інциденти та виявлення несанкціонованого проникнення шкідливого програмного забезпечення;
- захист співробітників на віддаленій роботі та хмарних додатків шляхом автоматизованої паспортної системи безпеки;
- використання додатків, призначених для фільтрації спамових і фішингових електронних листів;
- налаштування локального або хмарного програмного забезпечення, яке розміщується між користувачами хмарних сервісів і хмарних додатків і відстежує всі дії та забезпечує дотримання політики безпеки під час використання хмарних послуг, наприклад CASB (Cloud access security broker);

- встановлення індивідуального рівня захисту до різного роду даних та встановлення правильних пріоритетів, класифікація даних за значимістю перед налаштовуванням технологій безпеки;
- проводження комплексного аудиту інформаційної безпеки.

Таким чином, служба інформаційної безпеки підприємства сьогодні виконує не тільки традиційні завдання із забезпечення корпоративної інформаційної безпеки, але й використовує інноваційні методи і засоби з метою запобігання, протидії та реагування на кіберзагрози.

Література

1. Gartner дала рекомендации по информационной безопасности: топ-10 задач для компании. URL: https://www.tadviser.ru
2. Борсуковський Ю.В. Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Кібербезпека: освіта, наука, техніка. 2020. № 4(8). С. 34-48.

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ ЕФЕКТИВНОГО ЦЕНТРУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

Унучко Д.В.
Державний Університет телекомунікацій
м. Київ, Україна

У сучасному світі інформація є важливим джерелом, а її безпеку і правильне використання – одна з основних задач розвитку організації і виробництва і зниження рівня різних ризиків. Найважливіший актуальне питання для підприємства – інформаційна безпека.

Інформаційна безпека дозволяє організаціям і підприємствам захищати цифрову і аналогову інформацію. Вона забезпечує покриття криптографії, мобільних обчислень, соціальних мереж, інфраструктури і мереж, включаючи приватну, фінансову і корпоративну інформацію. Кібербезпека захищає як необроблені, так і важливі дані, але тільки від інтернет-загроз.

Організації приділяють велику увагу питанням інформаційної безпеки з багатьох причин. Основна мета інформаційної безпеки – забезпечити конфіденційність, цілісність і доступність інформації про підприємство. Оскільки вона охоплює безліч областей, то часто включає різні реалізації безпеки, включаючи безпеку програмного забезпечення, безпеку інфраструктури, криптографію, реагування на інциденти, управління уразливими і відновлення після збою.

Інформаційна безпека, являє собою набір інструментів і методів, використовуваних для захисту цифрової та аналогової інформації. Вона охоплює широкий спектр IT-областей, включаючи мережеву інфраструктуру і безпеку, аудит і тестування. Система інформаційної безпеки використовує такі інструменти, як аутентифікація і дозволу, щоб обмежити доступ неавторизованих користувачів до приватної інформації. Ці заходи допоможуть запобігти збитку від крадіжки, зміни або втрати інформації.

Кібер- та інформаційна безпека охоплюють різні цілі і напрямки, але також мають загальні характеристики. Інформаційна безпека – це більш широка категорія захисту, яка охоплює криптографію, мобільні обчислення і соціальні мережі. Вона займається інформаційною безпекою, яка використовується для захисту інформації від загроз, які пов'язані з людиною, таких як збої серверів або стихійні лиха. У свою чергу, кібербезпека

охоплює тільки інтернет-загрози і цифрові дані. Крім того, кібербезпека забезпечує захист необроблених і неконфіденційну даних на відміну від інформаційної безпека [1].

Створення ефективної стратегії інформаційної безпеки вимагає використання різних інструментів і технологій. У більшості стратегій використовується комбінація наступних технологій:

- Брандмауери – це рівень захисту, який можна застосовувати до мереж або додатків. Ці інструменти дозволяють фільтрувати трафік і передавати дані про трафік в системи моніторингу і виявлення. Брандмауери часто використовують встановлені списки і політики дозволу або заборони, які визначають дозволену швидкість або обсяг трафіку;
- Рішення для управління інцидентами і подіями безпеки SIEM дозволяють витягати і зіставляти інформацію з різних систем. Таке агрегування даних дозволяє групам більш ефективно виявляти загрози, краще управляти попередженнями і забезпечувати кращий контекст для розслідувань. SIEM також корисні для реєстрації системних подій або для звітів про події і продуктивності. Потім ви можете використовувати цю інформацію для перевірки або оптимізації конфігурацій.
- Стратегії запобігання втрати даних (DLP) включають інструменти і методи, які захищають дані від втрати або зміни. Це включає в себе класифікацію даних, резервне копіювання даних і відстеження обміну даними всередині і за межами організації.
- Система виявлення вторгнень (IDS) – це інструменти для моніторингу вхідного трафіку і виявлення загроз. Ці інструменти вимірюють трафік і попереджають про випадки, які здаються підозрілими або небезпечними.
- Система запобігання вторгнень (IPS) – ці рішення реагують на трафік, який визначається як підозрілий або шкідливий, шляхом блокування запитів або завершення призначених для користувача сеансів. Ви можете використовувати IP-рішення для управління вхідні та вихідні дані відповідно до визначених політиками безпеки.
- User Behavioral Analytics (UBA) – ці заходи збирають інформацію про дії користувачів і порівнюють їх поведінку з базовим. Потім в рішеннях буде використовуватися цей базовий рівень для порівняння з новим поведінкою для виявлення порушень. Потім рішення ідентифікує ці невідповідності як потенційні загрози.
- Кібербезпека блокчейна – технологія, яка заснована на фіксованих транзакційних події. В технології блокчейн розподілені програми користувача мережі перевіряють справжність транзакції і підтримують цілісність.
- Заходи EDR для кібербезпеки відстежують активність кінцевих точок, виявляють підозрілу активність і автоматично реагують на погрози. Ці рішення призначені для поліпшення видимості кінцевих точок і можуть використовуватися для запобігання проникнення загроз в ваші мережі або витоку інформації. Рішення EDR засновані на механізмах безперервного збору даних про кінцевих точках, виявлення і реєстрації подій.
- Cloud Security Position Management (CSPM) являє собой набір процедур і технологій, які ви можете використовувати для оцінки безпеки ваших хмарних ресурсів. Ці технології дозволяють сканувати конфігурації, порівнювати засоби захисту з контрольними показниками і забезпечувати узгоджене застосування політик безпеки. CSPM часто надають рекомендації щодо усунення неполадок або керівні принципи, які можна використовувати для підвищення рівня безпеки [3].

Основні рекомендації щодо для підвищення рівню інформаційної та кібербезпеки на підприємстві:

- Оновлення існуючого програмного забезпечення.
- Вибирати технологічні рішення і інструменти для запобігання виникненню ризиків. В першу чергу, це рішення для синхронізації і спільної роботи.
- Визначте конфіденційні дані, що вимагають особливого захисту.
- Розгляд можливості резервного копіювання ваших даних. Це запобіжить зміна, пошкодження або видалення важливих даних компанії.

- Розробка плану дій компанії на випадок кібератаки. Це допоможе продовжити роботу і швидше стати на ноги після можливого нападу [2].

Виявлення ризиків компанії та технологічна безпека, безумовно, є дуже важливою ланкою в кібербезпеки. Але перша лінія загрози - це ваші співробітники. Тому, встановлюючи бюджет на нові послуги та представляючи їх компанії, не забувайте навчати співробітників основам кібербезпеки.

Література

1. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. «Інформаційна та кібербезпека: соціотехнічний аспект». Київ: ДУТ, 2015. 288 с
2. Цимбалюк В. Інформаційна безпека підприємницької діяльності, визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації). *Підприємництво, господарство і право*. 2004. No3. С.88-91.
3. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісн. Хмельниц. нац. ун-ту. Сер.: Екон. науки*. 2010. No 2. Т. 2. С. 32–35.

МЕТОДИ КОНТРОЛЮ ЗА ОСНОВНИМИ МЕТРИКАМИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ (ЦЕНТРУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ) ПІДПРИЄМСТВА

Святненко В.О.
Державний університет телекомунікацій
м. Київ, Україна

На сучасному етапі інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої організації.

Створення розвиненого і захищеного середовища є неодмінною умовою розвитку підприємства, в основі якого мають бути найновіші автоматизовані технічні засоби. Це пов'язано з постійно зростаючою кількістю загроз, кібератак та інших негативних факторів, що впливають на інфраструктуру підприємства.

Сьогодні ця проблема є актуальною, так як незахищеність інформації може дуже дорого обійтися для будь-якої компанії. Дуже важливо вчасно отримувати дані про загрози, уразливості, порушення та інциденти в корпоративній інформаційній системі. Це дозволить своєчасно відреагувати і усунути їх.

Вимірювання - важливий аспект інформаційної безпеки, з яким рано чи пізно стикаються всі фахівці в цій галузі. Відстеження значень метрик дозволяє вчасно виявляти проблеми і вживати заходів щодо їх усунення.

Разом з тим складання каталогу метрик - індивідуальний процес для кожної організації. При правильному підході кожна метрика служить певній меті, що залежить від ситуації, і дозволяє отримати відповіді на конкретні питання. Можна сказати, що якщо організація не знає, які метрики в області ІБ їй необхідні, вона не потребує них, так як ще не готова до проведення вимірювань.

Всі метрики поділяються на наступні розділи інформаційної безпеки:

- управління інцидентами;
- управління активами;
- управління ризиками;
- управлінням вразливостями;
- аудит информаційної безпеки;

- управління информаційною безпекою і робота з користувачами.

Для представлених метрик організаціям слід визначити періодичність вимірювання, допустимий і критичний рівні, які дозволять інтерпретувати одержувані значення, а також цільову динаміку. Залежно від змісту, що вкладається в метрику, її цільова динаміка може бути позитивною (допустиме значення вище критичного) або негативною (допустиме значення нижче критичного). До методів і засобів організаційного захисту інформації відносяться організаційно-технічні й організаційно-правові заходи, проведені в процесі створення й експлуатації системи для забезпечення захисту інформації. Ці заходи повинні проводитися при будівництві або ремонті приміщень, у яких буде розміщатися системи; проектуванні системи, монтажі й налагодженню її технічних і програмних засобів; випробуваннях і перевірці працездатності системи.

До методів і засобів організаційного захисту інформації відносяться організаційно-технічні й організаційно-правові заходи, проведені в процесі створення й експлуатації системи для забезпечення захисту інформації. Ці заходи повинні проводитися при будівництві або ремонті приміщень, у яких буде розміщатися системи; проектуванні системи, монтажі й налагодженню її технічних і програмних засобів; випробуваннях і перевірці працездатності системи.

Основні властивості методів і засобів організаційного захисту:

- обмеження фізичного доступу до об'єктів захисту та реалізація режимних заходів;
- обмеження можливості перехоплення ПЕМВН;
- розмежування доступу до інформаційних ресурсів і процесам (встановлення правил розмежування доступу , шифрування інформації при її зберіганні і передачі , виявлення та знищення апаратних і програмних закладок);
- резервне копіювання найбільш важливих з точки зору втрати масивів документів;
- перед проведенням наради необхідно проводити візуальний огляд приміщення на предмет виявлення закладних пристроїв;
- кількість осіб, що у конфіденційних переговорах має бути обмежена до мінімуму;
- вхід сторонніх осіб під час проведення наради має бути заборонений;
- повинна бути чітко розроблена охорона виділеного приміщення під час наради, а також спостереження за обстановкою на поверсі ;
- будь-які роботи в кімнаті , що проводяться поза часом проведення конфіденційних нарад, наприклад: прибирання , ремонт побутової техніки, невеликий косметичний ремонт, повинен проводитися в обов'язковій присутності працівника служби безпеки;
- після проведення наради кімната повинна ретельно оглядатися , закриватися і опечатуватися;
- між нарадами кімната повинна бути закрита і опечатана відповідальною особою;
- профілактику зараження комп'ютерними вірусами.

Основою проведення організаційних заходів є використання й підготовка законодавчих і нормативних документів в області інформаційної безпеки, які на правовому рівні повинні регулювати доступ до інформації з боку користувачів.

Література

1. Ключові метрики інформаційної безпеки. URL: https://rvision.pro/blog-posts/klyuchevye-metriki-informatsionnoj-bezopasnosti-podborka-ot-r-vision/
2. Організаційні методи захисту інформації URL: https://tzi.ua/ua/organzacjn_metodi_zahistu_nformac.html

ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Єркін В.О.
Державний університет телекомунікацій
м.Київ, Україна

В умовах бурхливого розвитку інформаційних технологій та появи все більшої кількості інформаційних загроз інформаційні ресурси та інфраструктура для їх створення, обробки, передачі поступово стають головною цінністю для підприємства, а забезпечення інформаційної безпеки стає надзвичайно важливим для успішної ділової діяльності. Враховуючи ці обставини, вивчення основних принципів організаційного забезпечення інформаційної безпеки організації є актуальним та створює наукові передумови для вирішення практичних проблем у галузі інформаційної безпеки.

Інформаційні технології визнані рушієм далекосяжних структурних змін, забезпечують швидкий прогрес країни, її політику та економіку, розвиток суспільства та процвітання його громадян. Розробка та застосування інформаційних технологій значно спрощує вирішення проблеми безробіття та зайнятості населення, збільшує можливості для самоосвіти, придбання додаткових спеціальностей, обміну корисною інформацією про діяльність у будь-якій сфері національної економіки .

Сучасні інформаційні системи та технології є засобом підвищення продуктивності та ефективності праці працівників. Забезпечення інформаційної безпеки підприємства стає все більш важливим. Це пояснюється зростанням обсягу інформації, вдосконаленням засобів її зберігання, передачі та обробки. Наявність великої кількості інформації в електронному вигляді, використання локальних та глобальних мереж створюють якісно нові загрози конфіденційній інформації.

Інформаційна безпека — захищеність (стан захищеності) основних інтересів особистості, суспільства і держави в сфері інформації, включаючи інформаційну і телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі, як повнота, об’єктивність, доступність і конфіденційність. Слід відзначити, що задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб’єктами навколишньої дійсності і як наслідок — обґрунтованість рішень та дій, що приймаються.

Таким чином, використання інформаційних технологій значно підвищує ефективність процесів, зменшує витрати на їх реалізацію, але спричинює появу нових загроз функціонуванню підприємства. Застосовуючи системний підхід до інформаційної безпеки, підприємство повинно дотримуватися принципів конфіденційності, цілісності та доступності інформації, що підвищить ефективність.

Література

1. Батюк, А. Є. Інформаційні системи в менеджменті / А. Є. Батюк, З П. Двуліт, К. М. Обельовська, І. М.Огороднік, Л. П. Фабрі.— Львів: «Інтелект-Захід», 2004.— С. 343–384
2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев - К.: ООО ТИД «ДС», 2002. – 688 с
3. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
4. Низенко Е. І., Каленяк Е.І. Забезпечення інформаційної безпеки підприємництва: навч. посіб. Київ: МАУП, 2006. 134 с.
5. Цимбалюк, В. С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті / В. С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.— 2004.— №8.— С. 30–33.

РОЛЬ КАДРОВОЇ БЕЗПЕКИ В СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Степанець В.В.
Державний університет телекомунікацій
м. Київ, Україна

Питання кадрової безпеки як складової системи забезпечення інформаційної безпеки підприємства сьогодні є особливо актуальним, адже від добре організованих та скоординованих зусиль у цьому напрямку залежить впевненість керівництва фірми в компетентності та відданості своїх працівників. З одного боку, персонал є основою успішної бізнес-діяльності, ініціатором нововведень та найбільш відданим вболівальником свого підприємства. Водночас, саме працівники є основним джерелом проблем у сфері інформаційної безпеки. Тому одним із найбільш важливих аспектів управління інформаційною безпекою підприємства є здійснення комплексу заходів, спрямованих на безпеку персоналу.

Для найму кваліфікованих та надійних працівників вже на етапі відбору служба інформаційної безпеки має взаємодіяти з менеджерами з персоналу, щоб провести всі потрібні перевірки. Основними важливими пунктами перевірки є виявлення у потенційного кандидата на вакантну посаду судимості, адміністративних стягнень або розшукових справ; проблемних кредитних історій; зв'язків у кримінальному світі, в тому числі через родичів; встановлення фактів володіння рухомим та нерухомим майном, зокрема відповідно до заявлених даних, підтвердження справжності поданих документів [3].

У процесі відбору працівників, задіяних у сфері інформаційної безпеки, кадрові служби мають володіти відповідними розширеними повноваженнями, зокрема мати безпосередній доступ до необхідних корпоративних ресурсів: планів стратегічного розвитку компанії, інформаційних масивів, зокрема конфіденційного характеру, аналітики, внутрішньофірмових і зовнішніх досліджень, фінансів на відповідні кадрові програми (залучення кваліфікованих кадрів, управління лояльністю) тощо.

У Кодексі законів про працю України зазначено ряд документів, що безпосередньо впливають на безпеку підприємства, і служба персоналу зобов'язана забезпечити їх наявність, правильність, дієвість та відсутність негативних юридичних наслідків.

Важливим завданням роботи з персоналом у контексті інформаційної безпеки є встановлення приязних і конструктивних відносин працівників з роботодавцем та керівництвом компанії. У такі заходи з метою запобіганню внутрішніх загроз традиційно вкладається мало коштів. Керівництву та кадровим службам варто приділяти достатньо уваги умовам праці персоналу, матеріальним винагородам та нематеріальній мотивації, професійному та особистісному розвитку працівників, клімату в колективі й захисту від зовнішніх загроз [1]. Саме уважність і турбота про своїх працівників матиме наслідком формування лояльного і надійного колективу і, як наслідок, позитивно впливатиме на кадрову й інформаційну безпеку підприємства.

Разом з тим, невід'ємною частиною заходів кадрової безпеки є контроль діяльності працівників. У сфері інформаційної безпеки такі заходи мають особливе значення з огляду на залучення персоналу до роботи з комерційною таємницею та іншими конфіденційними даними. Це великий комплекс заходів, котрий націлений на мінімізацію можливостей заподіяння шкоди з боку персоналу та відпрацьовується, зокрема, із використанням сучасних програмних засобів для перевірки професійних та особистих якостей працівників, у тому числі перед працевлаштуванням, оцінювання результативності роботи, а також моніторингу діяльності персоналу.

У якості прикладу варто навести програмне забезпечення компанії «MIDOT», яке використовується для оцінки персоналу, як претендентів на посаду, так і тих, що вже

працюють [4]. Особливим різновидом тестування наразі є перевірка на детекторі брехні, яку можна використовувати як для профілактики порушень інформаційної безпеки, так і для їх розкриття.

Важливу роль у забезпеченні інформаційної безпеки персоналу відіграє співпраця компанії з правоохоронними органами. Так, у США взаємодія недержавних організацій з органами правопорядку стала вже досить ефективною, а у Франції масштаби діяльності спеціальних служб в промислово-торговельних фірмах і фінансових інститутах постійно зростають [5].

Загалом, заходи кадрової безпеки є важливим і обов'язковим елементом управління інформаційною безпекою підприємства і мають забезпечувати поглиблену перевірку кандидатів на посади з інформаційної безпеки, здійснення контролю діяльності персоналу, налагодження конструктивних відносин між керівництвом і колективом компанії як засобу формування корпоративної лояльності працівників.

Література

1. Пучкова С.І. Методичні підходи щодо забезпечення кадрової безпеки підприємства. URL: http://dspace.oneu.edu.ua/jspui/bitstream/
2. Швець Н. Методи виявлення і збереження кадрової безпеки, або як перемогти зловживання персоналу. *Персонал.* 2006. No 5 URL: http://www.personal.in.ua/article.php?ida=291
3. Економічна безпека підприємств: підручник / Ортинський В.Л., Керницький І.С., Живко З.Б. та ін.; Київ: Алерта, 2011. 704 с.
4. Технологія IntegriEXIT компанії Midot. URL: https://midot.com/ukrainian/product/integriexit/
5. Леонова Г.Г., Озаріна О.В. Досвід моделювання економічної безпеки зарубіжних підприємств URL:http://nauka.kushnir.mk.ua/?p=1032

ВПРОВАДЖЕННЯ ПРОЦЕДУР МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНІСТЬ ПІДПРИЄМСТВА

Чепур Ю.І.
Державний університет телекомунікацій
м.Київ,Україна

Система управління інформаційною безпекою (Information Security Management System) є частиною загальної системи управління, що базується на аналізі ризиків і призначеної для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області інформаційної безпеки. Систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Виділяються чотири стадії реалізації системи управління інформаційною безпекою:

1. формування політики в галузі ризиків;
2. аналіз бізнес-процесів;
3. аналіз ризиків;
4. формування цільової концепції.

Формування політики в галузі ризиків передбачає визначення принципів управління ними для всього підприємства в цілому. Ці принципи базуються на цілях підприємства, його стратегії, також на вимогах, пропонованих законом і стандартами в галузі інформаційної безпеки. Чинником ефективності системи управління інформаційною безпекою є її побудова на базі міжнародних стандартів ISO / IEC 17799: 2005, ISO / IEC 27001: 2015 та COBIT 2019 [1].

Стандарт ISO 27001 носить не технічний, а управлінський характер і спрямований на впровадження процесів, що дозволяють забезпечити належний рівень інформаційної безпеки компанії. СУІБ базується на процедурі оцінки та аналізу ризиків, інтегральних показників захищеності ключових інформаційних активів і виборі заходів щодо мінімізації ризиків до прийнятного залишкового рівня. Сьогодні процедури забезпечення інформаційної безпеки мають бути інтегровані в усі критичні бізнес/операційні процеси підприємства (організації).

Проведення комплексу заходів із побудови системи управління інформаційною безпекою відповідно до вимог стандарту ISO 27001 дозволить вирішити такі завдання:

- **Підвищення рівня безпеки.** Стандарт розроблений з урахуванням кращих світових практик забезпечення інформаційної безпеки;
- **Управління.** Стандарт передбачає побудову циклічного і керованого процесу забезпечення інформаційної безпеки;
- **Оптимізація витрат**. СУІБ дозволяє оптимізувати і обгрунтувати витрати на інформаційну безпеку;
- **Ризики.** Зниження рівня фінансових ризиків, пов'язаних з інформаційною безпекою, шляхом їх ідентифікації, оцінки та прийняття адекватних захисних заходів;
- **Привабливість.** Підвищення ступеня привабливості компанії на внутрішньому і зовнішньому ринках (конкурентні переваги;
- **Довіра.** Підвищення довіри з боку акціонерів, клієнтів, партнерів і контрагентів;
- **Репутація.** Підвищення рівня ділової репутації шляхом сертифікації СУІБ, яка демонструє високий рівень зрілості компанії [2].

Література

1. Система управління інформаційною безпекою URL: https://stud.com.ua/43080/ekonomika/sistema_upravlinnya_informatsiynoyu_bezpekoyu_pidpriyemstva.
2. Побудова системи управління інформаційною безпекою (СУІБ) URL: http://unit.com.ua/ua/postroenie-sistemy-upravleniya-infor/.
3. Стандарт ISO / IEC 27001: 2015 URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf.

СЕКЦІЯ 4. ЗАСОБИ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ

СИМЕТРИЧНА КРИПТОСИСТЕМА НА ДИФЕРЕНЦІАЛЬНИХ ПЕРЕТВОРЕННЯХ ЯК НОВИЙ ЗАСІБ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ VOIP-ТРАФІКУ

Грищук О.М.
Житомирський військовий інститут імені С. П. Корольова,
м. Житомир, Україна

Безперервність та успішність бізнесу не в останню чергу залежить від доступності та безпеки абонентів, які використовують засоби VoIP-телефонії [1]. З причини збільшення кількості кіберінцидентів [2], пов'язаних з компрометацією засобів VoIP-телефонії [3, 4] бізнес все частіше потребує використання засобів безпечного шифрування [5]. Таким чином, питання безпеки VoIP-трафіку наразі є актуальним.

Існуючі на сьогодні підходи забезпечення кібербезпеки VoIP-трафіку ґрунтуються в основному на використанні засобів шифрування на основі IPSec, SSH та SRTP протоколів [3]. Основним їх призначенням є забезпечення конфіденційності та захисту від відтворення [3, 6]. Є й інші протоколи шифрованої передачі VoIP-трафіку, наприклад для службової інформації – це TLS-протокол, призначений для шифрування номерів абонентів, імен користувачів тощо [7, 8]. Поряд з тим розвиток пост-квантової криптографії [9] ставить під загрозу їх компроментації.

Одним з перспективних підходів до забезпечення конфіденційності VoIP-трафіку вважається підхід, який ґрунтується на використанні криптосистеми Фредгольма [10]. Дана криптосистема відноситься до класу симетричних криптосистем. В її основу покладено ідею шифрування та розшифрування голосових повідомлень за рахунок використання інтегрального рівняння Фредгольма першого роду [11]. В силу некоректності вирішення зворотної задачі – задачі криптоаналізу запропонована симетрична криптосистема забезпечує гарантовану криптостійкість [10].

Незважаючи на перспективність згаданого вище підходу до сьогодні й досі не розроблено алгоритм шифрування та розшифрування VoIP-трафіку. Основним проблемним питанням є складність реалізації процедури розшифрування.

Для подолання згаданого проблемного питання в роботі пропонується використовувати два взаємодоповнюючі математичні апарати. Перший математичний апарат – це диференційні перетворення академіка Г. Є. Пухова [12]. Його запропоновано використовувати для шифрування/розшифрування VoIP-трафіку в квазіреальному масштабі часу. Другий математичний апарат – це метод регуляризації академіка А. М. Тихонова. Його запропоновано використовувати для розшифрування VoIP-трафіку.

Таким чином, запропонований підхід створює наукове підґрунтя для побудови нового класу симетричних криптосистем на диференціальних перетвореннях, які можна віднести до прогресивних засобів забезпечення кібербезпеки в системах інтернет-телефонії.

Література

1. How to Know if VoIP is the Right Solution for Your Business. *Weave Communications*. 2020. URL: https://www.getweave.com/en-ca/how-to-know-if-voip-is-the-right-solution-for-your-business/.
2. Грищук Р.В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.
3. Mentsiev A., Dzhangarov A. VoIP security threats. *Инженерный вестник Дона*. 2019. №1. С. 1–7.

4. Roy O. P. A Survey on Voice over Internet Protocol (VoIP) Reliability Research / O. P. Roy, V. Kumar. // IOP Conf. Series: Materials Science and Engineering. 2020. №1020. С. 1–9.
5. Claxson N. Securing VoIP: encrypting today's digital telephony systems / Claxson. // Network Security. 2018. №11. С. 11–13.
6. Yeun Chan Yeob, and Salman Mohammed AlMarzouqi. “Practical Implementations for Securing VoIP Enabled Mobile Devices.” Network and System Security, 2009. NSS'09. Third International Conference on. IEEE, 2009. PP. 409-415.
7. Защита от прослушивания разговоров – строим безопасную SIP телефонию своими руками. *Habr*. 2015. URL: https://habr.com/ru/company/ppbbxx/blog/253073/.
8. Снежко И. Шифрование голоса в VoIP – протоколы SRTP и TLS. *3cx*. 2019. URL: https://www.3cx.ru/blog/voip-encryption-srtp-tls/.
9. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process NIST. 2020. URL: https://www.gps949.com/pdf/NIST.IR.8309.pdf.
10. Грищук Р. В. Узагальнена модель криптосистеми Фредгольма. *Кібербезпека: освіта, наука, техніка*. 2019. №4. С. 14–23.
11. Броншпак Г. Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии. *Прикладная электроника*. 2014. № 3. С. 337-349.
12. Пухов Г.Е. Дифференциальные преобразования и математическое моделирование физических процессов : монография Київ: Наук. думка, 1986. 160 с.
13. Тихонов А. Арсенин Н. В. Я.Методы решения некорректных задач. Москва: Наука: Главная редакция физико-математической литературы, 1979. 285 с.

ПРОЕКТУВАННЯ ЗАСОБУ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Ковівчак Я.В., к.т.н., доц., Дубук В.І., к.т.н., доц., Мішак Р.О.
Національний університет “Львівська політехніка”
м. Львів, Україна

В сучасних умовах життєдіяльності суспільства його функціонування пов'язане з необхідністю обробки різних видів інформації та реалізації різно-манітних інформаційних процесів.

Важливою складовою комплексної безпеки сучасного суспільства є інфор-маційна безпека.

Інформаційна складова відіграє провідну роль у процесах державотво-рення, представленні та захисті інтересів держави та суспільства в цілому.

Безпека інформації, як об'єкту життєдіяльності суспільства, має потенційні

загрози, які посягають на її цілісність, збережність, захищеність.

Ст. 17 Конституції України визначено, що: "Захист суверенітету і територі-альної цілісності України, забезпечення її економічної та інформаційної без-пеки є найважливішими функціями держави, справою всього Українського народу" [1].

Разом з цим, як справедливо зауважують автори [2], "Закріплені в Консти-туції України права громадян на недоторканість приватного життя, особисту та сімейну таємницю, таємницю листування практично не мають достатнього правового, організаційного та технічного забезпечення". "Відставання вітчизняних інформаційних технологій змушує органи державної влади та місцевого самоврядування при створенні інформаційних систем іти шляхом закупівель імпортної техніки і залучення іноземних фірм, через що підви-щується ймовірність несанкціонованого доступу до інформації, що оброб-ляється, зростає залежність України від іноземних виробників комп'ютерної і телекомунікаційної техніки та програмного забезпечення" [2, с.154, 155].

При цьому серед множини завдань із забезпечення інформаційної безпеки України та подолання негативних тенденцій у її розвитку автори [2] вказують на вимогу "розроблення сучасних методів і засобів захисту інформації, забезпечення безпеки інформаційних технологій, насамперед тих, які використ-товуються у системах керування військами та зброєю, екологічно небезпечними та економічно важливими виробництвами" [2, с.156].

Вище вказане обумовлює актуальність розробки оригінальних програмних засобів, що реалізують на практиці технології захисту інформації.

При цьому, як зауважують автори [6, с.41] одним із найкращих способів захистити інформацію - приховати факт її існування. Цей вид захисту реалізується методами, засобами та способами стеганографії.

За визначенням авторів [3, с.251]: "За допомогою стеганографії прихо-вують сам факт існування таємного повідомлення, на відміну від криптографії, метою якої є приховування вмісту повідомлень шифруванням".

На практиці стеганографію застосовують з метою: прихованої передачі інформації, захисту автентичності електронних документів з допомогою цифро-вих водяних знаків, захисту оригінальності та унікальності електронних файлів з допомогою ідентифікаційних номерів, вбудовування заголовків у електронні документи [3, с.252] та захисту підтвердження електронних документів елект-ронним цифровим підписом.

Як вказують автори з Харківського національного економічного університе-тету [4, с. 6]: "Методи стеганографії дозволяють не тільки приховано переда-вати дані (так звана класична стеганографія), але й успішно вирішувати завдан-ня завадостійкої автентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв’язку, пошуку інформації в мультимедійних базах даних і т. д."

При реалізації стеганографії завдання вкладення інформації, яку необхідно приховати у оболонку-контейнер та її витяг здійснюється засобами стегано-графічної системи.

Узагальнена структурна схема стеганографічної системи може представ-лятися структурною схемою, побудованою на основі структурної схеми, наведеної у [4, с.16].

Рис.1. Структурна схема стеганографічної системи.

Після здійснення аналізу переваг і недоліків існуючих стеганографічних програмних засобів [3, с.264, 270; 5, с.41, 42], було розроблено оригінальний програмний засіб стеганографічного захисту інформації [5, с.42].

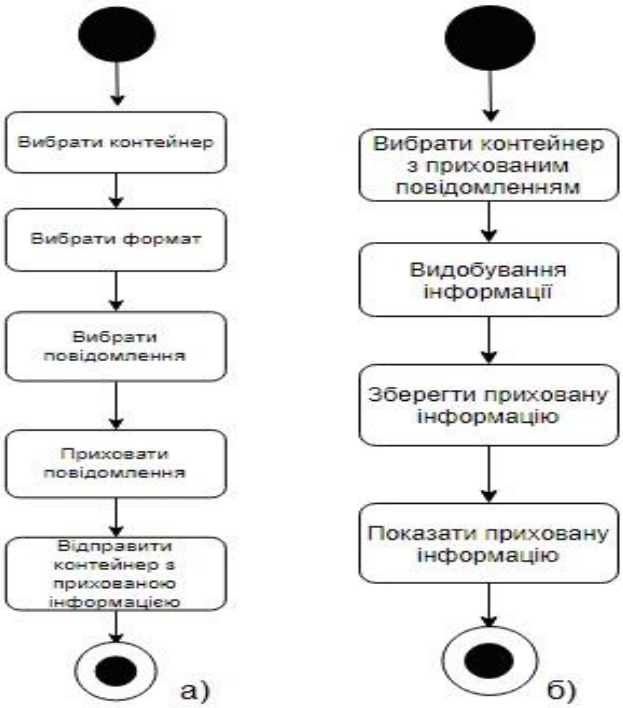


Рис.2. Діаграми діяльності для приховування (а) та витягу (б) інформації.

На рис.2а зображена діаграма діяльності приховування інформації. Щоб виконати цю операцію потрібно вибрати контейнер, в який буде виконуватись приховування. Після цього вибрати повідомлення і наступною операцією буде саме приховування. В результаті система відправить контейнер з прихованою інформацією. На рис.2б зображена діаграма витягу інформації. Користувач може витягти інформацію, в результаті дій: обрати та відправити системі контейнер з прихованою інформацією. Далі відбуватиметься витяг інформації. Після витягу зберігається прихована інформація і відображається користувачу.

У результаті було розроблено програмний засіб стеганографічного захисту інформації, з простим, зручним та зрозумілим людино-машинний інтерфейсом.

Рис.3. Графічний інтерфейс стеганографічного програмного засобу.

Розроблений програмний засіб стеганографії може використовуватися як самостійно, так і бути вбудованим у комплексну систему захисту інформації.

В перспективі проекту програмного засобу стеганографічного захисту інформації передбачається удосконалити і покращити людино-машинний інтер-фейс користувача, що підвищить його функціональність та зручність.

Література

1. Конституція України. Документ від 28.06.1996 №254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр/print
2. Дудикевич В.Б. Забезпечення інформаційної безпеки держави: навч. посіб-ник. В.Б. Дудикевич І.Р. Опірський П.І. Гаранюк В.С. Зачепило А.І. Партика. Львів: Видавництво Львівської політехніки, 2017. 204 с.
3. Бобало Ю.Я. Інформаційна безпека: навч. посібник. Ю.Я. Бобало, І.В. Горба-тий, М.Д. Кіселичник, А.П. Бондарєв, С.С. Войтусік, А.Я. Горпенюк, О.А. Нєм-кова, І.М. Журавель, Б.М. Березюк Є.І. Яковенко В.І. Отенко І.Я. Тишик./ за заг. ред. д-ра техн. наук, проф. Ю.Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.
4. Кузнецов О.О. Стеганографія: навч. посібник./ О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. Харків: Видавництво ХНЕУ, 2011. 232 с.
5. Мішак Р., Ковівчак Я. Розробка засобу стеганографічного захисту інфор-мації. *Технічні вісті*. 2020. № 1 (51), 2 (52). С. 41–42.

SIEM

Ющенко М.О.
Державний університет телекомунікацій
м. Київ, Україна

На сучасному етапі інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої організації.

Створення розвиненого і захищеного середовища є неодмінною умовою розвитку підприємства, в основі якого мають бути найновіші автоматизовані технічні засоби. Це пов'язано з постійно зростаючою кількістю загроз, кібератак та інших негативних факторів, що впливають на інфраструктуру підприємства.

Сьогодні ця проблема є актуальною, так як незахищеність інформації може дуже дорого обійтися для будь-якої компанії. Дуже важливо вчасно отримувати дані про загрози, уразливості, порушення та інциденти в корпоративній інформаційній системі. Це дозволить своєчасно відреагувати і усунути їх.

У таких випадках компаніям необхідно впроваджувати автоматизований засіб, який допоможе проаналізувати стан інформаційної безпеки. Кращим інтелектуальним рішенням на даний момент є клас рішень SIEM.

Незважаючи на свою відносну зрілість, ринок SIEM все ще зростає двозначними темпами. Основною тенденцією є все більш широке використання поведінкової аналітики та автоматизації для фільтрації менш нагальних попереджень, щоб групи безпеки могли зосередитись на найбільших загрозах. Аналітики розглядають хмару як зростаючий засіб надання послуг SIEM, як для SMB, так і для гібридних організацій, які шукають простіших способів відстежувати складне середовище.

Що таке SIEM?

Програмне забезпечення Security Information and Event Management (SIEM) надає спеціалістам інформаційної безпеки підприємства як уявлення, так і можливість відстежувати всі події, які відбуваються в їхньому IT-середовищі [1].

Технологія SIEM існує вже більше десяти років. Вона поєднує в собі управління подіями безпеки (SEM) – аналіз даних журналу та подій у режимі реального часу, щоб забезпечити моніторинг загроз, кореляцію подій, реагування на інциденти, та управлінням інформаційною безпекою (SIM), яка збирає, аналізує та звітує про дані журналу.

Як працює SIEM?

Програмне забезпечення SIEM збирає та агрегує дані журналу, згенеровані на всій технологічній інфраструктурі організації, від хостових систем і додатків до мережевих та захисних пристроїв, таких як брандмауери та антивірусні фільтри.

Після цього програмне забезпечення визначає та класифікує інциденти та події, а також аналізує їх. SIEM забезпечує дві основні цілі, які мають бути досягнуті [1]:

1) надавати звіти про інциденти та події, пов'язані з безпекою, такі як успішні та невдалі входи в систему, активність зловмисного програмного забезпечення та інші можливі зловмисні дії; та

2) надсилати сповіщення, якщо аналіз показує, що будь-яка діяльність виконується проти заздалегідь визначених наборів правил і, таким чином, вказує на потенційну проблему безпеки.

Програмне забезпечення SIEM в основному використовується великими організаціями та державними компаніями, де дотримання правил залишається найважливішим фактором використання цієї технології.

Ринок SIEM

На ринку SIEM є декілька домінуючих постачальників на основі продажів у всьому світі, зокрема IBM, Splunk та HPE. Є щонайменше ще кілька основних гравців, а саме: Alert Logic, Intel, LogRhythm, ManageEngine, Micro Focus, Solar Winds і Trustwave [2].

Прикладом SIEM є IBM QRadar. У більшості фірм IBM QRadar SIEM оцінюється високо, але складність впровадження може обмежити привабливість середніх та великих підприємств, які потребують основних можливостей SIEM, та тих, хто шукає єдину платформу, яка охоплює широкий спектр моніторингу безпеки та експлуатаційних технологій.

LogRhythm – ще один постачальник SIEM з високими рейтингами та популярністю. Цю систему легше розгортати, ніж деякі інші найпопулярніші продукти SIEM, але вона не може розширюватися, щоб підтримувати дуже великі обсяги подій. SIEM від LogRythm найкраще підходить для малих та середніх організацій, які вже мають певну функцію розвідки та аналітики загроз.

Програмне забезпечення SIEM від McAfee, можливо, відстає від IBM, Splunk та LogRhythm у загальній конкуренції SIEM, але його простота розгортання, а також інтеграція з іншими інструментами McAfee роблять його сильним конкурентом у багатьох списках SIEM.

Література

1. What is SIEM software? How it works. URL: https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html
2. Top SIEM Products. URL: https://www.esecurityplanet.com/products/top-siem-products.html

ОГЛЯД СУЧАСНИХ ЗАСОБІВ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

Запорожченко М.М.
Державний університет телекомунікацій
м. Київ, Україна

Мережева безпека являє собою набір певних вимог та політик, які стосуються інфраструктури комп'ютерної мережі організації та мають на меті попередження та моніторинг спроб отримання несанкціонованого доступу до інформації, її несанкціонованої модифікації та можливої відмови роботи всієї комп'ютерної мережі та інших мережевих ресурсів.

Зазвичай мережева безпека поділяється на три аспекти: фізичну безпеку, інженерно-технічну та організаційну. Засоби фізичного захисту необхідні для попередження отримання несанкціонованого фізичного доступу до мережевого обладнання сторонніми особами. До таких засобів можна віднести замки, біометричну автентифікацію та інші систему контролю доступу. Інженерно-технічні заходи захисту розроблені для захисту інформації, яка зберігається та передається мережею, від зовнішніх зловмисників та дій власних співробітників, які можуть порушити властивості інформації. Організаційні заходи захисту включають в себе політики безпеки, які контролюють дії користувачів, включаючи порядок їх автентифікації, надання їм прав доступу тощо.

Зазвичай стосовно мережі організації застосовуються комплексні заходи захисту. Вони можуть включати в себе міжмережеві екрани, системи виявлення та запобігання вторгнень, системи моніторингу та аналізу мережі, засоби захисту від мережевих атак, проксі-сервери та віртуальні приватні мережі.

Міжмережеві екрани, або брандмауери, є програмними або програмно-апаратними елементами комп'ютерної мережі організації, які контролюють і фільтрують весь мережевий трафік, що проходить через них, у відповідності з визначеними правилами. Вони призначені для відділення робочих станцій та серверів, які знаходяться у внутрішньому сегменті мережі організації, від зовнішніх каналів зв'язку; багатоетапної ідентифікації запитів, які надходять в мережу, та їх реєстрації; визначення можливості отримання доступу користувачем до внутрішніх ресурсів мережі, базуючись на наявних в нього повноваженнях та правах доступу; контролю цілісності даних та програмного забезпечення; економії адресного простору в мережі; приховування IP-адрес внутрішніх серверів [1].

Системи виявлення вторгнень – це програмні або апаратні засоби, які виявляють факти отримання несанкціонованого доступу до мережі або комп'ютерної системи, чи несанкціонованого управління системою. Завдяки моніторингу системою підозрілої активності можуть бути виявлені атакуючі, яким вдалося обійти брандмауер, що дозволить оперативніше вжити стосовно них певних дій.

Системи запобігання вторгнень – це програмні або апаратні системи мережевої та комп'ютерної безпеки, які виявляють вторгнення або порушення безпеки й активно блокують їх. Відмінність від систем виявлення вторгнень полягає в тому, що система запобігання вторгнень повинна відслідковувати активність в реальному часі та оперативно вживати контрзаходи щодо запобігання атак [2].

Віртуальна приватна мережа (Virtual Private Network, VPN) – це логічна мережа, яка дозволяє забезпечити одне або декілька мережевих з'єднань поверх інших мереж. VPN приймає запит користувача на себе і після цього перенаправляє його. Це значить, що трафік буде йти не від користувача, а від VPN, сервер якої може знаходитись будь-де. Це дозволить убезпечитись від стеження, блокування тощо.

Як можна побачити, існує велика кількість різноманітних засобів захисту мережі організації. Для результативного захисту рекомендується застосовувати комплекс заходів, які будуть доповнювати один одного. Це забезпечить кращий рівень стійкості мережі організації проти атак зловмисників.

Література

1. Міжмережевий екран. 2020. URL: https://tux.org.ua/mizhmerezhevij-ekran/.
2. Мєшков В.І., Віролайнен В.О. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. *Проблеми безпеки інформації в інформаційно-комунікаційних системах.* Київ: НТУУ КПІ РТФ, 2015. № 1. С. 1-4. URL: https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf

МЕТОДИ ТА ЗАСОБИ ФОРЕНЗИКИ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Жилін А.В., к.т.н., Волошин Г.В.
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"
м. Київ, Україна

У міру того, як комп'ютери, комп'ютерні мережі та обчислювальні пристрої в цілому набувають широкого поширення, ризик виникнення злочинів, пов'язаних із такими пристроями, зростає. Для виявлення слідів атак в комп'ютерних мережах, зловмисників що їх здійснюють й збору доказів щодо них, необхідно мати відповідні розроблені методики й засоби проведення слідчих дій, які прийнято називати форензикою. Наразі існують наукові праці які розкривають методології форензики в комп'ютерних мережах, але здебільшого описують роботу слідчого з юридичної точки зору. Тому постає задача щодо необхідності розробки методики проведення комп'ютерно-технічної експертизи в комп'ютерних мережах і аналізу апаратно-програмних засобів для цього.

У роботі запропоновано методику проведення та інструменти проведення криміналістичного аналізу в комп'ютерних мережах.

Одним із сервісів, які надають команди реагування на інциденти комп'ютерної безпеки CERT/CSIRT, є аналіз інцидентів, який полягає в оцінці всієї доступної інформації й додаткових доказів або артефактів, що пов'язані з інцидентом або подією. Якщо зазначені інциденти мають кримінальні ознаки, то застосовується ретельний, методичний процес проведення вже криміналістичного аналізу, який характеризується чітко прописаною процедурою та правилами його проведення. Згідно стандартів [1] та [2] експерти-криміналісти повинні бути кваліфікованими для належного поводження з цифровими доказами та повинні мати надійні технічні знання для вибору найкращих методів проведення розслідування. Адекватне та постійне навчання, а також періодичне оцінювання знань та вмінь забезпечують компетентність експертів та дають їм можливість для аналізу цифрових пристроїв, які можуть містити потенційні цифрові докази [3]. Необхідний рівень компетентності експертів-криміналістів може відрізнятися в залежності від країни. На даний момент не існує міжнародного узгодженого мінімального рівня підготовки та сертифікації спеціалістів в сфері форензики.

Тому для ефективного проведення розслідувань комп'ютерних злочинів було розглянуто моделі для проведення розслідувань та аналізу кіберзлочинів. Так, до них увійшли найбільш поширені: Digital Forensics Workshop Investigative Model (DFRWS), Abstract Digital Forensics Model (ADFM), Integrated Digital Investigation Process (IDIP), Enhanced Digital Investigation Process Model (EDIP), Computer Forensics Field Triage Process Model (CFFTPM), Digital Forensic Model based on Malaysian Investigation Process (DFMMIP).

Як результат їх аналізу й синтезу запропоновано методику проведення криміналістичного аналізу, який повинен виконати спеціаліст з комп'ютерної криміналістики під час розслідування кримінального злочину в апаратно-програмному засобі. Вона полягає у виконанні наступних кроків: визначити спосіб реалізації злому,

побудувати сценарій атаки, відновити її хронологію, зібрати решту слідів атаки, розробити необхідні заходи для запобігання подібної атаки, зменшити і відновити завдані збитки.

Для виконання цієї методики в цілому, або окремого її кроку необхідно використовувати спеціальний інструментарій, який підбирається індивідуально в залежності від поставленого завдання. До найбільш поширених можна віднести: Autopsy, Guymager, Volatility, FTKImager.

Представлена методологія та запропонований інструментарій дозволить надати можливості щодо ефективного проведення розслідувань комп'ютерних злочинів в комп'ютерних мережах та апаратно-програмних засобах.

Література

1. WSSN (World Standards Services Network). *World standards services network* 2006. URL: http://www.wssn.net/WSSN.
2. ISO (International Organization for Standardization: Standards FAQs. 2009a. URL: http://www.iso.org/iso/iso_ catalogue/faq_standards_2.htm.
3. ISO/IEC 27037: Guidelines for identification, collection and/or acquisition and preservation of digital evidence. 2010.

ЗАСОБИ МЕРЕЖЕВОЇ БЕЗПЕКИ

Харитончук М.М.
Державний університет телекомунікацій
м. Київ, Україна

Сучасний час потребує захисту інформації на будь-якому підприємстві, організації, що вимагає обирати ефективні засоби захисту. Різновиди засобів захисту інформації дозволяють їх комбінувати для забезпечення стійкості інформаційних систем від загроз. До засобів захисту інформації відносяться:

Антивірусні програми

Антивірус - це програма, яка виявляє й знешкоджує комп'ютерні віруси. Слід зауважити, що віруси у своєму розвиткові випереджають антивірусні програми, тому навіть у випадку регулярного користування антивірусів немає 100% гарантії безпеки. Антивірусні програми можуть виявляти та знищувати лише відомі віруси, при появі нового комп'ютерного вірусу захисту від нього не існує до тих пір, поки для нього не буде розроблено свій антивірус. Однак, багато сучасних антивірусних пакетів мають у своєму складі спеціальний програмний модуль, який називається евристичний аналізатор, і який здатний досліджувати вміст файлів на наявність коду, який характерний для комп'ютерних вірусів. Це дає змогу вчасно виявляти та попереджати про небезпеку зараження новим вірусом.

Біометричний захист інформації

Системи біометричного захисту використовують унікальні для кожної людини вимірювані фізіологічні характеристики для перевірки особи індивіда. Цей процес називається електронною аутентифікацією. Його сутність у визначенні, чи справді індивід є тією особою, за яку він себе видає. Це відрізняє аутентифікацію від ідентифікації та авторизації. Мета ідентифікації **полягає у** перевірці, чи відомий індивід системі, наприклад перевіркою пароля, а авторизація полягає в наданні користувачеві доступу до певних ресурсів залежно від його особи.

Біометричні системи забезпечують найбільш точну аутентифікацію, оскільки перевіряють параметри, які дуже важко або неможливо змінити або підробити. Їхні переваги

очевидні, оскільки традиційні системи захисту не здатні з’ясувати, наприклад, хто саме вводить код або вставляє смарт-картку.

Слід зазначити, що біометричні технології мають один суттєвий недолік. Вони спрацьовують завдяки тому, що системі відомі унікальні, конфіденційні характеристики кожної конкретної людини. Однак прибічники біометрії стверджують, що насправді вона забезпечує вищий рівень секретності, оскільки під час аутентифікації не залучається інформація про адресу людини, домашній телефон, банківський рахунок тощо.

Віртуальна приватна мережа

VPN (virtual private network, віртуальна приватна мережа) – це служба, яка дає змогу підключатися до інтернету за допомогою зашифрованого тунелю, щоб забезпечити конфіденційність дій в мережі й захистити ваші персональні дані. Мережі VPN використовуються для захисту підключення до публічних точок доступу Wi-Fi, приховування IP-адрес і конфіденційності перегляду веб-сторінок у браузері.

Криптографічний захист

Використання шифрування для перетворення тексту в незрозумілі сирі данні для їх захисту або для підтвердження їх цілісності за допомогою електронно-цифрового підпису або хеш-функцій.

Міжмережевий екран

Міжмережевий екран (МЕ) називають локальний або функціонально розподілений програмний (програмно-апаратний) засіб (комплекс), який реалізує контроль за інформацією, що надходить в автоматизовану систему і/або виходить з автоматизованої системи. Також зустрічаються загальноприйняті назви брандмауер і firewall (англ. вогняна стіна).

МЕ служить захисною стіною між локальною мережею та зовнішньою мережею і запобігає будь-яким загрозам. Він призначений для контролю вхідного і вихідного трафіку на комп’ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти, вспливаючі вікна та інше, не надсилати іншим “чужим” серверам інформацію про ваш комп’ютер, робить даремною роботу програм-троянів і засобів віддаленого адміністрування. Робота МЕ полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і в залежності від результатів аналізу пропускає пакети у внутрішню мережу (сегмент мережі) або повністю їх відфільтровує. Ефективність роботи МЕ, що працює під управлінням Windows, зумовлена тим, що він повністю заміщує реалізований стек протоколів TCP\IP, і тому порушення його роботи хакерами з допомогою спотворення протоколів зовнішньої мережі є неможливим.

Отже, необхідно зазначити, що поодиночне використання будь-якого з вище наведених засобів не є розумним рішенням, оскільки комплексне використання цих засобів зможе забезпечити більш безпечну передачу та збереження цілісності даних та правильне їх розподілення.

Література

1. Інформаційна і мережева безпека. URL:https://spez.com.ua/informatsiyna-i-merezheva-bezpeka/
2. Типи антивірусних програм. URL:https://sites.google.com/site/diresideinaction/tipi-antivirusnih-program
3. Біометричний захист інформації. URL: https://sites.google.com/site/zahistlokalnoiemerezi/zahist/biometricnij-zahist-informaciie

СЕКЦІЯ 5. ПРОТИДІЯ КІБЕРАТАКАМ НА СИСТЕМИ І БІЗНЕС-СЕРВІСИ КОМПАНІЇ

ПРОБЛЕМИ МОДЕЛЮВАННЯ ЗАГРОЗ В ІНФОРМАЦІЙНІЙ СФЕРІ

Дзюба Т.М., Опанасенко М.І.
Державний університет телекомунікацій
м. Київ, Україна
Стамбірська Р. Г.
Воєнно-дипломатична академія
імені Євгенія Березняка
м. Київ, Україна

В умовах дестабілізуючих негативних інформаційно-психологічних впливів та експансіоністської агресивної інформаційної політики Російської Федерації національний інформаційний простір України зазнає суттєвих викликів та загроз, які становлять небезпеку функціонування держави, її політичного й економічного розвитку, інтеграції у європейські та євроатлантичні структури. В таких умовах гарантувати інформаційну безпеку України лише реагуванням на виклики та загрози недостатньо.

Загрози, як правило, мають комплексний характер. Вони постійно змінюються, а ще частіше приховуються і мають дуже різноманітні прояви, на які важко впливати [1; 2]. При невірному тлумаченні або несвоєчасній ідентифікації таких проявів їх дестабілізуючий вплив суттєво посилюється. Розробити список усіх можливих загроз дуже складно, оскільки геополітичне протиборство ведеться одночасно на усіх рівнях інформаційного простору: глобальному, регіональному та національному, і залежить від конкретних цілей держави. Якщо не виявити момент, коли розпочинається робота з підготовки підґрунтя для основного "удару", який, як відомо, вже корекції не піддається, масштаби наслідків нам відомі на прикладі агресії Російської Федерації.

Спеціалісти цієї сфери діяльності погоджуються з тим, що створення системи раннього виявлення загроз, яка має визначати найменші коливання і зміни в інформаційному просторі національного рівня, дасть можливість діяти на упередження, попереджати виникнення кризових ситуацій, розробляти ефективні механізми протидії конкретним загрозам або мінімізувати шкоду від інформаційних операцій проти нашої держави.

Створення такої системи надзвичайно складне завдання. Інформаційним операціям, які зачіпають соціальні процеси, притаманна вкрай складна природа, вони мають дуже багато відмінних рис і практично не повторюють одна одну, тому дуже важко піддаються аналізу й моделюванню. Соціальні процедури та процеси, як правило складно оцінювати й моделювати через те, що їх результати відносяться до психологічних і соціологічних, а не фізичних процесів. Саме цей факт визначає проблематичність прогнозування результатів моделювання інформаційних операцій та виявленню їх проявів.

У дослідженнях фахівців НАН України, зокрема Інституту проблем реєстрації інформації, відмічається про необхідність врахування при моделюванні складних інформаційних систем реалістичних правил поведінки її окремих елементів. На їх думку, ефективніше в таких системах вирішувати зворотню задачу – по реальній поведінці певних залежностей оцінювати величину параметрів моделі.

В монографії Додонова А.Г. "Распознавание информационных операций" запропоновано ряд моделей інформаційних потоків в мережі Інтернет, який є лише однією із складових інформаційного простору і все частіше стає середовищем проведення інформаційних операцій. В цій роботі для моделювання процесів виявлення інформаційних впливів пропонується використовувати такі моделі:

модель з порогами, в тому числі з лінійними;

модель незалежних каскадів;

модель на снові клітинних автоматів;

модель Ізінга;

моделі на снові ланцюгів Маркова [3, с. 25].

Щоб обрати ефективні математичні платформи для прогнозування можливих сценаріїв динаміки соціальних процесів на якісному рівні, необхідно проаналізувати ряд часткових питань, зокрема технології створення інформаційних операцій і впливів, суб'єкти впливу й агенти на які його спрямовано та закономірності зміни основних й другорядних параметрів інформаційних потоків, які для цього задіюються.

Тому для створення системи раннього виявлення загроз в інформаційній сфері необхідно якомога ширше окреслити структуру національного інформаційного простору, при тому врахувати досвід й погляди провідних країн світу на розбудову власного інформаційного простору, механізми та закономірності, яким регулюються інформаційні потоки в комплексі зі знаннями про етапи підготовки та проведення інформаційних операцій й особливості протікання процесів інформаційно-психологічного впливу на ментальну модель поведінки окремих груп суспільства.

Література

1. Копанчук В.О. Інформаційна безпека як складова національної безпеки України: сучасні виклики та механізми протидії негативним інформаційно-психологічним впливам URL: 035.pdf (nuczu.edu.ua)

2. Прав Р.Ю. Протидія зовнішнім інформаційним загрозам в Україні URL: DOI: 10.32702/23066814.2020.2.141

3. Распознавание информационных операций : монографія / Додонов А. Г. та ін. Київ: ТОВ "Інжиніринг", 2017. 282 с.

ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ВНУТРІШНІХ ЗАГРОЗ ІНФОРМАЦІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА (ОРГАНІЗАЦІЇ)

Побойний О.С
Державний Університет Телекомунікацій
м. Київ, Україна

Створення ефективної системи управління інформаційною безпекою є неможливим без чіткого визначення загроз інформації, що охороняється. Під загрозами інформації прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного володіння інформацією.

За джерелом походження загрози інформаційній безпеці можуть поділятися на внутрішні та зовнішні. Проаналізувавши можливості утворення внутрішніх та зовнішніх загроз, можна перерахувати їх в порядку зменшення імовірності реалізації:

- внутрішні загроз;
- зовнішні загрози;
- загрози, які створюють випадкові особи.

До внутрішніх загроз відносять дії (навмисні чи не навмисні) співробітників, що протидіють інтересам підприємства, наслідком яких може бути втрата інформаційних ресурсів, підрив іміджу компанії, виникнення проблем у відносинах з реальними чи потенційними партнерами.

Значна частина внутрішніх загроз реалізується за участі персоналу, то ж можна сказати, що головним джерелом загроз є працівники конкретної організації.

Таким чином внутрішні загрози можуть утворюватися внаслідок:

- непрофесійних дій працівників;
- низького стану виховної та профілактичної роботи в організації;
- недосконалої системи заробітної плати та стимулювання праці персоналу;
- порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи в організації;
- психологічних та комунікаційних особливостей працівників;

Для нейтралізації внутрішніх загроз потрібно прийняти наступні заходи:

- організаційні заходи з захисту інформації;
- контрольно-правові заходи (контроль за виконанням персоналом вимог відповідних нормативних документів);
- інженерно-технічні заходи;
- робота з кадрами (підбір та навчання персоналу, підвищення їхньої кваліфікації);
- психологічні заходи (встановлення відео спостереження).

Отже, внутрішні загрози безпеки існують завжди і не залежать від ролі, місця, значення організації чи наявності зовнішніх загроз.

Тому керівництву організації потрібно серйозно звертати увагу на проблеми захисту інформації від внутрішніх загроз, адже для цього існують всі необхідні засоби як технічні так і організаційні.

Література

1. Ткачук Т., Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту. *Право України*. 2011. № 3. 366с.
2. Скиба В., Курбатов В. Керівництво по захисту від внутрішніх загроз інформаційної безпеки Москва: Пітер, 2008. 320с.
3. Скляренко А. Загрози конфіденційності інформації, пов'язані з персоналом, бізнес та безпека. 2010. №1. 92с.

ДОСЛІДЖЕННЯ ВЗАЄМОДІЇ МІЖ ВІДДІЛАМИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ

Солодяк В.І.
Державний університет телекомунікацій
м. Київ, Україна

Кібератаки стали звичним явищем у всьому світі, становлячи реальну і серйозну загрозу для організацій. Зросла не тільки кількість атак, а і їхня складність, масштабність та летальність. Компаніям часто доводиться стикатися з економічними наслідками втраченої інформації та довіри клієнтів після серйозних кібератак. Коли трапляється інцидент з безпекою, кожна секунда має значення. Шкідливе зараження швидко розповсюджується, програма-вимога може нанести катастрофічну шкоду, а скомпрометовані облікові записи можуть використовуватися для ескалації привілеїв, що веде зловмисників до більш чутливих активів.

Incident response (IR) (реакція на інцидент) - це структурована методологія для обробки інцидентів безпеки, порушень та кіберзагроз. Чітко визначений план реагування на аварії (IRP) дозволяє вам ефективно ідентифікувати, мінімізувати збитки та зменшити

вартість кібератаки, одночасно знаходячи та встановлюючи причину для запобігання майбутнім атакам.

План реагування на інциденти кібербезпеки

Залежно від ступені порушення, слід повідомити про напад інші відділи. У багатьох випадках іншим підрозділам, таким як служба обслуговування клієнтів, фінанси або IT, потрібно негайно вжити заходів. У вашому плані реагування на події має бути чітко зазначено, кого залежно від типу та тяжкості порушення слід кому інформувати. План повинен містити повні контактні дані та способи спілкування з кожною відповідною стороною, щоб заощадити час після наслідків нападу. Першим пріоритетом під час впровадження кібербезпеки реагування на інциденти є підготовка заздалегідь, складання конкретного плану IP. Ваша методологія реагування на події повинна бути перевірена боєм до того, як відбудеться суттєва атака або порушення даних. Він повинен розглядати наступні етапи відповіді, визначені NIST

- Підготовка - заздалегідь сплануйте, як боротися з інцидентами безпеки та запобігати їм
- Виявлення та аналіз - охоплює все, від моніторингу потенційних векторів атак, пошуку ознак інциденту до встановлення пріоритетів
- Обмеження, викорінення та відновлення - Розробка стратегії стримування, виявлення та пом'якшення хостів та систем, що зазнали атаки, та складання плану відновлення
- Діяльність після інцидентів - Перегляд отриманих уроків та складання плану збереження доказів

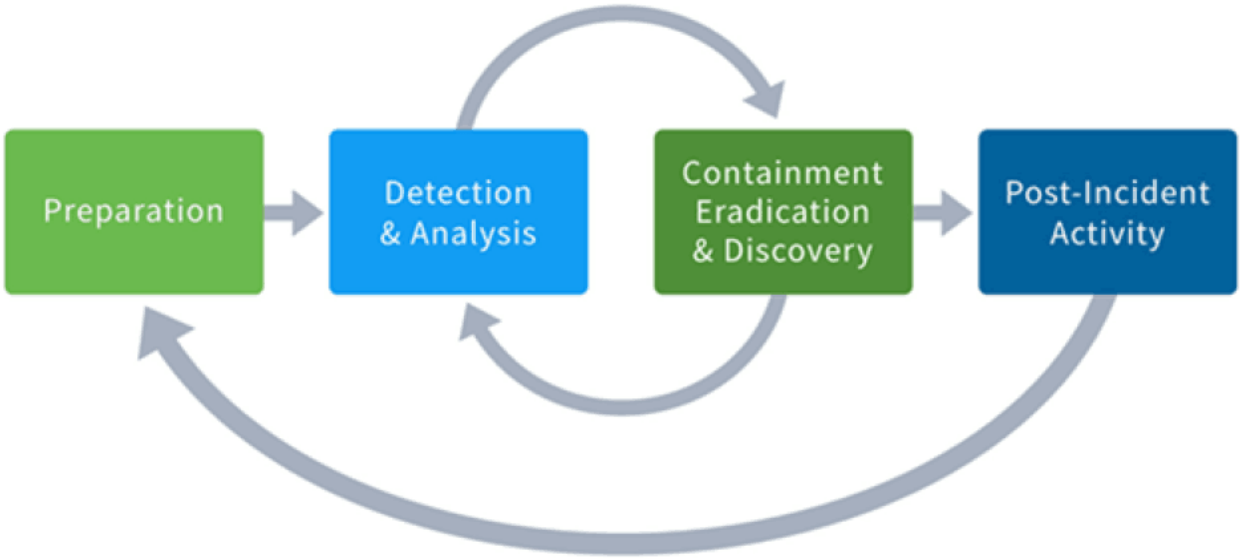


Рисунок 1 - Рекомендовані етапи NIST для реагування на інцидент кібербезпеки

Інцидент із безпекою є аналогом лісової пожежі. Після того, як команда виявила інцидент та його джерело, їм потрібно запобігти пошкодженню. Це може включати відключення доступу до мережі для комп’ютерів, які, як відомо, заражені вірусами або іншим шкідливим програмним забезпеченням (щоб їх можна було помістити на карантин) та встановлення виправлень безпеки для вирішення проблем з шкідливим програмним забезпеченням або мережевих вразливостей. Можливо, їм доведеться скинути паролі для користувачів, у яких були порушені облікові записи, або заблокувати облікові записи інсайдерів, які могли спричинити інцидент. Далі мета команди полягає, щоб внести зміни, мінімізуючи вплив на діяльність організації. Цього можна досягти обмеживши обсяг даних, що піддаються.

Це робиться наступним чином:

- Визначте та виправте всіх постраждалих хостів, включаючи хостів у вашій організації та поза нею
- Виділіть корінь атаки, щоб видалити всі екземпляри програмного забезпечення
- Проведіть аналіз шкідливого програмного забезпечення, щоб визначити ступінь збитку
- Перевірте, чи зреагував зловмисник на ваші дії
- Передбачте інший тип атаки та створіть відповідь
- Залиште час, щоб переконатися, що мережа в безпеці та що зловмисник не здійснює подальших дій

Методологія реагування на аварії дозволяє організаціям заздалегідь визначити контрзаходи реагування. Існує широкий спектр підходів до IP. Більшість фахівців з безпеки погоджуються з шістьма кроками реагування на інциденти, рекомендованими NIST, включаючи підготовку, виявлення та аналіз, стримування, викорінення, відновлення та аудит після аварії.

Що стосується підготовки, багато організацій використовують комбінацію контрольних списків оцінки, детальних планів реагування на аварії, узагальнених та діючих посібників з реагування на аварії, а також політик, які можуть автоматизувати деякі процеси. Хоча вона добре спланована, методологія реагування на інциденти повинна залишатися гнучкою, дозволяючи постійне вдосконалення.

Література

1. Люк Фойгт Етапи реагування на аварії: 6 кроків для реагування на інциденти, що стосуються безпеки URL: https://www.exabeam.com/incident-response/the-three-elements-of-incident-response-plan-team-and-tools/
2. Прамод Брокар. Три елементи реагування на аварії URL: https://www.exabeam.com/incident-response/steps/

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАПОБІГАННЯ, ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ІНСАЙДЕРСЬКИХ КІБЕРАТАК

Сайніді М.С.
Державний університет телекомунікацій
м. Київ, Україна

Останнім часом спостерігається загальносвітова тенденція зростання рівня кіберзлочинності. Нажаль, сьогодні наша держава поряд із Бразилією, Китаєм, Індією т аіншими країнами стає міжнародним центром зазначеної протиправної діяльності [1]. Так, розкрадання коштів в системах інтернет-банкінгу, даних кредитних карт, шахрайство в інформаційних мережах та інсайдерські витоки інформації стають повсякденними явищами на вітчизняних теренах [1].

Інсайдерські загрози реалізуються за рахунок вразливостей системи захисту інформації. Дані уразливості визначаються не тільки пробілами в системі безпеки і політики, але і в організації управління доступом до ресурсів.

Для створення системи контролю доступу насамперед необхідно визначити безліч суб'єктів і об'єктів доступу.

Застосування підходу розмежування доступу зменшує ймовірність інсайдерської загрози, так як визначальним фактором для дій інсайдера є коло його можливостей для

нанесення шкоди. Але повністю виключити таку загрозу не можна, так як завжди є ймовірність того, що інсайдером виявиться суб'єкт з достатнім рівнем доступу для реалізації широкого спектру загроз.

Ця проблема вимагає більш широкого, системного підходу до кібербезпеки загалом, не тільки на рівні бізнесу, але на рівні держави загалом.

Звернувшись до досвіду країн ЄС, США, можна виокремити такі аспекти, які слід було б впровадити Україні для забезпечення кібербезпеки:

– побудова ефективної урядової моделі, спрямованої на забезпечення кібербезпеки;

– визначення адекватного механізму, в основному у вигляді суспільно-державного партнерства, який дозволить приватним та державним зацікавленим суб'єктам обговорювати та визначати політику у сфері забезпечення кібербезпеки;

– визначення цілей та способів розвитку державних можливостей, а також необхідної законодавчої бази для участі у міжнародній боротьбі з кіберзлочинністю;

– визначення ключових інформаційних інфраструктур, у тому числі – основних активів, сервісів та взаємозалежностей;

– підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту для ключових інформаційних інфраструктур;

– розробка системного та інтегрованого підходу до державного управління ризиками;

– запровадження нової програми освіти, в якій буде зроблено акцент на навчання IT-фахівців та професіоналів в області кібербезпеки;

– розвиток міжнародної співпраці у зазначеній сфері [2].

Огляд моделей управління доступом показує, що існують різні варіанти розмежування доступу. Але жодна модель не захистить від людського фактора. Тому ймовірність інсайдерської загрози існує завжди, адже інсайдером може стати будь-який суб'єкт з будь-яким набором повноважень. Розглянуті варіанти загроз показують, що існує досить великий список можливостей для інсайдерів. Щоб розробити якісну модель протидії інсайдерам, необхідно провести класифікацію інсайдерів, визначити можливості кожного окремого класу і, відповідно до цього, визначити можливі заходи і засоби захисту.

Література

1. Довбиш М. Кіберзлочинність в Україні. URL: https://www.science-community.org/ru/node/16132

2. Государственные стратегии кибербезопасности. URL: http://www.securitylab.ru/analytics/429498.php

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМАХ

Очковський Є.О.
Державний Університет Телекомунікацій
м.Київ, Україна

Інформаційно-аналітична система (ІАС) — це комп'ютерна система, яка дозволяє отримувати, створювати інформацію та здійснювати її обробку та аналіз.

Задачами ІАС є ефективне зберігання, обробка та аналіз даних. Технологічна платформа ІАС дозволяє підприємству (організації) здійснювати інтеграцію та координацію його бізнес-процесів.

ІАС забезпечує для підприємства (організації) єдиний інформаційний простір і гарантує, що ця інформація буде доступна на всіх функціональних рівнях ієрархії та управління.

За способами застосування інформаційно-аналітичні системи поділяються на системи для рішення тактичних і стратегічних завдань

Інформаційно-аналітичні системи підрозділів передбачають більшу деталізацію й більш складну аналітичну обробку. Ці системи допомагають підготувати інформацію для прийняття рішень в області збуту, продуктової пропозиції, фінансового планування.

Інформаційно-аналітичні системи верхнього рівня призначені для керівників верхньої ланки й слугують для прийняття стратегічних рішень.

До типових завдань, які вирішуються за допомогою інформаційно-аналітичних систем, відносяться:

– складання консолідованої звітності й надання зведеної інформації про діяльність підприємства (фінансові, виробничі й інші показники, динаміка їхніх змін і тенденціїй);

– аналіз діяльності дочірніх підприємств, філій і підрозділів компанії (аналіз прибутковості, витрат, виконання плану);

– аналіз фінансової діяльності (основні фінансові показники, тенденції, взаєморозрахунки), оптимізація фінансових потоків, реальна оцінка собівартості продукції;

– проведення комплексної оцінки діяльності підприємства, заснованої на постійному контролі найбільш істотних її аспектів: фінансів, відносин з партнерами й клієнтами, внутрішнього стану компанії, темпів розвитку;

– аналіз збутових процесів (маркетингові компанії, складання плану, контроль виконання розпоряджень, розрахунки за відвантажену продукцію, прогноз надходження засобів, прогноз попиту).

Переваги, одержувані підприємством після впровадження корпоративної інформаційно-аналітичної системи:

– наявність у керівників ефективних інструментів оцінки стану бізнесу на основі єдиного джерела ключових показників, що відповідаєі реальному стану;

– можливість оцінки перспектив розвитку;

– підвищення обґрунтованості прийняття управлінських рішень;

– можливість узгодження оперативних планів і бюджетів зі стратегічними цілями;

– розширені можливості аналітики, які надані сховищем даних, засобами багатомірного аналізу даних, прогнозування й моделювання різних ситуацій за принципом "Що, якщо?";

– розширені можливості стратегічного керування на основі потужних засобів аналізу й звітності;

– виключення проблем, пов'язаних з оцінкою ситуації на основі показників, одержуваних на основі неінтегрованих рішень.

Шляхи вдосконалення інформаційної безпеки на рівні суспільства та корпорації:

- забезпечення конституційних прав і свобод громадян в інформаційній сфері: свободи слова; права на отримання інформації та користування нею; права на приватну таємницю, таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень; захищеності конфіденційної інформації (персональних даних); права на інтелектуальну власність;

- формування відкритого й безпечного інформаційного простору, що сприяє розвитку громадянського суспільства через: забезпечення доступності інформації, незалежності ЗМІ; посилення контролю представницьких органів за діяльністю державних ЗМІ; розвиток інформаційної інфраструктури; розробку та впровадження новітніх інформаційних технологій; постійне поповнення та надійний захист національного інформаційного ресурсу;

недопущення монополізму в усіх ланках продукування, накопичення, зберігання та поширення інформації; запобігання розповсюдження інформації, що провокує політичну або соціальну нетерпимість, міжетнічні або міжконфесійні конфлікти, сепаратизм; обмеження негативного інформаційного впливу на суспільну свідомість і психіку громадян;

- захист інформаційного простору України від негативного зовнішнього впливу через: забезпечення захищеності вітчизняних інформаційних систем (насамперед, інформаційно-аналітичних систем органів державної влади та місцевого самоврядування, автоматизованих систем управління військових формувань) від несанкціонованого доступу; недопущення витоку таємної, конфіденційної та іншої інформації з обмеженим доступом; протидію інформаційній експансії з боку інших держав; подолання технічної та технологічної залежності вітчизняної інформаційної інфраструктури від зарубіжних виробників;

- якісне інформаційно-аналітичне забезпечення діяльності органів державної влади та місцевого самоврядування через: забезпечення відкритості органів державної влади (в т. ч. силових структур), громадського контролю за їх діяльністю; активне залучення інтелектуального потенціалу наукових установ, неурядових аналітичних центрів, громадських організацій; автоматизацію процесів збору, аналізу та використання інформації; створення системи інформаційних мереж, сполучених баз даних центральних і місцевих органів державної влади та місцевого самоврядування; впровадження систем електронного документообігу; створення мережі ситуаційних центрів для оперативного інформаційно-аналітичного забезпечення керівництва держави в надзвичайних (нештатних) ситуаціях;

- перетворення виробництва інформаційної продукції та послуг на потужний чинник економічного зростання України через: забезпечення пріоритетного розвитку вітчизняного виробництва інформаційних технологій та комп'ютерних систем; усунення монополізму та інших перешкод становленню ринкових відносин в інформаційній сфері; державну підтримку, в т.ч. пільгове оподаткування суб'єктів господарювання, які виробляють та/або впроваджують новітні інформаційні технології; зосередження зусиль на загальній комп'ютеризації; підвищення комп'ютерної грамотності населення;

- збільшення обсягів та підвищення рівня підготовки фахівців у цій галузі, створення гідних умов для їх працевлаштування в Україні;

- інтеграція України до світового інформаційного простору через: гармонізацію законодавства України в інформаційній сфері з нормами міжнародного права; адаптацію вітчизняної системи стандартів до світових аналогів; підвищення конкурентоспроможності вітчизняних ЗМІ, поширення їх діяльності на зарубіжні країни; створення іномовних інформаційних ресурсів про економічний, науковий, освітній, культурний, туристичний потенціал України; модернізацію систем зв'язку; інтенсивний розвиток вітчизняного сегменту мережі Інтернет;

- збереження власної культурної ідентичності за умов посилення процесів глобалізації через: розвиток внутрішніх джерел поповнення інформаційних ресурсів (освіти, науки, культури); захист від інформаційно-культурної експансії з боку інших держав; накопичення україномовних інформаційних ресурсів; забезпечення користувачів комп'ютерної техніки мовно адаптованими програмними продуктами.

Література

1. Інформаційно-аналітична діяльність працівників. URL: https://core.ac.uk/download/pdf/32310627.pdf
2. Інформаційно-аналітична діяльність. URL:http://www.nbuviap.gov.ua/images/nak_mon_partneriv/IAD.pdf

ОРГАНІЗАЦІЯ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Бойчук Л.Я.
Державний університет телекомунікацій
м. Київ, Україна

Інцидент назавжди відбувається відкрито. Навпаки, зловмисники намагаються зробити все, щоб не залишити в системі слідів своєї діяльності. Прийняття рішення про настання події інциденту багато в чому залежить від компетентності експертів команди реагування. Необхідно відрізняти випадкову помилку оператора від зловмисного цілеспрямованого впливу на інформаційну систему. Керівництво організацій повинно звернути увагу на цю обставину і надати експертам команди реагування певну свободу дій [1, с.58-64].

Розглянемо для початку так звану, анатомію інциденту. Існує декілька етапів, які можна виділити в ході інциденту:

1) detection - інтервал між першою помилкою, яку ми віддали користувачеві, до того, як черговому прийшло SMS

2) reaction - від отримання повідомлення про проблему до моменту, коли людина приступив до вирішення даної проблеми (зазвичай в цей момент подія в моніторингу перетворюється на стан Acknowledged)

3) investigation - від початку роботи над проблемою до моменту, коли зрозуміла причина інциденту і ми знаємо, що потрібно зробити, щоб відновити роботу.

4) elimination - час відновлення, наприклад, відкатуємо реліз, промоутім новий master primary сервер БД [2, с.78].

Складання діагностичних матриць служить для візуалізації результатів аналізу подій, що відбуваються в інформаційний системі. Така матриця формується з рядків потенційних ознак інциденту та стовпців – типів інцидентів. Дається оцінка події за шкалою пріоритетів «високий», «середній» та «низький». Діагностична матриця покликана документувати процес логічних висновків експертів під час прийняття рішення і, поряд з іншими документами, використовується для розслідування інциденту.

При аналізі інцидентів інформаційної безпеки (ІІБ) організація повинна виконати таке:

- своєчасно ідентифікувати невдалі та успішні порушення безпеки і інциденти безпеки;
- допомогти у виявленні подій безпеки, таким чином запобігти інцидентам безпеки шляхом використання індикаторів [3, с.78-83].

Таким чином, управління ІІБ передбачає проведення таких заходів:

1) Повідомлення про події інформаційної безпеки. Ці повідомлення повинні якомога швидше поширюватися належними управлінськими каналами.

2) Повідомлення про уразливості захисту. Необхідно зобов'язати всіх співробітників, підрядчиків і користувачів із сторонніх організацій, що використовують інформаційні системи та сервіси, відмічати і повідомляти про всі спостережувані або передбачувані уразливості захисту систем або сервісів.

3) Відповідальність і процедури. Необхідно встановити відповідальність керівників та визначені процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти інформаційної безпеки.

4) Навчання інцидентам ІБ. Повинні бути реалізовані механізми, які надають можливість виміряти та відстежувати типи, об'єми і вартість ІІБ.

5) Збір доказів. Якщо в результаті аналізу ІІБ встановлено, що дії осіб потребують правової кваліфікації, то необхідно зібрати, зберегти та надати докази такої протиправної діяльності у встановленому правовою системою певної країни порядку.

Література

1. Дмитрієв А.А. Внутрішній аудит системи менеджменту інформаційної безпеки за вимогами ISO/IEC 27001. Один з варіантів реалізації процесу. Das Management. 2011. № 2. С. 58-64.
2. Information technology. Security techniques. Information security incident management : ISO 27035:2011. 78 p.
3. Дмитрієв А.А. Ризик-менеджмент за вимогами міжнародного стандарту ISO/IEC 27001. Один із способів побачити майбутнє без машини часу. *Das Management*. 2010. № 4. С. 79-83.

СЕКЦІЯ 6. БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ КОМПАНІЇ

БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЙ У АСПЕКТІ ВПЛИВУ ЕЛЕКТРОМАГНІТНОГО ІМПУЛЬСУ НА РАДІОЕЛЕКТРОННІ ЗАСОБИ ТА ЕЛЕКТРОННІ ПРИСТРОЇ

Кирилюк В.А, Іщенко Д.А.
Житомирський військовий інститут імені С.П.Корольова,
м. Житомир, Україна

Однією з особливостей сучасних війн і збройних конфліктів є ведення бойових дій в урбанізованій місцевості з використанням засобів як вогневого ураження так і радіоелектронної боротьби. За аналізом існуючих нині факторів та умов електромагнітної обстановки в урбанізованої місцевості, перспектив її розвитку слід прогнозовано очікувати значного її ускладнення в разі розгортанні бойових дій з застосуванням електромагнітної зброї. Фактор створення штучного електромагнітного імпульсу (ЕМІ) має негативний характер щодо об'єктів критичної інфраструктури організацій, тому що обумовлює зовнішні діючі чинники сформованих електромагнітних полів, які, проникаючи в технічні засоби, викликають функціональне ураження їх радіоелектронних засобів (РЕЗ) та електронних пристроїв (ЕП).

Вплив ЕМІ може бути досить значним. За даними [1] EMP is a threat for (ЕМІ є загрозою для): National security (національної безпеки); Data centers (центів обробки даних); Telecommunications (телекомунікації); Heating companies (компаній опалення); Transportation sector (транспортного сектору); Banks and other financial services (банківських та інших фінансових секторів); Security systems (систем безпеки); The electricity distribution infrastructure (інфраструктури розподілу електрики); Hospitals and public health facilities (госпіталям і громадським медичним закладам); Oil/gas industry (нафтової та газовій індустрії); Water treatment facilities (водоочисним спорудам); All other not mentioned technology driven instances (все інші не згадані об'єкти, керовані технологією автоматизованого управління).

Аналіз, сучасних методів та аналітичний огляд науково-технічної та нормативної інформації показав, що на сьогодні існує потреба вдосконалення захисту об'єктів критичної інфраструктури, їх РЕЗ та ЕП від впливу засобів створення ЕМІ. Встановлено можливість та доцільність адаптації окремих результатів, раніш досягнутих у дослідження радіоелектронного захисту військових об'єктів від зброї ЕМІ [2; 3], для вирішення визначеної потреби.

Засобами створення ЕМІ у цієй роботі вважаємо неядерні засоби генерування ЕМІ, спеціально розроблені й виготовлені для функціонального ураження (подавлення) елементів радіоелектронної апаратури (РЕЗ та ЕП) у складі об'єктів, керованих з використанням мережних та операційних систем у технологіях автоматизованого управління.

Оцінювання безпеки об'єктів критичної інфраструктури (ОКІ) організацій щодо впливу засобів ЕМІ на радіоелектронну апартуру здійснюється з метою визначення електромагнітної стійкості ОКІ у різних умовах воєнно-політичної, оперативної та електромагнітної обстановки. Оцінювання безпеки ОКІ від впливу засобів ЕМІ передбачає: аналіз можливостей щодо застосування засобів ЕМІ в районі ОКІ; оцінювання електромагнітної стійкості ОКІ.

Аналіз можливостей щодо застосування засобів ЕМІ проводиться відповідними компетентними службами ОКІ за інформацією правоохоронних, органів державного (місцевого) управління щодо загальних рівнів небезпеки в районі ОКІ.

Пропонується для оцінювання електромагнітної стійкості ОКІ проведення таких процедур.

Розподілення ОКІ на функціональні організаційно-технічні системи, наприклад: управління персоналом, управління технологічними процесами, управління безпекою тощо.

Виділення у визначених організаційно-технічних системах системоутворюючих технічних підсистем, функціонування яких є обов'язково потрібним для функціонування ОКІ. Визначення в таких підсистемах засобів радіоелектронної апартури – елементів техніки (засобів автоматизованого управління, обчислювальної техніки, комунікації, тощо), від яких залежить виконання технологічних процесів з використанням операційних систем та мережних технологій.

Після виділення в засобах окремих елементів РЕА, для кожного типу РЕА розраховуються просторові показники імовірного виведення його з ладу (тимчасово, або не обернено) відносно кожного прогнозованого до застосування засобу ЕМІ [5-7]. Загальний висновок щодо електромагнітної стійкості ОКІ робиться за наймеш стійким до ЕМІ елементом радіоелектронної апартури ОКІ.

В разі визнання особою, що приймає рішення, недостатньої електромагнітної стійкості ОКІ для забезпечення безпеки об'єктів критичної інфраструктури (ОКІ) організацій у цілому,розробляються варіанти необхідних організаційних (організаційно-технічних) заходів підвищення безпеки.

Отже, роботу присвячено вирішенню актуальної науково-практичної задачі – методики оцінювання ефективності та удосконалення організаційних заходів і застосування технічних засобів захисту РЕА ОКІ від впливу засобів ЕМІ.

Література

1. EMP protection / electromagnetic pulse protection. URL:https://hollandshielding.com/EMP-Protection?_ga=2.236100551.797705764.1613404512-113534524.1613404512.
2. Методика оцінювання стійкості радіоелектронних засобів військових об'єктів до впливу електромагнітного імпульсу зброї / Д. А. Іщенко, В. А. Кирилюк, І. А. Павленко, Д. В. Пясковський, А.М. Стариков. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*. 2016. Вип. 13. С.51-61. URL: http://nbuv.gov.ua/UJRN/Psvz_2016_13_8
3. Іщенко Д.А. Науково-методичний апарат оцінювання захищеності радіоелектронних засобів військового призначення від впливу електромагнітної зброї / Д. А. Іщенко, В. А. Кирилюк, А.М. Стариков. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*. 2018. Вип. 15. С. 143-155. URL:http://nbuv.gov.ua/UJRN/Psvz_2018_15_16
4. Федоров П.М., Богучарський В.В., Гамалій Н.В. Методика розрахунку густини потоку випромінювання зразків електромагнітної зброї. ЦНДІ ОВТ ЗС України. Вип. 4(59). Київ: ЦНДІ ОВТ ЗС України, 2015. С. 168–180.
5. Федоров П.М., Богучарський В.В., Гамалій Н.В. Оцінка реальних уражальних можливостей сучасної зброї електромагнітного імпульсу. *ЦНДІ ОВТ ЗС України*. Вип. 3(62). Київ : ЦНДІ ОВТ ЗС України, 2016. С.165–176.
6. Федоров П.М., Богучарський В.В., Гамалій Н.В. Розрахунок зон ураження зброї електромагнітного імпульсу. В.. *Озброєння та військова техніка*. 2018. № 2. С. 75-82. URL:http://nbuv.gov.ua/UJRN/ovt_2018_2_15

БЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ КОМПАНІЇ

Алексеєнко А.В.
Державний Університет Телекомунікацій
м. Київ, Україна

Об'є́кти крити́чної інфраструкту́ри — підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв.

Закон України «Про основні засади забезпечення кібербезпеки України» використовує термін «**Критично важливі об'єкти інфраструктури**», визначаючи їх як юридичні особи, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Цей Закон також надає взаємопов'язане визначення **об'єкт критичної інформаційної інфраструктури**: комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури.

ПРОЕКТ ПОСТАНОВИ КМУ «ПРО ЗАТВЕРДЖЕННЯ ПОРЯДКУ ВІДНЕСЕННЯ ОБ'ЄКТІВ ДО ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

До складу Порядку входять наступні документи:

1. Порядок віднесення об'єктів до об'єктів критичної інфраструктури
2. Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави
3. Методика категоризації об'єктів критичної інфраструктури

Проектом постанови визначається : власник та/або керівник об'єкта критичної інфраструктури (далі – оператор основних послуг) – державний орган, підприємство, установа, організація, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належать об'єкти критичної інфраструктури та який/яка відповідає за їх поточне функціонування; життєво важливі послуги та функції (далі – основні послуги) – послуги та функції, які надаються органами державної влади, державними установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні (виконанні) яких призводять до негативних наслідків для населення, суспільства, соціальноекономічного стану та національної безпеки і оборони України; уповноважений орган державної влади відповідальний за сектор (підсектор) критичної інфраструктури – центральний орган виконавчої влади, інший державний орган, який забезпечує формування та реалізацію державної політики в одній чи декількох сферах. сектор (підсектор) критичної інфраструктури – сукупність об'єктів критичної інфраструктури, які належать до одного сектору (підсектору) економіки та/або мають спільну функціональну спрямованість;

Порядок віднесення об'єктів до об'єктів критичної інфраструктури встановлює:

- категорії критичності об'єктів критичної інфраструктури;
- механізм ідентифікації об'єктів критичної інфраструктури;

- визначає необхідність формування Національного переліку об’єктів критичної інфраструктури та секторальних переліків об’єктів критичної інфраструктури та відповідальних за їх формування.
-

Література

1. URL:https://uk.wikipedia.org/wiki/%D0%9E%D0%B1%27%D1%94%D0%BA%D1%82%D0%B8_%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D0%BE%D1%97_%D1%96%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B8
2. URL:https://niss.gov.ua/sites/default/files/2019-10

КОНЦЕПТУАЛЬНІ ЗАСАДИ КІБЕРСТІЙКОСТІ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ПРИКЛАДІ ВЕЛИКОЇ БРИТАНІЇ

Легомінова С.В., д.е.н., проф.
Державний університет телекомунікацій,
м.Київ, Україна

Критичною інфраструктурою у Великій Британії визнають: “критичні елементи інфраструктури (установки, системи, майданчики, об’єкти, власність, інформація, люди, мережі та процеси), втрата або порушення діяльності яких призвели б до серйозного негативного впливу на можливість отримання і надання або на цілісність важливих послуг, унаслідок чого можуть виникнути тяжкі наслідки для економіки і соціальної сфери або втрати життя людей” [1].

Стійкість критичної інфраструктури визначається, як здатність активів, мереж та систем прогнозувати руйнівні події, переносити їх, адаптуватися та швидко відновлюватися після них [2].

Виділяють 13 національних секторів (в попередньому переліку їх було 9) інфраструктури: хімічна галузь, промисловість, цивільні ядерні комунікації, оборона, надзвичайні служби, енергетика, фінанси, продовольство, уряд, охорона здоров'я, космос, транспорт та вода.

Великобританія, за зразком США, орієнтується у захисті критичної інфраструктури на протидію тероризму і порушенню кіберпростору.

Основоположними стратегічними документами, що формують нормативно-правову базу для національної СЗБСКІ, у Великій Британії є такі чинні документи:

1) Стратегія національної безпеки (2010) [3];

2) Урядова настанова “Забезпечення функціонування країни: Природні небезпеки та інфраструктура” (2011) [4];

3) Стратегія кібербезпеки Сполученого Королівства. Захист та сприяння Сполученого Королівства у цифровому світі (2011) [5];

4) Стратегічна національна основа стійкості громад (2011) [6];

5) Стратегічний огляд у сфері оборони та безпеки: захищене та процвітаюче Сполучене Королівство (2015) [7].

Координація дій щодо захисту критичної інфраструктури у Великій Британії на національному рівні покладена на: урядову установу Центр захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI).

Центр захисту національної критичної інфраструктури є основним державним органом, який надає консультації з питань безпеки національної інфраструктури

підприємствам, установам та організаціям. CPNI функціонує при Службі безпеки MI-5, підзвітний його директору та підконтрольний МВС. Слугує міжвідомчим центром для участі різних учасників у захисті критичноъ ынфраструктури, адже для виконання своїх задач залучає різних суб'єктів та використовує ресурси ряду державних установ, Служби безпеки (MI-5), CESG (Національний технічний орган у справах інформації уряду Великої Британії) та інших організацій.

Надає комплексні консультації з питань безпеки підприємствам і організаціям, які є операторами критичної інфраструктури, включаючи інформаційні, кадрові та технічні аспекти безпеки, допомагаючи знизити вразливість національної критичної інфраструктури від тероризму та інших загроз. Рекомендації із захисту критичної інфраструктури надаються у вигляді індивідуальних консультацій, тренінгів, онлайн-інформації та опублікування консультаційних матеріалів. Діяльність CPNI спрямована на забезпечення збереження основних послуг економіки Великобританії (зв'язок, медична допомога, енергетика, фінанси, харчові продукти, транспорт тощо). Без них держава може зазнати серйозних економічних збитків, соціальних загострень, навіть значних людських втрат.

У жовтні 2016 р. було створено Центр національної кібербезпеки (National Cybersecurity Center, NCSC), який об'єднує експертизу CESG (групи з інформаційного забезпечення), Центр кібероцінки (Centre for Cyber Assessment), CERT-UK та Центр захисту національної інфраструктури [8].

Національний центр кібербезпеки Великобританії – організація, яка надає консультативну допомогу і підтримку державному і приватному секторам з питань протидії загрозам комп'ютерної безпеки. NCSC створено з метою захисту критично важливих об'єктів в Інтернет-сфері і здійснення протидії кіберзагрозам. В центр включені експерти в галузі безпеки команди з реагування на комп'ютерні надзвичайні ситуації CERT-UK. Діяльність NCSC, враховуючи американську Директиву № 41 (PPD-41), зосереджена на кіберінцидентах. Метою діяльності є покращення кіберзахисту об'єктів критичної інфраструктури, мереж державного та приватного секторів, надання консультацій операторам та громадянам для функціонування та ведення бізнесу з використанням інформаційних мереж та Інтернету, своєчасне виявлення кібератак і їх швидка нейтралізація, виявлення загроз функціонуванню сайтів державних відомств та блокування поширення вірусних програм; участь у розробці "Стратегії щодо захисту кіберпростору" та у формуванні переліку загроз у даній сфері.

NCSC визначає ризики для вжиття відповідних контрзаходів. З метою посилення кіберзахисту з 2015 р. реалізує програму "10 кроків до кібербезпеки", де пропонується алгоритм дій для захисту операторів від кібератак.

В межах програми "10 кроків до кібербезпеки", передбачена спільна діяльність з департаментом бізнесу, інновацій та навичок (BIS), Кабінетом Міністрів та CPNI. Діяльність здійснюється в інтересах національної безпеки, економічного добробуту Великобританії та з метою попередження, виявлення або припинення тяжких злочинів. До основних задач входить протидія: кіберзагрозам (для цього співпрацює з операторами критичної інфраструктури, для забезпечення безперервності основних послуг, які вчиняються з використанням цифрових мереж; з урядом та промисловістю, яким надає інформацію про загрози та експертні поради щодо захисту інформації; з правоохоронними органами для розслідування злочинів в Інтернет-сфері); тероризму – в частині недопущення поширення через Інтернет, набору нових бранців та координації вчинення терактів тощо; вчиненню тяжких злочинів; шпигунству, оскільки, розвиток технологічного світу означає, що кіберзлочинці можуть вчиняти збір даних від представників державних організацій та приватних компаній в інформаційній, комунікаційній та промисловій сфері, генетиці та обороні.

Отже, кіберстійкість об'єктів критичної інфраструктури забезпечується завдяки чіткому розумінню поняття критична інфраструктура, правовому регулюванню захисту

критичної інфраструктури та чітко організованої та налагодженої взаємодії структур, які забезпечують захист.

Література

1. Cabinet Office. Public Summary of Sector Security and Resilience Plans. (2017). URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_ data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_ pdf___002_.pdf
2. Cabinet Office. Keeping the Country Running: Natural Hazards and Infrastructure. A Guide to improving the resilience of critical infrastructure and essential services (2011). URL: https://www.gov.uk/government/publications/keeping-the-country-running-natural-hazardsand-infrastructure
3. . A Strong Britain in an Age of Uncertainty: The National Security Strategy. (2010). URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_ data/file/61936/national-security-strategy.pdf
4. Cabinet Office. Keeping the Country Running: Natural Hazards and Infrastructure. A Guide to improving the resilience of critical infrastructure and essential services (2011). URL: https:// www.gov.uk/government/publications/keeping-the-country-running-natural-hazards-andinfrastructure
5. The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_ data/file/60961/uk-cyber-security-strategy-final.pdf
6. Strategic National Framework on Community Resilience. (2011). URL: https://m.oxfordshire. gov.uk/cms/sites/default/files/folders/documents/fireandpublicsafety/emergency/StrategicNationalFramework.pdf
7. National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom. (2015). URL: https://assets.publishing.service.gov.uk/government/ uploads/system/uploads/ attachment_data/file/555607/2015_Strategic_Defence_and_Security_ Review.pdf
8. Циплинський Ю.І. Порядок формування переліку об’єктів критичної інформаційної інфраструктури: основні підходи, стандарти і критерії, міжнародний досвід URL: http://kiev-chamber.org.ua/files/tsuplynskiy.pdf
9. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНИХ ІНФРАСТРУКТУР

Каблучко Д.М.
Державний університет телекомунікацій
м. Київ, Україна

Національний інститут стратегічних досліджень , досліджуючи тривалий час забезпечення національної безпеки, винайшли дуже багато ідей та концепцій щодо вдосконалення системи національної безпеки. Одна із таких ідей питання забезпечення безпеки та стійкості важливих інфраструктур країн, що розглядається крізь призму

забезпечення національної безпеки. Також передові країни стали визначати стійкість як пріоритетний напрям розвитку політики у сфері національної безпеки.

Зокрема, розглядаються нові питання Стратегічні документи ЄС, що затверджують Глобальну стратегію ЄС з питань зовнішньої політики та політики безпеки, і НАТО. У липні 2016 року держави-члени НАТО та уряди затвердили завдання забезпечення національної стабільності.

Цей напрям в Україні набув розвитку також і завдяки зусиллям науковців НІСД, які тривалий час здійснювали дослідження у сфері захисту критичної інфраструктури. Саме ці напрацювання лягли в основу схваленої Кабінетом Міністрів України (КМУ) наприкінці 2017 р. Концепції створення державної системи захисту критичної інфраструктури.

Надалі ці ідеї були втіленні в розробці теоретичних засад створення державної БСКІ. З позицій системного підходу сфера відповідальності державної системи БСКІ стосується переважно організаційно-функціональної структури життєдіяльності об'єкта, яка забезпечує взаємодію, обмін ресурсами та інформацією між елементами об'єкта, таким чином, система забезпечення БСКІ може виступати складовою частиною системи забезпечення національної стійкості, а результати її роботи та інформація, що в ній циркулюватиме, будуть використовуватися в рамках цієї більшої системи.

Актуальність цього питання підтверджується гібридними методами ведення війни, які набули поширення в останні десятиліття. Гібридні війни відкрили нові виклики національній безпеці, зокрема, оскільки вони ведуть до: розмиття раніше чітко визначених меж між станом війни та миру та межами національної та міжнародної систем безпеки; поступове ускладнення регулювання міжнародних економічних, політичних та безпекових відносин; зростання екстремізму; нівелювання морально-етичних обмежень щодо використання насильства як окремими країнами, так і громадянами. Усі ці виклики стають загрозою для країн, які не здійснюють адаптацію своєї системи забезпечення національної безпеки до викликів часу. Саме це характеризувало Україну до 2014 р. Система забезпечення національної безпеки України, фактично виявилася неспроможною адекватно відреагувати на виклики, які виникли. Вивчення досвіду України щодо реакції Росії на гібридну війну проти неї стало головним стимулом для перегляду підходи до забезпечення національної безпеки не лише в Україні, а й у ряді інших країн.

Викладений вище огляд національних підходів до забезпечення БСКІ дозволяє сформулювати такі основні висновки щодо побудови аналогічної системи в Україні:

1. Попри наявність загальновизнаних принципів та підходів щодо забезпечення БСКІ кожна національна система є по суті унікальною і неминуче несе на собі відбиток національної специфіки, тому слід уникати механічного копіювання зарубіжного досвіду на українських теренах.

2. Разом із тим, для більшості розвинутих країн, насамперед країн – членів ЄС та НАТО, загальновизнаними є низка основоположних підходів і принципів, які реалізуються при створенні системи БСКІ з тими чи тими варіаціями залежно від конкретних умов:

1) безпека та стійкість критичної інфраструктури належать до пріоритетних завдань секторів національної безпеки і оборони, а відповідна діяльність урегульовується цілою низкою нормативно-правових актів, у т. ч. національного рівня;

2) забезпечення БСКІ здійснюється на системній основі, тобто шляхом створення відповідних національних (державних) систем;

3) системи БСКІ, що створюються, призначені забезпечувати безпеку та стійкість щодо всіх видів фізичних загроз та кіберзагроз;

4) національні системи БСКІ для забезпечення виконання поставлених перед ними цілей повинні:

• удосконалювати механізми та процедури ВОІ на всіх рівнях управління, функціонувати на основі ризик-орієнтованих підходів, чіткого розподілу повноважень і відповідальності щодо КІ (для цього зазвичай визначають відповідальний державний орган або органи);

• розвивати ДПП, взаємодію з іншими суб'єктами системи з метою ефективного залучення населення, суспільства, бізнесу та державних установ і організацій до розв'язання проблем забезпечення БСКІ;

• налагоджувати ефективний обмін інформацією між усіма суб'єктами процесу забезпечення БСКІ;

• забезпечувати виконання функцій інтегрування та аналізу даних для підтримки процесів планування та прийняття рішень стосовно КІ;

• проводити підготовку кадрів і населення для забезпечення БСКІ;

• постійно перевіряти готовність сил і засобів, планів і процедур ВОІ під час регулярних навчань на всіх рівнях управління.

Література

1. Зелена книга з питань захисту критичної інфраструктури в Україні – НІСД, 2015. – URL: http://www.niss.gov.ua/public/File/2015_table/Green%20Paper %20on%20CIP_ua.pdf

2. Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні: матеріали Міжнар. наук.-практ. конф. (7-8 листопада 2013 р., Київ – Вишгород) / упоряд. Д. С. Бірюков, С. І. Кондратов. Київ: НІСД, 2014

3. Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ: НІСД, 2012.

СЕКЦІЯ 7. ОСВІТА Й ОБІЗНАНІСТЬ, ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ

КІБЕРОБІЗНАНІСТЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ЖИТОМИРСЬКОГО ВІЙСЬКОВОГО ІНСТИТУТУ імені С. П. КОРОЛЬОВА: ДОСВІД ТА ПЕРСПЕКТИВИ

Заслужений діяч науки і техніки України,
Грищук Р.В., д.т.н., проф.
Житомирський військовий інститут імені С. П. Корольова,
м. Житомир, Україна

Актуалізація в останні роки проблеми забезпечення кібербезпеки держави потребує кардинального перегляду освітніх програм з підготовки військових та цивільних фахівців в зазначеній галузі [1]. Існуючі освітні програми з підготовки відповідних фахівців як на першому (бакалаврському), так і на другому (магістерському) рівнях в своїй більшості суттєво віддалені від кібербезпекових реалій [2], що призводить до формального віддалення теорії та практики забезпечення кібербезпеки.

Результати аналізу наявного досвіду [3] та існуючої національної інституційної бази [4] дають змогу прийти до висновку, що перед закладами вищої освіти та вищими військовими навчальними закладами в плані автономії відкривається безліч можливостей щодо покращення якості як власних освітніх програм з кібербезпеки зокрема, так і освітнього процесу в цілому. Але, на жаль, з аналізу більшості таких освітніх програм експертним шляхом встановлено – гонитва за новою перспективною спеціальністю зіштовхується з проблемою підміни бажаного з дійсним. Тому в доповіді за мету поставлено розкриття досвіду та перспектив покращення якості підготовки курсантів та студентів високотехнологічних спеціальностей шляхом підвищення рівня їх кіберобізнаності.

Підготовку фахівців в галузі кібербезпеки в Житомирському військовому інституті імені С. П. Корольова (ЖВІ) поставлено ще в 2007 р. За діючими на той час інституційними нормами в ЖВІ здійснювалася підготовка для студентів у галузі знань 1701 “Інформаційна безпека” за напрямом підготовки 6.170101 “Безпека інформаційних та комунікаційних систем” спеціальності 7.17010101 “Безпека інформаційних та комунікаційних систем” за кваліфікацією 3439 “Фахівець із захисту інформації в інформаційно-комунікаційних системах”. Поряд з тим зміни в освітньому середовищі й інші зовнішні та внутрішні фактори обумовили необхідність переходу на нові освітні стандарти.

Перше, що було зроблено – це проведено організаційно-шатні зміни та реформовано кафедру безпеки інформаційно-комунікаційних систем. Її правонаступницею в 2017 р. стала кафедра захисту інформації та кібербезпеки [5], яку укомплектовано висококваліфікованими військовими та цивільними науково-педагогічними працівниками, спроможними підвищити кіберобізнаність навчаємих.

Друге – це розроблено й встановленим порядком через вчену раду військового інституту затверджено нову освітню програму, а також внесено зміни до діючих навчальних планів. Приведення підготовки здобувачів вищої освіти в даній царині до єдиної системи дозволило вибудувати структурно-логічну схему проходження навчальних дисциплін яку, як приклад, приведено на рисунку нижче.

Третє, не менш головне, – набула кардинального розвитку та удосконалення матеріально-технічна база новоствореної кафедри. Було розгорнуто навчально-лабораторний кіберкластер в складі локальної мережної академії *Cisco* та навчальної лабораторії *Кіберполігон*. Локальна мережна академія *Cisco*, розгорнута в ЖВІ, надає можливості здобуття навчаємими цілої низки компетентностей за такими напрямками як *Introduction to Cybersecurity, Cybersecurity Essentials, CCNA Cybersecurity Operations* та ін. [6]. Навчальний кіберполігон, розгорнутий за фінансового сприяння та технічної підтримки науково-

виробничого центру *“Інфозахист”* є унікальним хабом для дослідження та відпрацювання курсантами та студентами заходів протидії кіберзагрозам, місцем для проведення наукових розробок, проведення практичних, лабораторних занять та навчань з кібербезпеки [7].

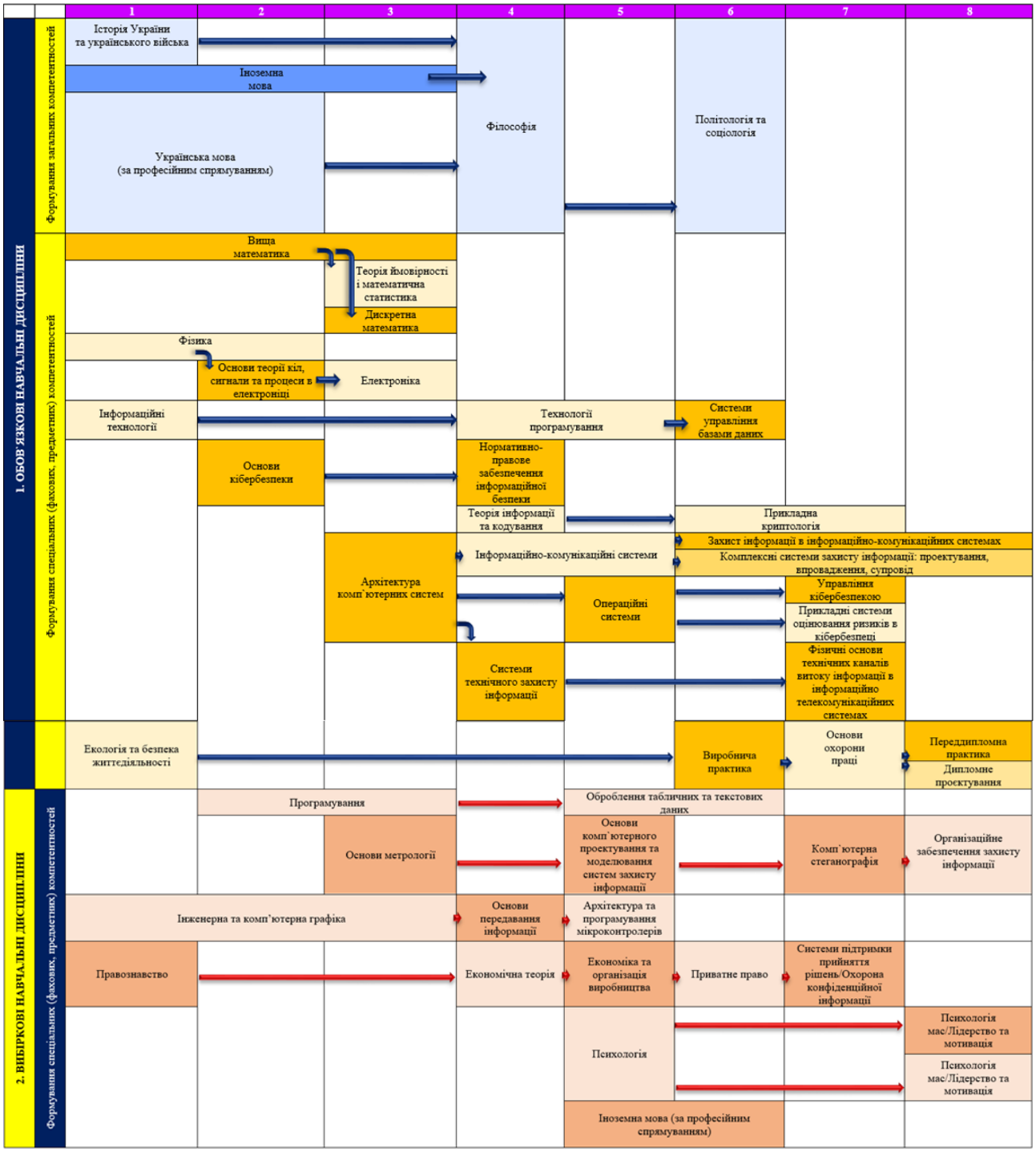


Рис. 1. Траєкторії засвоєння навчальних дисциплін відповідно до структурно-логічної схеми освітньої програми “Кібербезпека” на першому (бакалаврському рівні) студентів заочної форми навчання з числа військовослужбовців військової служби за контрактом

Четвертою особливістю, яка суттєво підняла рівень кіберобізнаності здобувачів вищої освіти в ЖВІ й відрізняє підготовку фахівців від інших закладів вищої освіти та вищих військових навчальних закладів, стало введення наскрізного курсу “Кібербезпека

інформаційно-телекомунікаційних систем” для всіх без винятку спеціальностей та спеціалізацій. Таким чином, в ЖВІ створені всі необхідні та достатні умови для здобуття вищої освіти в галузі кібербезпеки.

Основними перспективами підвищення кіберобізнаності здобувачів вищої освіти в ЖВІ вбачається подальша інтеграція в європейське та євроатлантичне освітнє середовище, входження до провідних світових кіберком’юніті, а також нарощення інтенсивності підготовки науково-педагогічних кадрів – докторів філософії та докторів наук в галузі кібербезпеки.

Література

1. Грищук Р.В. Основи кібернетичної безпеки : монографія / Р.В. Грищук, Ю.Г. Даник ; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.
2. Грабар І.Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька / за заг. ред. проф. Р. В. Грищука. Житомир: ЖНАЕУ, 2019. 280 с.
3. Діордіца І. Освітні стандарти підготовки фахівців із кібербезпеки: теорія і практика. *Національний юридичний журнал*. 2017. №23. С. 50–53.
4. Стандарт вищої освіти України: спеціальність 125- кібербезпека. МОН України. 2018. URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/125-kierbezpeka-bakalavr.pdf.
5. https://www.zvir.zt.ua.
6. Korolyov Zhytomyr Military Institute CISCO ACADEMY URL CISCO. 2018 URL: https://www.netacad.com/portal/managing/details.
7. НВЦ «Інфозахист». *Інфозахист*. 2001. URL: https://infozahyst.com/about/.

КІБЕРБЕЗПЕКА КРАЇН ЄС: МОЖЛИВОСТІ ВДОСКОНАЛЕННЯ

Рабчун Д.І., к.т.н., Парубець Б.Р.
Державний університет телекомунікацій,
м. Київ, Україна

Нині, більшість країн нашого світу мають спроектовані загальнодержавні мережі кібернетичної безпеки, що значно збільшує можливість акумулювання засобами приватного сектору та державних органів боротися з кіберзагрозами, що в свою чергу забезпечує кібербезпеку країн. Це не обходить і країн-членів ЄС.

Взагалі, проблема кібербезпеки тривожить людство ще з часів становлення інформаційно-комунікаційних систем. А ось першим законодавчим актом врегулювання даного питання стала Конвенція Ради Європи про кіберзлочинність, яка з'явилася у Будапешті листопадом 2001 року. Її було ратифіковано більше ніж півсотнею країн. Резонансною подією для ЄС стало ухвалення Стратегії кібербезпеки в рамках ЄС. Її метою вважають відкритий, надійний і безпечний кіберпростір. Щоб забезпечити це належним чином, передбачені заходи з наступних напрямків [4]:

1) досягнення кіберстійкості;

2) суттєве скорочення кіберзлочинності;

3) розробка політики кібероборони, пов’язаної зі Спільною політикою безпеки і оборони;

4) розвиток виробничих і технологічних ресурсів для кібербезпеки;

5) створення узгодженої міжнародної політики кіберпростору для ЄС і просування його основних цінностей.

Стратегія та Порядок денний були опубліковані навесні 2015 року, в липні 2016 року Європейська Комісія оприлюднила «Додаткові заходи по сприянню розвитку індустрії кібер-захисту». Також у липні 2016 року було ухвалено Директиву ЄС 2016/1148 щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (NIS Directive) [5]. Вона є значним досягненням задля збільшення кіберстійкості ЄС та забезпечення відповіді на кіберзагрози в ЄС, оскільки вона базується на формі мінімальної гармонізації, що дає можливість визначити багато деталей окремими країнами-членами Європейського Союзу з супутнім ризиком меншого впливу [6]. Тож для досягнення поставлених цілей, Директива зобов'язала країни-члени ухвалити відповідні національні стратегії, створювати групи зі співробітництва з метою підтримки і сприяння стратегічній співпраці та обміну інформацією між державами-членами та встановлювати вимоги безпеки для операторів цифрових послуг тощо. Також щоб підвищити рівень панєвропейського співробітництва створюються спеціальні мережі та група співробітництва, яка буде забезпечувати планування, керування, обмін інформацією та підготовку звітів щодо стану кібербезпеки в усіх країнах ЄС [6]. Значний вплив на можливості та готовність держав-членів до нового в зазначеній галузі очікується від надання довгострокового стратегічного аналізу кіберзагроз та інцидентів, що дасть можливість визначити нові тенденції, дізнатися про авторитетні рекомендації та звіти з питань кібербезпеки, спрямованих на приватні організації та громадян, допоможе у проведенні експертизи та передового досвіду між державами-членами.

Здавалося, що достатньо всього, щоб країни-члени ЄС мали можливість захистити себе від кібератак, але на жаль це не так. Сучасного законодавства в цій галузі недостатньо. Оскільки більшість проблем кібербезпеки викликана стрімкою потужністю технологічної революція в галузі використання комп'ютерів та телекомунікацій, що призвела до зміни та збільшення апаратного парку, а також суттєвого прискорення швидкості передачі даних, охоплення світового простору інформаційними наземними і мобільними комунікаційними мережами. Все це супроводжувалося збільшенням пропускної спроможності, взаємозв'язаності та швидкодії інформаційних систем [5]. Щоб вдосконалити кібербезпечність, перш за все необхідно приділяти достатньо уваги питанням безпеки та конфіденційності при проектуванні та експлуатації хмарних додатків. Хмарні додатки – це парадигма, що передбачає віддалену обробку та зберігання даних. По-друге, необхідно забезпечити нормативно-правову базу, яка може протистояти як поточним, так і майбутнім викликам, які ставить перед ним науково-технічний прогрес. Також варто зазначити, що необхідно забезпечити заохочення переходу державних та недержавних структур до систем із відкритим початковим кодом і використання ліцензійно-чистих відкритих форматів даних [7], що дозволяє не тільки підвищити стійкість роботи відповідних підрозділів, але й однозначно заощадити значні бюджетні кошти.

Таким чином, хоча кібербезпека ЄС набирає нових обертів і шляхом створення нового законодавства, однак через те, що стрімко почався розвиток технологій, інформаційний прогрес спричинив проблему захищеності персональних даних через виникнення глобальних лідерів, що призвело до концентрації інформації в руках «великих гравців мережі». Що в свою чергу тягне за собою необхідність вдосконалення як прогалин в законодавстві, так і звернення уваги на проблеми створення нових додатків та інформаційних просторів.

Література

1. Василенко М. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства. *Юридичний вісник*. 2018. № 3. С. 17–24.
2. Василенко М. Якість кібербезпеки інформаційно-комунікаційних систем (ІКС) та деякі законодавчі питання щодо її підвищення. *Юридичний вісник*. 2018. № 4.
3. Резолюція Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки» від 20 грудня 2002 р. № 57/239 URL: http://www.un.org/ru/ga/second/57/second_res.shtml

4. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union. URL: https://ec.europa.eu/digital-singlemarket/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity.
5. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*. 2016. L. 194. P. 1-30.
6. Tauwhare, R. (2016). Improving cybersecurity in the European Union: the Network and Information Security Directive. *Journal of Internet Law*, 19(2), 1–12.
7. Schmidthuber L., Stütz S., Hilgers D. Outcomes of open government: Does an on-line platform improve citizens' perception of local government? *International Journal of Public Sector Management.* 2019.

РОЛЬ НАВЧАЛЬНИХ КІБЕРПОЛІГОНІВ У ПІДГОТОВЦІ ФАХІВЦІВ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Гуменюк І.В., к.т.н., Жуков А.О., Розенцвіт М.О.
Житомирський військовий інститут
імені С. П. Корольова,
м. Житомир, Україна

Аналіз стану кіберпростору держави свідчить про те, що сучасні методи та способи реалізації цих загроз постійно змінюється та модернізується. Прикладом того є застосуванням спецслужбами Російської Федерації технологічно-удосконалених ботнет-мереж для проведення успішних кіберакцій у мережах інформаційно-телекомунікаційних систем державного та військового призначення. Тому в умовах, що склалися актуальним є модернізація існуючих систем захисту об'єктів критичної інфраструктури для забезпечення відповідного рівня кібербезпеки.

Одним з перспективних напрямів технологічного досягнення такої мети є проектування, розробка та застосування навчально-лабораторних комплексів – кіберполігонів. Кіберполігон – це спеціальне середовище, яке являє собою сукупність спеціалізованого апаратно-програмного забезпечення, об'єднаного мережними комунікаціями, що може бути інтегрованим до мережі Інтернет, та призначене для підвищення рівня технічної підготовки персоналу при вирішенні ними спеціальних завдань (протидії кібертероризму, кіберзлочинності, забезпечення кібероборони тощо) та випробування новітніх технологій гарантування кібербезпеки [1, с. 152].

Технічно структура Кіберполігону складається з двох функціонально-пов'язаних кластерів: комплекту кібероборони (кібербезпеки, кіберзахисту) та кіберрозвідки (тестування на кіберзахищеність) відповідно. Програмним ж ядром є новітній дестрибутив операційної системи сімейства Linux. Функціональне призначення програмної та апаратної складових визначається безпосередніми класами задач кожного із компонентів Кіберполігону.

На теперішній час з урахуванням аналізу передового досвіду застосування сучасних навчально-лабораторних комплексів на базі Житомирського військового інституту імені С. П. Корольова розгорнутий та ефективно функціонує комплекс Кіберполігон [2] для проведення науково-практичних досліджень, відпрацювання навчальних заходів з протидії гібридних впливів у кіберпросторі, якісної підготовки фахівців із кібербезпеки. Особливістю застосування навчально-лабораторного комплексу Кіберполігон є реальна можливість удосконалення практичних навичок курсантами (студентами) у вигляді командних (групових) змагань, зокрема таких як Capture The Flag, Escape Route тощо.

Такий підхід забезпечує підвищення кваліфікації кіберспеціалістів, проведення наукових досліджень, ознайомлення з особливостями протидії кібернетичним загрозам та впливам в кіберпросторі, висококваліфіковану підготовку військових та цивільних фахівців з галузі кібербезпеки.

Література

1. Грищук Р. В. Кіберполігон як навчальне середовище з метою підготовки персоналу для боротьби з кіберзлочинністю. Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукр. наук.-практ. конф. Одеса: Одеський держ. ун-т внутр. спр., 2017. С. 152-153.
2. Навчальний кіберполігон відкрили в Житомирському військовому інституті. URL:https://censor.net/ua/photo_news/3222663/navchalnyyi_kiberpoligon_vidkryly_v_jytomyrskomu_viyiskovomu_instytuti_fotoreportaj.

КОНЦЕПЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ “ІНФОРМАЦІЙНА БЕЗПЕКА ОСОБИСТОСТІ, СУСПІЛЬСТВА, ДЕРЖАВИ”

Супрунов Ю.М., к.і.н., Жарков Я.М., к.і.н., доц.
Військовий інститут Київського національного університету імені Тараса Шевченка;
Бабенко О.П.
Національний університет оборони України імені Івана Черняховського
м. Київ, Україна

Прискорений розвиток інформаційного суспільства, недостатньо контрольоване поширення новітніх інформаційних технологій, утворення глобального інформаційного простору призвело до того, що інформаційні технології стали основним каналом / джерелом інформації для кожної людини, здійснюють безпосередній вплив на її психічну діяльність, формування її соціальної поведінки. Фактично навкруги людини створюється її індивідуальний "віртуальний інформаційний простір" з можливістю практично безперешкодного доступу, моніторингу та диференційованого інформаційно-психологічного впливу (ІПсВ) на конкретну особистість. Людина в цих умовах може втратити свою незалежну особистість, перетворитись у "віртуальний біоресурс" для рефлексивного управління і інформаційно-психологічних маніпуляцій.

Це посилює можливості безпосереднього ІПсВ на населення країни, особовий склад її збройних сил, інших військових формувань, що ускладнює ефективне вирішення завдання їх інформаційного захисту з боку відповідних державних структур без усвідомленої допомоги самої людини.

Тому є виключно важливим забезпечити безпеку взаємодії людини з інформаційними технологіями (інформаційним середовищем) шляхом отримання певного мінімуму знань про закони розвитку інформаційного суспільства (його окремі негативні чинники і ризики), нормативно-правові засади забезпечення інформаційної / кібернетичної безпеки, можливий деструктивний вплив та основи захисту від інформаційних загроз для особистості і суспільства. Це завдання особливо актуальне відносно молоді, осіб, що отримують вищу освіту з усіх галузей знань / спеціальностей, особливо у сфері інформаційних технологій.

Аналіз досвіду підготовки фахівців з вищою освітою у провідних країнах світу доводить, що така підготовка організована в межах освітньо-професійних програм бакалавра (магістра) як в рамках окремих навчальних дисциплін, так і шляхом створення комплексних навчальних курсів на базі окремих розділів, тем / занять відповідних навчальних дисциплін, спеціалізованих семінарів тощо. У складі комплексного навчального курсу з інформаційної

безпеки як змістовне і функціональне ядро доцільно мати окрему навчальну дисципліну «Інформаційна безпека особистості, суспільства, держави» («Безпека інформаційного середовища) та окремі розділи (теми, заняття, навчальні питання) інших навчальних дисциплін, що викладаються у певній логічній послідовності.

Метою викладання навчальної дисципліни "Інформаційна безпека особистості, суспільства, держави" є формування сучасних поглядів з теоретичних основ інформаційної безпеки особистості, суспільства і держави, технологій здійснення негативних ІПсВ на систему державного управління, суспільство, особистість та шляхів захисту від них, формування вмінь та прищеплення первинних практичних навичок з організації та забезпечення інформаційної (кібернетичної) безпеки з урахуванням специфіки професійної діяльності фахівця з вищою освітою відповідної спеціальності.

Навчальна дисципліна розглядає базові поняття та нормативно-правові засади інформаційної безпеки, інформаційні ризики / загрози, загальний алгоритм забезпечення інформаційної безпеки особистості, суспільства, держави як складової національної і воєнної.

Основною компетентністю, яка набувається в результаті засвоєння навчальної дисципліни є здатність до участі у проведенні заходів із забезпечення інформаційної (кібернетичної) безпеки особистості, суспільства, держави, виявлення застосування технологій негативних ІПсВ на систему державного управління, суспільство, особистість, визначення шляхів захисту інформаційної безпеки України.

Робоча навчальна програма зазначеної навчальної дисципліни обсягом від 4 кредитів може передбачати 5 основних тем / розділів:

основи інформаційної (кібернетичної) безпеки держави – організаційно-правові аспекти;

інформаційні війни як джерело загроз національній безпеці України;

інформаційна безпека держави;

інформаційна безпека суспільства;

інформаційна безпека особистості.

В процесі викладання навчальної дисципліни вивчаються:

теоретичні та прикладні аспекти забезпечення інформаційної безпеки держави у воєнній сфері;

технології інформаційного впливу;

засоби масових комунікацій в інформаційному протиборстві;

загальна система забезпечення інформаційної безпеки відповідних структур;

основні методи безпечного використання сучасних інформаційних технологій.

Методика вивчення дисципліни крім лекційних і семінарських занять передбачає інтенсивні практичні заняття та самостійну роботу студентів, комплексування навчальних занять за навчальним планом та факультативних занять, застосування деяких активних методів навчання, які використовуються для організації навчання у стислі терміни, зокрема:

методів "занурення", проектів, навчання у співробітництві, які реалізовувались комплексним змістовним поєднанням практичних занять, військово-наукової роботи, факультативної підготовки рефератів (з їх обов'язковим публічним захистом), читацьких конференцій, робота в міні-групах над додатковою літературою (реалізація принципу "знання кожного – знання всієї групи"), контекстного навчання в умовах регулярного залучення студентів до забезпечення інформаційних заходів в інституті тощо. Частина питань відпрацьовується методом «від зворотнього».

Зрозуміло, що вивчення даної навчальної дисципліни за визначений бюджет навчального часу у певному семестрі забезпечить надання певного обсягу знань та вмінь, але не може забезпечити формування спроможностей з власного інформаційного самозахисту на рівні, що дозволить ефективно протистояти деструктивним ІПсВ. Це завдання більш тривалого часу на протязі усього терміну навчання. Система підготовки фахівців з вищою освітою в контексті інформаційної безпеки повинна забезпечувати організаційні умови

активізації їх навчальної діяльності, які сприяють постійному і послідовному розвитку визначених вмінь та спроможностей, розширенню загального світогляду, забезпеченню сформованості визначених компетенцій у встановлені терміни навчання.

Таким чином, доцільно згадати досвід формування комплексних навчальних курсів, які поєднують у логічній послідовності змістовні елементи до 4–6 навчальних дисциплін як варіативної, так і нормативної складової освітньо-професійних програм. Зокрема, комплексний навчальний курс з інформаційної безпеки міг би також передбачати низку факультативних занять та планове залучення студентів до організації і проведення відповідних заходів виховної роботи, повсякденної діяльності та деяких масових заходів.

Введення до навчальних планів підготовки фахівців з вищою освітою навчальної дисципліни "Інформаційна безпека особистості, суспільства, держави" та комплексного навчального курсу з інформаційної безпеки сприятиме не тільки вирішенню завдань забезпечення інформаційної безпеки держави, але й в комплексі з іншими освітніми заходами з визначеними категоріями населення країни забезпечить спроможність особистості до інформаційного самозахисту, сприятиме адаптації особистості і суспільства до життя в інформаційному суспільстві, зниженню ефективності деструктивних інформаційних впливів.

ВИКОРИСТАННЯ СПЕЦІАЛІЗОВАНОГО КЛАСУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОЇ ФОРМИ НАВЧАННЯ

Супрунов Ю.М., к.і.н., Степанишин Р.Д., Дубовський О.Г.
Військовий інститут Київського національного університету імені Тараса Шевченка
м. Київ, Україна

Розвиток інформаційних технологій (ІТ) призводить до трансформації всіх сфер сучасного життя. Не виключенням є військова справа, оскільки застосування ІТ в процесі планування, організації і ведення бойових дій значно впливає на успіх дій військових формувань. Впровадження ІТ в освітній процес суттєво змінює його характер, розширює можливості, але й створює нові проблеми, висуває підвищені вимоги до кваліфікації науково-педагогічних працівників та рівня навчально-лабораторної бази. Особливо це характерно для організації підготовки фахівців у сфері ІТ, яка повинна використовувати ІТ не тільки для забезпечення навчального процесу, але й навчати слухачів використовувати ІТ у своїй професійній діяльності.

Виходячи з цього кафедрою зарубіжної воєнної інформації ВІ КНУ імені Тараса Шевченка проводиться робота з удосконалення навчально-лабораторної бази підготовки фахівців у сфері інформаційно-аналітичної діяльності. З цією метою у 2020 році на кафедрі був розгорнутий новітній спеціалізований клас інформаційних технологій (СКІТ), призначений для проведення всіх видів занять та самостійної роботи за напрямком підготовки.

Зважаючи на особливості зазначених програмних засобів та інші завдання, які повинні виконуватись курсантами в процесі навчання, конфігурація СКІТ вибиралась виходячи з наступних вимог:

кількість робочих місць не менше ніж одна ПЕОМ на двох слухачів (розгорнуто 13 робочих місць слухачів та робоче місце викладача, що забезпечує проведення занять з кожною з навчальних груп з 1 по 6 курси);

ПЕОМ з продуктивністю, яка забезпечує обробку потокової відео та аудіо інформації в комплексі з забезпеченням інших завдань;

конфігурація ПЕОМ з двома моніторами, що дає змогу розширити робоче поле користувача, збільшує продуктивність роботи та забезпечує комфортну роботу двох курсантів (для великих груп);

організація робочих місць у локальну мережу із забезпеченням високошвидкісного доступу до мережі Інтернет з кожного з них;

використання в якості основного демонстраційного засобу електронної сенсорної панелі як для роботи в локальній мережі, так і з автономним доступом до мережі Інтернет.

Необхідно зазначити, що організація локальної мережі була здійснена за клієнт-серверною архітектурою, але з метою оптимізації серверна частина була розгорнута на ПЕОМ викладача з широким використанням засобів віртуалізації (зокрема, це дало змогу відмовитись від окремого сервера та змонтувати серверну операційну систему як "віртуальну машину"). Крім того, на ПЕОМ викладача було встановлене програмне забезпечення для контролю поточної роботи слухачів та введення певних обмежень використання ПЕОМ у разі необхідності.

Незважаючи на специфічну конфігурацію СКІТ, пандемія 2020 року відразу визначила питання про використання його ресурсів для організації дистанційної форми навчання для забезпечення неперервної підготовки слухачів в умовах карантинних обмежень. Це завдання було успішно виконано певним удосконаленням СКІТ шляхом організації доступу до різних платформ дистанційного навчання та дообладнання класу засобами відеозв'язку (вебкамерами).

Організація занять на кафедрі спеціалізації має свої особливості, які сприяли забезпеченню необхідної якості дистанційного навчання:

заняття в СКІТ проводились виключно з навчальними групами за спеціалізацією кафедри з 1 по 6 курси (лекційний потік – 1 навчальна група), що визначає більш високий рівень керованості слухачів та ефективності занять, у тому числі за дистанційною формою;

належний рівень самоорганізації кожної навчальної групи (підготовлений командир групи, здатний забезпечити порядок і дисципліну; відповідальний за навчальну дисципліну – постійна контактна особа з викладачем, яка виконувала певні функції диспетчеризації при підготовці до занять та зворотного зв'язку; 1-2 слухача підготовлених до експлуатації обладнання класу, технічної підтримки, у т.ч. для оперативного усунення апаратно-програмних збоїв);

активне використання відпрацьованої і зрозумілої кожному слухачу з початку навчання кредитно-модульної системи організації навчального процесу та модульно-рейтингового контролю знань та вмінь, якість і повнота лекційних та інших методичних матеріалів, що надаються слухачам;

організація роботи слухачів при підготовці і проведенні більшості занять у складі команд (мікрогруп) для забезпечення командного впливу на кожного слухача та підвищення мотивації їх роботи;

методика проведення практичних занять, яка у т.ч. передбачає розподілений пошук інформації з використанням глобальної мережі Інтернет, її аналітичну обробку та підготовку аналітичних документів, ІТ-продукції та відповідних доповідей-презентацій.

Дообладнання СКІТ надало можливість проведення дистанційної форми занять зі слухачами за спеціалізацією кафедри викладачами різних інститутів і кафедр університету, які використовували декілька платформ дистанційного навчання та різні методики проведення занять.

Проведення семінарських та окремих практичних занять у формі дистанційних відео-конференцій також надає можливість залучення до них провідних фахівців у певних галузях, замовників на підготовку фахівців (для ознайомлення з рівнем підготовки слухачів та надання рекомендацій) тощо.

В цілому успішний досвід використання СКІТ для проведення занять за дистанційною формою показав ряд особливостей, які необхідно враховувати при організації зазначеного процесу, зокрема:

важливо забезпечувати доступ до різних дистанційних платформ (Zoom, TeamViewer, MS Teams, дистанційної платформи університету тощо) для досягнення більшої гнучкості в організації навчального процесу. Необхідно звертати увагу на відмінності в дистанційних платформах і на набір додаткових інструментів, які вони пропонують;

при роботі з великою групою добре себе зарекомендувала електронна сенсорна панель, особливо під час проведення лекційних занять та в умовах неможливості забезпечити слухачів достатньою кількість вебкамер. В таких умовах викладач мав змогу контролювати процес навчання за допомогою основної вебкамери закріпленої на сенсорній панелі;

забезпечення слухачів засобами комунікації (у випадку СКІТ – професійними аудіогарнітурами) дало змогу якісно проводити семінарські заняття, забезпечувати зворотний зв'язок між викладачем та слухачами, а останнім – можливість якісно презентувати власні розробки і брати участь в обговореннях;

проведення дистанційних занять значно залежить від технічних умов (справність ПЕОМ, швидкість доступу до мережі Інтернет та якість такого доступу, вчасне оновлення програмного забезпечення тощо), що в ряді випадків вимагає залучення для організації занять підготовленого технічного персоналу;

незважаючи на всі переваги, дистанційна форма навчання вимагає від навчальних груп високого рівня організованості та самодисципліни, що при централізованому проведенні дистанційних занять потребує проведення періодичного контролю.

Таким чином, організація навчального процесу на кафедрі, різноманіття сучасних технологічних і програмних рішень, а також використання технічних можливостей СКІТ дали можливість в умовах пандемії якісно організувати та на високому рівні проводити заняття за дистанційною формою.

Разом з тим, позитивний досвід впровадження зазначених рішень продемонстрував важливість врахування всіх технічних та організаційних особливостей процесу дистанційного навчання, необхідність завчасної підготовки і залучення навченого персоналу для уникнення збоїв та оперативного вирішення виникаючих проблем.

ПІДХІД ДО ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ НАСЕЛЕННЯ ДЕРЖАВИ У КІБЕРПРОСТОРІ

Міхєєв Ю.І., к.т.н., Носова Г.Д.
Житомирський військовий інститут імені С. П. Корольова
м. Житомир, Україна

Стрімкий розвиток інформаційних технологій сприяв розширенню переліку сфер життя суспільства, залучених до кібернетичного простору і, одночасно, розширили можливості щодо здійснення впливів на населення держави як соціальний компонент цього простору. При чому, вплив на зазначений компонент здійснюється як через технологічні вразливості, так і через інформаційну складову шляхом впровадження методів інформаційно-психологічного впливу, технологій маніпуляції у інформаційні повідомлення та подальшого їх розповсюдження через засоби масової комунікації.

Несвоєчасне реагування на загрози інформаційно-психологічній безпеці населення держави може поступово призводити до невдоволення населення рішеннями (прийнятими законами) керівництва держави, активізації акцій протестів проти діючої влади, "кольорових революцій", терористичних актів та збройного конфлікту в середні держави [1, с. 37]. Отже, актуальним на сьогодні є завдання своєчасного виявлення ознак інформаційно-психологічного впливу в кіберпросторі та впровадження дієвих контрзаходів.

У цілому виявлення ознак інформаційно-психологічного впливу передбачає проведення контент-аналізу інформаційних повідомлень. У роботі наведено основні етапи оцінювання текстових повідомлень з метою виявлення в них ознак інформаційно-психологічного впливу:

оцінювання повідомлення для визначення рівня сприйняття цільовою аудиторією;
оцінювання сенсаційності повідомлення;
оцінювання повідомлення за емоційним впливом на підсвідомість;
оцінювання повідомлення на предмет наявності методів психологічного впливу;
оцінювання аргументованості викладених фактів у повідомлені.

Оцінювання текстового повідомлення для визначення рівня сприйняття цільовою аудиторією пов'язане з визначенням рівня читабельності та доступності тексту [2, с. 8]. При цьому доцільно використати такі показники: індекс туманності Ганнінга [3], індекс Флеша-Кінкейда, індекс SMOG, індекс Колемана-Ліу [4, с. 283] та індекс зручності читання [5, с. 82]. За проведеними розрахунками аналітик отримує інформацію безпосередньо про характеристику освіченості цільової аудиторії, на яку цей контент розраховано.

Оцінка сенсаційності повідомлення є досить інформативним параметром про наявність текстовому контенті ознак інформаційно-психологічного впливу. Виявлення часткових показників сенсаційності здійснюється методами контент-аналізу та Text Mining. У роботі запропоновано інтегральний показник оцінювання сенсаційності повідомлення, який враховує рівень уваги цільової аудиторії, рівень несподіваності, рівень підсилення значущості тексту, рівень звернення до лідера.

Розглядаючи інформаційно-психологічний вплив як спонукання до дії, зрозуміло, що найкращий спосіб досягнення цієї мети є створення такого контенту, який у першу чергу впливатиме на первісні людські реакції, тобто змусить цільову аудиторію у своїх діях керуватися емоціями. Тож при аналізі контенту важливою характеристикою є емоційна насиченість повідомлення. У роботі запропоновано інтегральний показник оцінки емоційної насиченості повідомлення, який враховує рівень вираження ознак об'єкта, рівень лексичних порівнянь, рівень вигуків, рівень позначення дії, рівень акцентування.

Для визначення методів психологічного впливу, застосованих при формуванні текстового контенту повідомлення, використовуються прийоми якісного контент-аналізу у поєднанні з механізмами фільтрації тексту на предмет виявлення ключових слів за визначеними тематиками. При цьому важливо конкретизувати використані при формуванні маніпулятивного текстового контенту методи психологічного впливу, до яких відносяться: "розвішування ярликів", "спрощення", "доступне пояснення", "цитата та рекомендації", "статистика", а також спосіб апеляції – "легітимність". У роботі запропоновано ідентифікувати методи за показниками, які враховують рівень штампування, рівень неоднозначності висловлювань, рівень посилання на думку авторитетів, рівень посилання на думку загалу, рівень посилання на інші джерела, рівень цифрової насиченості.

Ступінь аргументованості повідомлення – показник, при аналізі якого можна отримати дані по виду маніпулятивного впливу, закладеного у текстовому контенті. У роботі запропонований інтегральний показник, який складається з двох часткових показників: рівня посилання на анонімне джерело та рівня авторизованості думки. Рівень авторизованості думки характеризує посилання або на авторитетну думку, або на особисті роздуми автора. При цьому маніпулятивність технології спирається на психологічну особливість людини покладатися на судження "спеціаліста".

На нашу думку, застосування викладеного у доповіді методичного підходу з виявлення інформаційно-психологічних впливів на соціальний компонент кібернетичного простору доцільно використовувати при розробці відповідних автоматизованих систем, що у, свою чергу, забезпечить своєчасне виявлення інформаційних загроз та подальше адекватне реагування на них з метою підвищення рівня кібербезпеки держави.

Література

1. Молодецька-Гринчук К. В. Семантичний аналіз текстового контенту для виявлення інформаційних впливів на акторів у соціальних інтернетсервісах: матеріали міжнар. наук.-практ. конф. *Проблеми і перспективи розвитку ІТіндустрії*. Харків, 2017. С. 58.
2. DuBay W. H. The Principles of Readability. *Costa Mesa*. California: Impact Information, 2004. 74 p.
3. Gunning R. The technique of clear writing. New York: NY:McGraw-Hill International Book Co, 1952. 157 p.
4. Coleman M. A, Liau T. L. Computer readability formula designed for machine scoring. *Journal of Applied Psychology*. 1975. №60. P. 283–284.
5. Кричковська А.М., Паращин Ж.П., Швед О.В., Губицька І.І., Болібрух Л.Д., Новіков В.П. Застосування інформаційних технологій для стандартизації методології створення навчальної літератури. *Вісник Національного університету "Львівська політехніка*". 2014. № 803: Інформатизація вищого навчального закладу. С. 81–85.

СЕРТИФІКАЦІЯ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СВІТОВИЙ ДОСВІД ТА ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

Яровий І.І.
Державний Університет телекомунікацій
м. Київ

Як свідчить статистика, людський чинник грає визначальну роль у здійсненні порушень інформаційної та кібербезпеки. Згідно зі звітом Cyber Risk Analytics «2019 Midyear Quick View Data Breach Report», в першій половині 2019 року було виявлено понад 3800 інцидентів кібербезпеки, в результаті чого було скомпрометовано понад 4,1 мільярда інформаційних повідомлень. Ця цифра на 54% більше в порівнянні з тим же періодом 2018 року. Понад 60% виявлених порушень були результатом людських помилок. З огляду на зазначене, очевидною є нагальна потреба в освіті в галузі кібербезпеки.

Вітчизняні та зарубіжні вчені у своїх роботах розглядають сучасні підходи до підготовки фахівців у сфері інформаційної та кібербезпеки, аналізують досвід використання систем кібербезпеки західних партнерів та пропонують загальні підходи щодо організації системи освіти в галузі кіберзахисту. Проте недостатньо досліджено питання щодо аналізу світового досвіду підготовки фахівців в рамкам курсів підвищення кваліфікації та сертифікації.

З метою формування якісної програми підготовки фахівців в рамках курсової підготовки проведено аналіз відомих світових систем підготовки та сертифікації фахівців в галузі інформаційної та кібербезпеки, які сьогодні вважаються лідерами, серед них:

- CISM (Сертифікований менеджер з інформаційної безпеки);
- CISSP (Сертифікований професіонал з безпеки інформаційних систем);
- CISA (Сертифікований аудитор з інформаційної безпеки);
- CEH (Сертифікований етичний хакер);
- CompTIA Security+ (Сертифікований IT-спеціаліст з безпеки);
- GSEC (Сертифікований спеціаліст з основ інформаційної безпеки) та інші.
- У результаті аналізу основних сертифікаційних курсів встановлено наступне:
- система підготовки, як правило, передбачає невеликий термін навчання – 1 тиждень;
- підготовка, містить як базову так спеціалізовану компоненту;

- базова підготовка націлена на розгляд загальних понять і принципів роботи, а також на використання класичних, загальновизнаних і, як правило, відкритих апаратних та програмних платформ;
- спеціалізована підготовка, в більшості, заснована на використанні окремих, складних комерційних продуктів або власних розробок компанії, які пропонується придбати після проходження підготовки;
- підготовка є постійним і обов'язковим процесом роботи спеціаліста в сфері інформаційної безпеки, оскільки прийоми та методи проведення кібератак постійно змінюються;
- підготовка передбачає різні форми проведення: з викладачем, з використанням електронних та паперових підручниками, відеофільмів, онлайн-тестів та спеціальних платформ для навчання;
- обов'язковим елементом є проведення складного комплексного екзамену з видачею відповідного сертифікату;
- термін дії такого сертифікату в більшості випадків не перевищує трьох років, що відповідає загальній тенденції розвитку технологій в сфері інформаційної та кібербезпеки;
- спеціалістам пропонуються системи курсової підготовки, так звані «дорожні карти», які складаються як в рамках підготовки в одній компанії, так і в рамках підготовки в різних навчальних центрах та компаніях.

Під час розробки програм базової підготовки фахівців за напрямом інформаційної та кібербезпеки пропонується, в першу чергу, розглядати наступні питання: вивчення вимог керівних документів, що регламентують питання інформаційної та кібербезпеки; вивчення досвіду країн-партнерів НАТО в даній галузі; стислий огляд відомих світових та вітчизняних систем підготовки, в першу чергу, можливостей пройти додаткове навчання самостійно та дистанційно й отримати відповідний сертифікат; огляд продуктів відомих світових і вітчизняних виробників апаратного та програмного забезпечення для інформаційної та кібербезпеки; вивчення питань практичного застосування загальнодоступних програмних та апаратних рішень.

Література

1. Best InfoSec and Cybersecurity Certifications of 2020. 2020. URL: https://www.businessnewsdaily.com/10708-information-securitycertifications.html)
2. Кибербезопасность: Типовой учебный план – NATO. 2016. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20171004_1610-cybersecurity-curriculum-r.pdf
3. Sabillon R. and other. Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada Journal of Cases on Information Technology. 2019. 21(3). URL: https://www.igi-global.com/article/an-effective-cybersecuritytraining-model-to-support-an-organizational-awareness-program/227676
4. Діорбіца І. Стан підготовки фахівців у сфері кібербезпеки. Visegrad Journal on Human Rights. 2016. 6/1. URL: http://vjhr.sk/archive/2016_6/part_1/11.pdf
5. Даник Ю., Зінченко А. Кіберосвіта та її особливості. *Військова освіта*. 2018. №2(38). С. 67–84. URL: http://znpvo.nuou.org.ua/article/download/160748/161579

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ СЕРВІСІВ ДЛЯ ПОШУКУ ТА АНАЛІЗУ СТОРІНОК В СОЦІАЛЬНІЙ МЕРЕЖІ

Гуревич Ю.А.
Військовий інститут Київського національного університету імені Тараса Шевченка
м. Київ, Україна

Більшість експертних висновків говорять, що 90 відсотків необхідної інформації, яка добувається відповідними аналітичними структурами, поступає з відкритих джерел. Соціальні мережі, різноманітні сайти, форуми все це відкриває безліч можливостей для проведення розслідувань, а також для прийняття управлінських рішень. Осмислення цих можливостей необхідне для покращення інформаційних спроможностей структур розвідки з відкритих джерел (Open source intelligence, OSINT).

Одне із базових завдань, яке ставиться перед підрозділами OSINT є пошук інформації про конкретну фізичну особу чи групу людей. Для цього використовують різні методи збору інформації. Але, в першу чергу, аналізуються персональні сторінки в соціальних мережах, адже більшість людей активно веде свої сторінки в соціальних мережах: постить фотографії, пише пости, добавляє друзів і «лайкає» їх фотографії, відмічає своїх родичів. Така їх активність допомагає фахівцям, які проводять OSINT, збирати необхідну інформацію.

Особливу цікавість представляє російська соціальна мережа ВКонтакте, яка є достатньо поширеною (заборонена в Україні). Починати пошук варто із окремого акаунта, який не має бути пов'язаний із основним акаунтом фахівця OSINT. Акаунти не мають бути пов'язанні між собою електронними скриньками, номерами телефонів чи наповненням контенту. Варто зберігати повну анонімність під час пошуку інформації.

Починати аналіз інформації варто з огляду профіля ВК, адже по ньому можна зібрати первинну інформацію. Так, можна дізнатися місце проживання особи, групи, в яких вона бере участь, адже це можуть бути як групи по інтересам, так і групи пов'язані з професійною діяльністю, іншими об'єктами, які пов'язані з інтересами даної особи. Знаючи в яких групах є людина, ми можемо сформувати попередню картину особистості. Вся ця інформація в залежності від поставлених завдань може бути корисною для фахівця OSINT.

Безпосередній аналіз профілю та відповідної особи потрібно здійснювати за допомогою сторонніх ресурсів, які допомагають автоматизувати деякі процеси. Використовувати можна наступні ресурси у певній послідовності (певним алгоритмом аналізу інформації) [1, с. 203].

YASIV [2]. Корисний сервіс, який допомагає аналізувати друзів, здійснює пошук серед друзів та встановлює взаємозв'язки між ними. Він створює візуалізацію зв'язків між друзями, а також показує хто в кого є у друзях. Завдяки цьому сервісу, також, можна шукати дубльовані та фейкові сторінки.

220VK [3]**.** З точку зору OSINT тут є багато корисних функцій, які можна використовувати: можна побачити коли користувач останній раз був в мережі, які сторінки він лайкає, з яких міст його друзі; онлайн-трекер дозволяє дізнатись коли людина буває онлайн. Також даний ресурс дозволяє шукати друзів користувача, якщо його сторінка закрита.

VK.city4me [4]**.** По функціоналу він зхожий на попередній сервіс, проте доповнює його. Так, завдяки цьому сервісу можна детально проаналізувати активність користувача, дізнатися з якого пристрою він заходив і скільки був онлайн, а також відслідковувати активність друзів.

Vkdia [5]**.** Дозволяє аналізувати активність друзів, а також порівнювати її з активністю самого об'єкта. За результатом видає ймовірні варіанти з ким наш об'єкт міг спілкуватися. Якщо довше моніторити сторінку, то можна доволі точно визначити круг спілкування особи.

Photo-map [6]**.** Дозволяє ставити точку на карті і шукати фото в певному радіусі від цієї точки. Також можливо налаштовувати конкретні параметри пошуку.

Глаз Бога [7]**.** Це корисний телеграм-бот, який дозволяє уточнювати інформацію по об'єкту за допомогою фотографій, номеру телефону, нікнейму. Видає приблизні фотографії, де може бути об'єкт, показує оголошення, які пов'язані із номером телефону об'єкта. Одним словом, доволі сильно полегшує роботу для того, хто збирає інформацію.

Отже, процес збору інформації з соціальної мережі ВКонтакте є доволі ресурсозатратним, адже необхідно зібрати та проаналізувати великі обсяги інформації, що звісно займає багато часу. Тому для спрощення роботи необхідно використовувати вищезазначені сервіси, так як вони в значній мірі дозволяють автоматизувати процес збору та аналізу інформації. З точки зору OSINT соціальна мережа ВКонтакте є чудовим відкритим джерелом для пошуку інформації на конкретну особу.

В умовах обмежених ресурсів використання даних сервісів відповідними аналітичними структурами дозволить підвищити їх пошукові можливості. Однак, все ж таки необхідно вести розробку і власного програмного забезпечення для пошуку та моніторингу інформації , автоматизації процесів пошуку і обробки інформації. Все це потребує більш комплексного підходу, щодо ефективного вдосконалення системи OSINT відповідних структур нашої держави.

Література

1. Nihad A. Hassan, Rami Hijazi. Open Source Intelligence Methods and Tools A Practical Guide to Online Intelligence. 2018. p. 203-205
2. Онлайн сервіс YASIV URL: https://www.yasiv.com/vk
3. Онлайн сервіс 220vk URL: https://220vk.com
4. Онлайн сервіс VK.city4me URL: http://vk.city4me.com
5. Онлайн сервіс vkdia URL: https://vkdia.com
6. Онлайн сервіс photo-map URL: http://photo-map.ru/
7. Онлайн сервіс eyeofgod URL: https://eyeofgod.info/

ІНФОРМАЦІЙНІ ВПЛИВИ НА ЖИТТЯ СУСПІЛЬСТВА

Малявін Є.В.
Національний технічний університет "Харківський політехнічний інститут"
м. Харків, Україна

В сучасному світі володіти достовірною інформацією означає ефективно управляти соціальним середовищем, гарантовано маючи високий ступінь оптимізації діяльності, що сприяє не тільки вдосконаленню особистості, а й консолідації малих груп та стає найважливішим завданням соціальної практики сьогодення. Висока відповідальність за кінцевий результат прийнятого рішення змушує нас менше покладатися тільки на інтуїтивний підхід, а в більшій мірі вміло відбирати потрібну, соціально-значущу, корисну інформацію, використовувати різні джерела та канали доведення її до суспільної в цілому та індивідуальної свідомості, зокрема.

Для українського суспільства в сучасних реаліях особливої актуальності набуває розвиток соціальних інформаційних технологій, які б було доцільно ефективно використовувати для досягнення політичної, економічної, духовної та навіть військової переваг. Також слід враховувати той факт, що в останньому випадку вплив інформації може бути конфліктогенним та руйнівним, здатним привести до самих серйозних деформацій індивідуальної свідомості, аж до зміни психіки, доведення її до хворобливого стану. Більш

того, інформація негативного плану може стати спонукальним мотивом до девіантної, антисоціальної поведінки, підбурювати до порушення громадського спокою та екстремістських виступів. Сьогодні вчені вже з впевненістю говорять про інформаційні війни які розгортаються на теренах багаточисельних соціальних мереж та в Інтернет просторі. Пересічні громадяни усе частіше стикаються з інформаційною агресією, маніпуляцією та пропагандою. Усе вище сказане є вагомим аргументом, який обумовлює нагальну потребу в глибокому науковому аналізі проблем інформаційної безпеки, особливо коли це стосується особистості, бо вона завжди виступала головним рушієм суспільного прогресу. Розгляд проблеми з соціологічної точки зору сьогодні є особливо важливим, тому що в основі більшості сучасних інформаційних технологій, систем і суперсистем лежать включені соціальні процеси, бо завжди об'єктом їх впливу виступає конкретна особистість, яка живе в реальних історичних умовах.

Таким чином, можна відзначити, що актуальність проблеми інформаційних впливів на життя пересічних громадян у XXI столітті є прогресуючою тенденцією розвитку інформаційного суспільства, яка супроводжується реально існуючими загрозами інформаційній безпеці особистості, особливо в нинішніх умовах системної кризи, що охопила всі сторони життя українського суспільства. Отже, з впевненістю можна сказати про існування суспільної потреби у створенні основ системи протидії та локалізації інформаційних загроз, суспільних механізмів профілактики негативного впливу інформації на життя людини, що потребує необхідність системного наукового аналізу вищезгаданих питань.

Найбільш важливою проблемою, яку першочергово необхідно вирішувати вченим, на наш погляд, є положення і висновки про інформаційне суспільство як прояв глобальної закономірності; виявлення її характерних рис і характеристик. Однак, віртуальна реальність залишається віртуальною, а от же жодні соціальні акції по аналогії з реальним життям не здатні прищепити навички реального спілкування, в результаті чого формуються комунікативні здібності віртуальної взаємодії на шкоду реальним стосункам.

Активне втручання в соціальне життя інформаційного простору та збільшення його цінностей і норм ускладнює безпосереднє міжособистісне спілкування, яке так необхідно людині для культивування соціальності, проходження усіх етапів соціалізації, що не здатні компенсувати жодні технічні та інформаційні засоби і носії. В результаті цього суспільство позбавляється справжньої соціальності, заснованої на єдності та дії людських цінностей, спрямованих на створення соціально здорового середовища, основою якого є взаєморозуміння, взаємоприйняття, співпраця і та соціальне буття як таке.

СОЦІАЛЬНІ РИЗИКИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ: БЕЗПЕКА, ЧИ НЕБЕЗПЕКА

Маргулов А.Х., д.і.н., проф.
Дніпропетровський державний університет внутрішніх справ
м. Дніпро, Україна

У сучасному світі інформація стала грати принципово іншу роль: вона перетворилася в ідола сучасного людства, за допомогою якого відбувається виправдання його дій і вчинків. Більш того, інформаційні ресурси почали активно використовуватись для здійснення маніпулятивних впливів на людину в різних сферах життя суспільства, формувати певну громадську думку шляхом нав'язування «порядку денного» та інтерпретації подій в заданому напрямку, що подаються в «потрібному» світлі. В зазначеному контексті інформаційний простір виступає як сфера виробництва і відтворення інформаційних ризиків.

Отже, сучасне українське суспільство розвивається в рамках світового технологічного та інформаційного процесів і за масштабом використання інформаційно-комп'ютерних технологій та розвитку ринку телекомунікацій, впевнено рухається в напрямку формування суспільства інформаційного типу. Паралельно з цим процесом виникають загрози для безпеки суспільства з боку мас-медіа, які починають активно застосовувати технології маніпулятивних впливів на суспільну свідомість у вигляді масовості культури, проникнення в неї елементів агресії, жорсткості та насилля, що сприяє поглибленню духовної кризи сучасного соціуму.

Адекватне використання можливостей інформаційного простору та інформаційних технологій може стати запорукою успішної і безпечної діяльності індивіда, соціальної групи, суспільства. В іншому випадку очевидні блага інформаційної революції та інформаційного суспільства можуть обернутися негативними явищами, які пов'язані з парадоксами інформаційного суспільства. Ці парадокси були зібрані та детально проаналізовані в роботі І. А. Мальковской [1, с. 39].

В свою чергу хотілося б зупинити увагу на певних ризиках для соціуму, які створюють новітні інформаційні технології.

Перший ризик полягає в тому, що «суспільство знання» стрімко перетворюється на «суспільство незнання» і через 40-50 років світову-систему чекають моральна та інституційна кризи, оскільки відбудеться заміна «високої» культури на «низьку». Передумовою для цього стане активна передача та продаж низької якості знань за умов надмірного надлишку соціальної інформації «реципієнтам», «цільовим групам», «аудиторіям».

Вже сьогодні можемо фіксувати зростання розриву між науковою і масовою інформацією, призначеною для різних соціальних груп, причому перша поступово зникає, поки друга «масово поширюється. В інформаційному просторі спотворюється сам факт знання, перекроюються на потрібний лад події, реальні факти підміняються вигаданими, а от же абсолютно нівелюються інтереси особистості, тож сучасний інформаційно-комунікативний світ перетворюється в світ буденного і банального піару.

Другий ризик інформаційного суспільства пов'язаний з можливістю втрати сучасним соціумом лідируючої ролі в інформаційному просторі, що пов'язано з активізацією маніпулятивної діяльності ЗМІ, які використовують потужні технології впливу на свідомість широких мас. Ідентичність молодих людей набуває мережевого характеру, який сприяє втраті соціальних орієнтирів, а от же провокує неможливість фільтрувати інформацію, аналізуючи її зміст.

Третій ризик інформаційного суспільства полягає в тому, що існує вертикальна модель управління соціальною системою, активованою «на горі» і позбавленою сигналів знизу, в той час як глобальне управління потребує корекції знизу й участі громадян в управлінському процесі. Вертикальна модель управління та ігнорування більшої частини

суспільства спровокують виникнення інституційних диспропорцій, культурних трансформацій і конфліктів. З урахуванням зростання націоналізму, тероризму, ксенофобії та расизму в сучасному світі проблема управління та «соціального порядку» в умовах інформаційному суспільстві стане життєво важливою.

Четвертий ризик полягає в тому, що інформаційне суспільство пережило два різнопланових і різноспрямованих стрибка: до інтеграції людства як соціальної спільноти, пов'язаної Всесвітньою павутиною, і до дезінтеграції соціуму, в якому окремий індивід почав вважати, що зможе вижити самостійно, дистанціювавшись від громади.

П'ятий ризик інформаційного суспільства полягає в проблемі створення простору, який існує поза фізичним часом, що відбувається за допомогою пропаганди способу життя і думки на кшталт «тут і зараз», але при цьому змінюється й розуміння соціального часу, втрачається його значущість. Йдеться про те, що індивід - споживач медіа ніби постійно перебуває поза історією, поза її подіями, котрі відбуваються в даний момент, занурюючись в простір, яки актуалізує тільки даний момент часу та формує поза-історичну свідомість індивіда й аудиторії в цілому. Проблема полягає в тому, що, втрачаючи «соціальне», людина не знаходить і справжнє «індивідуальне», розчиняючись в масі, визначеній загальною назвою «споживачі», або «користувачі», які не мають ні вікової, ні гендерної приналежності, локальної (територіальної, етнічної, національної) характеристик. В результаті Інтернет-спілкування створює особливий тип особистості «техно-людину», що втратила почуття соціальної причетності та соціального простору і часу [2].

Шостий ризик інформаційного суспільства актуалізує проблему протистояння двох понять – «діяльності» і «діяння». Справа в тому, що з розвитком інформаційних технологій втрачається справжнє уявлення про те, що таке діяльність, і формується уявлення про те, що все навколо «робиться» – кимось іншим, а не конкретною людиною. При цьому створення певного іміджу людини, організації і т.д. рідко відповідає реальному образу, оскільки їх автори відірвані від соціальної реальності бо живуть у власному світі створеному інформаційними технологіями. Таким чином, реальна суб'єктність замінюється віртуальною, а справжність підміняють різного виду комунікації, які перетворюють життя на низку соціальних спекуляцій.

Нарешті сьомий ризик інформаційного суспільства зводиться до співвідношення категорій «бути» і «мати». Людина під впливом інформаційно-комунікативних технологій починає «фрагментувати» життя і втрачає свою особистісну цілісність. Питання про формування та набуття себе, а також прояві мотивів і сенсу життя під час самовизначення набуває принципового значення в суспільстві інформаційного типу, бо залежність від інформації «вбиває» залежність від комунікації в формі теперішнього особистісного спілкування.

Таким чином, сучасний соціум знаходиться в стані боротьби між двома тенденціями – переходу до «інформаційного» суспільства чи вибір традиційного із збереженням класичних «комунікативних» практик. У міру зростання кількості споживачів масової інформації розрив між двома зазначеними напрямками буде збільшуватись, а отже простір інформаційного суспільства буде розширюватись за рахунок зменшення прихильників комунікативного. Більш того, буде скорочуватися простір справжньої комунікації за рахунок збільшення інформаційної, розрахованої на масового користувача. Тож ми стоїмо на порозі виникнення принципового нового типу суспільства.

Література

1. Мальковская И. А. Социологический профиль информационно-коммуникатив-ного профиля. *Социологические исследования*. 2017. № 2. С. 38-45.
2. Information Society: Challenges for Politics, Economy and Society. URL: http:// www.bmwi-info2000.de/gip/ fakten/zvei_e/index.html

БЕЗПІЛОТНИЙ АВТОМОБІЛЬ. ЙОГО СИСТЕМА ЗАХИСТУ

Лук'яненко Т.Ю.
Державний університет телекомунікацій
м. Київ, Україна

Сучасний автомобіль вже може називатися розумним. Активний круїз-контроль, стеження за дорожніми знаками і розміткою - технології, що застосовуються автовиробниками все більш масово. Навіть на відносно бюджетному авто сьогодні можна зустріти функції інтелектуальної парковки. Всі ці функції стали тому, що більшість автомобілів вже не має фізичного зв'язку між органами управління і, умовно, колесами (а також коробкою, гальмівною системою та ін.). Тепер кермо і педалі - це інтерфейс бортового комп'ютера, який безпосередньо і управляє автомобілем. Результат - гігабайти коду, що відповідає за логіку управління та аналіз телеметрії від різних датчиків.

До недавнього часу потенційні ризики проникнення в бортове обладнання не дуже турбували автовиробників і громадськість, так як не до всіх систем можна було підключитися віддалено.

Однак ситуація змінюється. Зараз існує безліч протиугінних комплексів і систем комфортного користування, що надають віддалений доступ до важливих функцій автомобіля. Відомі випадки компрометації подібних систем, що завдали серйозних матеріальних втрат. Рік тому в системі безключового доступу і запуску Land Rover була виявлена вразливість, яка приводила до мимовільного відмикання дверей. І це тільки верхівка айсберга.

Основна і найсерйозніша, якщо буде здійснена кібератака, - загроза життю водія. У 2015 році Chrysler відкликав 1,4 мільйона автомобілів після того, як пара хакерів продемонструвала виданню WIRED, що вони можуть віддалено контролювати систему Jeep через Інтернет.

Типовий легковий автомобіль останнього покоління містить під капотом не лише двигун, а й більш 100 млн рядків коду. Навіть відносно прості моделі мають близько 30 електронних блоків управління (ЕБУ), оснащених власними процесорами і прошивкою. В люксових авто таких блоків може бути більше ста. Щоб взаємодіяти між собою, ці ЕБУ підключаються через лабіринт цифрових шин. Тут і CAN (Control Area Network), і Ethernet, і FlexRay, LIN і MOST. Всі вони працюють з різною швидкістю, передають різні типи даних і забезпечують з'єднання між різними частинами автомобіля.

Хоч у різних виробників автомобільних мереж, кожен вендор реалізує їх по-різному, але всі архітектури мають спільні компоненти: шлюзи, ЕБУ, шини CAN, USB- і бездротові інтерфейси. При всіх відмінностях вони виконують подібні функції і взаємодіють між собою одним чином.

Підключений до інтернету автомобіль має значну кількість відкритих портів, які потенційно можуть використовувати кіберзлочинці. А враховуючи невідповідальне відношення до питань безпеки з боку розробників автомобілів, проникнення в будь-який доступний ЕБУ – відносно просте завдання. Перехопивши контроль над одним модулем, атакуючий може переміщатися від одного керуючого блоку до іншого і виробляти найрізноманітніші види атак, наприклад:

- DoS-атаки на ЕБУ рульового управління або гальмівної системи, які можуть привести до аварії зі смертельними наслідками;
- блокування інформаційно-розважальної системи або відключення запуску двигуна з вимогою викупу;
- впровадження недійсних даних в потік обміну між модулями або модифікація переданих даних з метою, наприклад, порушити режим роботи двигуна і вивести його з ладу;
- відключення ЕБУ з використанням протоколів виявлення помилок;

перехоплення керування автомобілем, в результаті якого може статися аварія, причому встановити справжнього винуватця в цьому випадку практично неможливо.

Щоб вирішити проблеми безпеки, галузева група ISO і SAE розробила звід керівних принципів забезпечення безпеки підключених автомобілів - ISO/SAE 21434.

Контрольні точки для всіх компаній, у випадку потенційних загроз:

- управління кібербезпекою повинно грунтуватися на постійному моніторингу ризиків в рамках всієї організації, включаючи виробництво і весь ланцюжок постачальників;
- для впровадження кібербезпеки організаціям знадобиться сильна культура ІБ та якісна підготовка кадрів;
- керівники всіх рівнів повинні працювати над впровадженням знань в області кібербезпеки на всіх етапах бізнесу і впроваджувати їх в своїх підрозділах; для цього можна скористатися рекомендаціями стандарту управління інформаційною безпекою ISO / IEC 27001.

Для кожної виявленої вразливості необхідно встановити, чи може вона бути використана для атаки. Всі помилки і події повинні бути проаналізовані.

Щоб не надати потенційним злочинцям можливість скористатися виявленої вразливістю, можливе застосування наступних заходів:

- тимчасове відключення некритичних компонентів;
- повідомлення користувачів про ризик;
- створення і перевірка виправлення коду командою розробників;
- створення і розгортання виправлень безпеки.

Підключення автомобілі – один з компонентів складної екосистеми, яка містить мільйони взаємозв'язків, кінцевих точок і користувачів. Складність розумної транспортної системи досягла такого рівня, що вкрай складно прогнозувати, в яку частину буде направлена чергова атака. У зв'язку з цим, захист підключених автомобілів не обмежується софтом і електронікою транспортного засобу. Необхідно також забезпечити захист бекенда і мережі передачі даних.

Література

1. Взлом автомобілів стає все більш небезпечним. URL: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
2. Збитки компанії Chrysler URL:https://www.theverge.com/2015/7/24/9032179/chrysler-announces-voluntary-recall-hack
3. Інженерія кібербезпеки. Електричні та електронні компоненти та загальні аспекти системи. URL:https://www.iso.org/standard/70918.html

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ІНСТИТУТ ОСВІТИ

Клименко О.Ю., д.соц.н., проф.
Державний університет телекомунікацій,
м. Київ, Україна

Кожна людина, котра живе на початку XXI століття повинна вміти орієнтуватися в цілому комплексі соціальних проблем, пов’язаних з процесами інформатизації, які не обмежуються лише освоєнням нових технологічних досягнень. Нині без перебільшення можна стверджувати, що здатність самостійно аналізувати і оцінювати можливі наслідки розвитку інформаційного суспільства для сучасного життя, включаючи зміни пов’язані з перебудовою структури зайнятості населення, розвитком ІТ-технологій, трансформацією

системи освіти, впливає на саму якість повсякденного буття окремої людини, а тому набуває беззаперечної актуальності. Висока пластичність і динамічність сучасного світу робить подібну компетентність населення однією з найважливіших умов як процвітання суспільства в цілому, так і соціальної успішності його окремих представників.

Життя в інформаційному суспільстві передбачає осмислення всебічної інформатизації, в першу чергу усвідомлення її соціальних наслідків, оскільки саме це є необхідною умовою розуміння самої природи змін, що відбуваються та здійснюють комплексний вплив на всі сфери діяльності людини. Відповідно до цього для наукового співтовариства представляється необхідним дати систематичне висвітлення процесів інформатизації як соціального явища у всьому різноманітті його зв'язків і відносин. Це передбачає аналіз відповідної «інформаційної реальності», під якою прийнято розуміти сукупність інформаційних процесів, систем і комунікацій, що мають соціальну значимість для функціонування і розвитку соціуму.

Сучасна система освіти теж охоплена процесами інформатизації. З огляду на її значимість, як одного з основних інститутів суспільства, питання інформатизаціє є актуальнім та такою, що заслуговує особливої увагу. Така ситуація пояснюється наступними чинниками.

По-перше, вітчизняна система освіти характеризується інтенсивним впровадженням сучасних інформаційних технологій, які виступають пусковим механізмом для виникнення певних трансформацій як в її організаційній структурі, так і в методах і методиках викладання у вищій школі.

По-друге, освіта покликана готувати підростаюче покоління до життя та соціально активної діяльності в межах сформованого інформаційного середовища з усіма характерними для нього особливостями, що передбачає введення деяких нових параметрів до педагогіки та виховного процесу, зокрема, особливо в контексті його соціально-виховної функції (що передбачає втручання до процесів соціалізації).

По-третє, набуття нового знання відбувається настільки швидко, що освітній процес не встигає його відтворювати, тож студенти усвідомлено отримують вже застарілу інформацію. Тому роль інституту освіти нівелюється, через ускладнення виконання ним основних функцій за умов надмірно швидкого розвитку ІТ-технологій.

По-четверте, загострюється проблема «комп'ютерної грамотності» й «інформаційної культури особистості», як особливо актуальних для сучасної вітчизняної освіти.

Враховуючи усе вище викладене, з впевненістю можна сказати про необхідність створення нової парадигми освіти, основою якої повинен стати принцип безперервності у набуті знання. Такі вимоги ставе перед людиною інформаційне суспільство, зміни технологій в якому настільки швидкі, що змушують людину знаходитись у постійному пошуку нового знання.

Модель відкритої, безперервної освіти покликана гармонізувати соціальну динаміку шляхом врахування основних потреб особистості та суспільства. Отже подальший технічний розвиток передбачає широке застосування сучасних інформаційних технологій в якості підґрунтя для навчального процесу.

Універсальність можливостей ІТ-технологій стосується без винятку усіх дисциплін які викладаються у вищій школі. З огляду на неприпустимість переходу навчання у площину виключної інформатизації освіти шляхом її технологізації, слід звернути особливу увагу на різноманітні соціально-культурні та психологічні наслідки цього процесу.

Таким чином, людині в умовах інформаційного суспільства необхідно самому обирати коло своїх інтересів і визначати рід своїх занять, самостійно формувати власне соціальне середовище через вибір оточення і визначати свою приналежність до тієї чи іншої формальної або неформальної групи, необхідно бути відкритим до прийняття нового знання, а також до переосмислення своїх ціннісних орієнтирів та моральних устоїв.

Особливо слід відзначити роль науки в інформаційному суспільстві, бо вона нерозривно пов'язана з проблемами вищої школи. У цьому сенсі можна не сумніватись щодо

посилення ролі науки в інформаційному суспільстві, яка стає основою технічного та соціального прогресу.

Розвиток ІТ-технологій надав можливість для зростання технологічної сили людини, вимагаючи від неї високого рівня соціальної відповідальності, що обумовило необхідність володіти не тільки професійними знаннями і компетентностями, але й ставити перед собою високі гуманістичні цілі, які б сприяли гармонійному розвитку сучасного суспільства паралельно з стрімким технічним прогресом. Окрім того, в складних умовах тотальної технологізації особистості ще необхідно зберегти цілісність особистості та її індивідуальність, що доволі складно через наявність певних протиріч. З одного боку – необхідність розуміти свою відповідальність в рамках певних соціальних дій, з іншого – тотальне знецінення традиційних цінностей, масовість спроб маніпулювати свідомістю на фоні існування віртуальної реальності. Таким чином, в інформаційному суспільстві в рамках існування інституту освіти процедура навчання переходе у віртуальний світи, а набуття знань перетворюється в існування у віртуальній реальності, яка для особистості стає більш важливою, ніж сама соціальна дійсність

ЦИФРОВА НЕРІВНІСТЬ ЯК ПЕРЕДУМОВА СОЦІАЛЬНОЇ СТРАТИФІКАЦІЇ

Слющинський Б.В., д.соц.н., проф.,
Маріупольський державний університет
м. Маріуполь, Україна

У соціально-економічній сфері перші ознаки серйозних змін, пов’язаних с формуванням інформаційного суспільства почали проявлятися ще на прикінці 50-х років XX ст. в самій промислово розвиненій країні світу – Сполучених Штатах Америки. Соціологи підрахували, що з загальної кількості зайнятих у сфері виробництва, число «білих комірців», які працюють з інформацією на технічних посадах клерків і менеджерів з управління вперше перевищила кількість «синіх комірців», – робітників, котрі займаються виробництвом промислових товарів. Зміни в структурі зайнятості та самого характеру праці – один з головних економічних показників глибинних соціально-економічних трансформацій в суспільстві в момент виникнення суспільства інформаційного типу. У наступні десятиліття зазначена різниця в структурі зайнятості стала стрімко зростати. Вже у 2000 р. в США понад 80 % зайнятого трудового населення мало справу з виробництвом і обробкою інформації, а фабричний пролетаріат істотно скоротився і складав не більше 12 % від працездатного населення. Статистичні дані численних досліджень показують неухильне зростання історичного процесу «розмивання» основних соціальних структур – сформованих у своїй більшості з головних виробників суспільного добробуту та об’єктів експлуатації в індустріальному суспільстві. На початку XIX століття в сільському господарстві США було зайнято майже 75 % від усієї робочої сили; за півстоліття ця частка скоротилася до 67 % відсотків, а за наступні 100 років впала вже в 3,5 рази – до 20 %. За останні 40 років частка зайнятих в аграрному секторі США зменшилася ще у вісім разів і склала сьогодні, за різними підрахунками, від 2,5 до 3 %в. В результаті, з 1994 року статистичні органи Сполучених Штатів перестали враховувати частку фермерів в складі населення через її незначності [1]. Подібні процеси розвиваються і в більшості європейських країн. Отже експерти прогнозують, що в найближчі десять років 25 з 26 створюваних робочих місць в США припадуть на сферу послуг, а загальна частка зайнятих в ній складе 86 % сукупної робочої сили. Так, ще на початку 80-х років XX століття частка працівників, безпосередньо зайнятих

в виробничих операціях, не перевищувала в США 12 %, сьогодні вона скоротилася до 10%, а в Японії подібні цифри становлять відповідно 15 % і 12 % [2].

У зв'язку з вище наведеним можна стверджувати про актуалізацію в сучасному суспільстві проблеми «цифрової нерівності», а також реального усвідомлення можливості використання нових технологій для розширення контролю держави над своїми громадянами. Під «цифровим розривом» розуміють відношення до нерівності в доступі до Інтернет, що стає додатковим джерелом соціальної нерівності з усіма наслідками.

Традиційні засоби масової інформації працюють переважно в режимі інформаційного монологу (односторонньої комунікації), за допомогою якої відповідні структури впливають на розум індивідів та підтримують контроль над більшістю членів суспільства. Комп'ютерні ж технології відкрили можливість багатосторонньої комунікації. Кожен, хто має доступ до мережі, може виступати як одержувачем, так і відправником інформації.

Для певних сфер життя суспільства, таких як політика т економіка Інтернет платформа є альтернативним механізмом для здійснення маніпуляцій. Тексти та відео в мережі можуть існувати місяцями та навіть роки, а в умовах посилення фінансового контролю за рекламою в традиційних ЗМІ, Інтернет має серйозні переваги. Глобальна Мережа дозволяє забезпечити постійний диспут до інформації з можливістю зворотного зв'язку в реальному часі.

Застосування ІТ-технологій може сприяти зміцненню репресивних функцій держави, обмеження політичної свободи громадян і, врешті-решт, встановлення системи «комп'ютерного тероризму». Загроза політичного та поліцейського спостереження над людьми за допомогою сучасної інформаційної техніки вже є реальною.

Революційні процеси в області інформаційних і телекомунікаційних технологій очевидні та неминучі. Однак, вплив цих процесів як на суспільство, так і на окремих його членів суттєво відрізняється. В умовах інформаційної глобалізації ні одна країна вже не в змозі ізолювати своє населення від впливу колосальних потоків найрізноманітнішої інформації. Тому свідомість людей в XXI ст. формується не тільки під впливом ситуації в рамках свого соціокультурного простору, але також і під впливом інформації з зовнішнього світу. Таким чином ІТ-технології можуть впливати на формування в суспільстві вже принципово нової соціально-політичної ситуації, зразків якої в історії людства ніколи раніше не було. У зв'язку з цим, як ніколи раніше, загострюється проблема інформаційної та соціальної безпеки, що стосується як окремих людей, так і суспільства в цілому. Звідси набувають життєво важливого значення міждисциплінарні і, в першу чергу, соціально-політичні дослідження проблем інформаційної безпеки, кіберзлочинів, інформаційного протиборства та інформаційних воєн.

Література

1. Силичев Д.А. Социальные последствия перехода от индустриализма и модерна к постиндустриализму и постмодерну. Вопросы философии. 2005. № 7. С. 3-20.
2. Luttenberg J. Educational reform as dynamic system of problems: Towards an analytic instruments. *Journal of Educational Change*. 2013. Vol. 14. No. 3. P. 335-352.

ВИКЛИКИ ТА РИЗИКИ ПРОФЕСІЙНО-ТЕХНІЧНОЇ ОСВІТИ В УКРАЇНІ

Москаленко Л.М., к. філос. н.
Державний університет телекомунікацій,
м. Київ, Україна

Останні декілька років на українському ринку праці зберігається тенденція до збільшення числа вакансій серед кваліфікованих робітничих професій. Так, аналіз відкритих даних державної служби зайнятості в контексті структури ринку вакансій за кодом професії, фіксує, що найвища кількість дефіциту вакансій доводиться на робочі професії з кодом 7 і 8 - це кваліфікаційні працівники з інструментом і робітники по обслуговуванню і експлуатації машин. Позитивна динаміка в цих групах зберігається останні декілька років і сумарно складає майже половину незакритих вакансій ринку зайнятості в Україні. В 2017 році дефіцит вакансій з робочих професій складає 56%, в 2018 році - 52,1%, в 2019 році - 46,5% [2].

Існує комплекс причин, які сприяють формуванню дефіциту в робочих професіях. Це і скорочення кількості випускників шкіл, і старіння населення, і, відповідно, скорочення кількості кваліфікованих робітників по причині їх виходу на пенсію, і відтік фахівців, які фінансово мотивовані заробітками за кордоном, і неспроможність нинішньої системи професійної освіти заповнити вакуум потреб в кваліфікованих працівниках.

Основний сектор освітнього ринку в професійній підготовці з робочих професій належить професійно-технічним освітнім установам формального типу.

Останнє десятиліття в Україні спостерігається різке скорочення професійно-технічних освітніх установ. За даними державної служби статистики в Україні на 26% зменшилася кількість освітніх установ цього типу. А студентів - майже в двічі. Так, в 2008-2009 н.р. у професійно-технічних освітніх установах навчалося 288,1 тис. студентів, а в 2019 н.р. їх чисельність скоротилася до 131 тис. студентів [3].

З 2015 року спостерігається спроба реорганізувати професійно-технічну освіту, у тому числі реформувати її систему фінансування. Законами України "Про Державний бюджет України на 2016 рік" [5] і "Про внесення змін до Бюджетного кодексу України" [4] фінансування установ професійно-технічної освіти було перекладено з державного бюджету на відповідні місцеві бюджети. Основною метою введених змін було досягнення децентралізації професійно-технічної освіти, що, повинно було сприяти оптимізації витрат на освіту із-за переорієнтації на потреби регіональної промисловості.

За даними МОН, можливості місцевого бюджету покривають лише трохи більше 60% фінансових потреб учбових закладів в регіонах. ПТУ, розташовані за межами міст обласного значення, знаходяться в катастрофічному фінансовому стані, оскільки нинішні фінансові механізми покривають їх потреби тільки на 45% [8]. Доля витрат на систему професійно-технічної освіта в консолідованому бюджеті на освіту в 2020 році складає 4,55% (у 2016 році - 4,78%) [7, С.163]. Це у черговий раз підтверджує той факт, що фінансування здійснюється на низькому рівні, покриває тільки витрати споживання і майже не передбачає витрат на модернізацію та розвиток.

Більшість із вже розроблених і затверджених Міністерством освіті і науки України стандартів професійної освіти готувалися по застарілих методиках і без участі працедавців, тому вони не відповідають сучасним ринковим вимогам і не можуть використовуватися для якісної підготовки кваліфікованих робітників [6].

Також актуальнім залишається питання педагогічних кадрів. Зокрема, дефіцит майстрів виробничого навчання, породжений відтоком висококваліфікованих кадрів у виробництво із-за значно більшого розміру оплати праці. Так, за даними державної служби зайнятості в 2018 році було зафіксовано 138 незакритих вакансій на посаду викладача професійно-технічної установи, в 2019 році - 161 вакансія, а в 2020 році за період січень-листопад - 110 вакансій [2].

Одним з важливих чинників, який сприяє дефіциту робочих професій являється їх непрестижність серед молодих людей. Українська молодь у більшій своїй частині орієнтована на здобуття вищої освіти. За останні 30 років випуск кваліфікованих робітників в Україні скоротився більш ніж на 35%. Одночасно випуск фахівців з вищою освітою виріс в 1,4 разу.

Можливо, однією з основних причин непопулярності професійно-технічної освіти як серед молоді, так і в українському суспільстві в цілому, є сформований стереотип ПТУ як своєрідної панацеї для соціальної інклюзії та інтеграції уразливих категорій населення. Зокрема, в 2019 році серед загального контингенту учнів було 4,17% дітей-сиріт та тих, які залишилися без піклування батьків, 10,3% дітей з неповних сімей, 8% дітей, - з неблагополучних і малозабезпечених сімей і 2% дітей - з особливими освітніми потребами [3].

Відсутність збалансованості ринку освітніх послуг і потреб регіонального ринку праці. В результаті соціологічного моніторингу професій в категоріях робітників з інструментом і робітників з обслуговування та експлуатації машин було зафіксовано, що впродовж останніх декілька років в Україні в цій категорії сформувався список найбільш затребуваних професій, які вже декілька років потрапляють в ТОП списку дефіцитних вакансій.

Порівняльний аналіз кількості випускників профтехучилища за 2019 рік і дефіцит найбільш затребуваних робочих професій (топ 10 найбільш популярних дефіцитних вакансій в 2019 році) зафіксував, що в різних регіонах показник затребуваних професій, по яких відсутня підготовка фахівців коливається від 30% до 70%.Також по деяким професіям існує негативний дисбаланс, коли підготовка фахівців значною мірою перевищує потребу регіонального ринку в цих робочих професіях. Наприклад, в Хмельницькій області кількість випускників за фахом "Електромонтер по ремонту і обслуговуванню електроустаткування" в 2,4 разу перевищує потребу регіонального ринку, а "Електрогазозварник" - в 8 разів [10]. Формат статті не дозволяє надати усі результати (по усіх регіонах України), тому тут сформовані головні висновки дослідження.

5. Висновки. Вочевидь, що нинішня система професійної освіти вимагає трансформації і модернізації, а також адаптації відповідно до регіональних потреб ринку праці. Рішення проблем, що склалися в системі професійної освіти в Україні, вимагає впровадження і реалізації низки заходів. Виходячи їх вищевикладеного матеріалу і результатів дослідження потреб регіонального ринку праці у фахівцях з робочих професій, рекомендуємо:

- **Впровадження збалансованої регіональної стратегії**. Розробити стратегію економічного розвитку регіону, в якій професійно-технічні заклади є суб'єктами системи освіти, що реалізують регіональне замовлення на підготовку робочих кадрів для пріоритетних напрямів регіонального ринку праці.

- **Неформальна освіта.** Розглядати професійну підготовку як частину освіти дорослих, яка передбачає розвиток професійних компетенцій шляхом залученості до неформальну освіту як більш гнучкої та адаптивної системі у навчанні робітничим професіям;

Компетентнісний підхід. Пріоритетним розглядати і реалізовувати компетентнісний підхід в професійно-технічній освіті, який забезпечує формування нових і поглиблених професійних компетенцій, які відповідають сучасним і перспективним потребам ринку праці.

- **Розширення цільової аудиторії**. Адаптувати учбові програми під концепцію освіти впродовж життя та пропонувати навчальні курси для дорослого населення з підготовки на дефіцитні робочі професії.

- **Моніторинг регіонального ринку праці**. Розробити постійно діючий механізм моніторингу регіонального ринку праці, оновлюючи списки актуальних робочих професій/ затребуваних професійних компетенцій.

Література
1. Новиков В., Черниченко В. Актуальные проблемы развития дуального образования в Украине. Экономико-правовое и демографическое исследование. Lap Lambert Fcademic Publishing, 2020. 82 с.
2. Державна служба зайнятості України Офіційний сайт державної служби зайнятості України URL: https://www.dcz.gov.ua
3. Державна служба статистики України Офіційний сайт Державної служби статистики України. URL: http://www.ukrstat.gov.ua/
4. Закон України "Про внесення змін до Бюджетного кодексу України" від 24.12.2015 року №911 (Відомості Верховної Ради (ВВР) Сайт: Законодавство України. URL: http://zakon.rada.gov.ua/laws/show/914-19/sp:max25
5. Закон України "Про Державний бюджет України на 2016 рік" від 25.12.2015 року №928-VIII (Відомості Верховної Ради (ВВР) Сайт: Законодавство України. URL: http://zakon.rada.gov.ua/laws/show/928-19
6. Освітня реформа: результати та перспективи/ Інформаційно-аналітичний збірник К.: 2019. 227 с.
7. Стратегія розвитку професійної (професійно-технічної) освіти на період до 2023 року (проєкт) Офіційний сайт Міністерства освіти та науки України. URL:https://mon.gov.ua
8. Сучасний стан фінансування професійно-технічної освіти в Україні URL: https://feao.org.ua
9. Щорічна доповідь Президентові України, Верховній Раді України, Кабінету Міністрів України про становище молоді в Україні Молодь на ринку праці: навички XXI століття та побудова кар'єри. Офіційний сайт Міністерства молоді та спорту України URL:http://dsmsu.gov.ua/index/ua/material/49156
10. Офіційний реєстр суб'єктів освітньої діяльності URL: https://info.edbo.gov.ua/

ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ

Сокуренко Д.О.
Державний університет телекомунікацій
м. Київ, Україна

«Кібербезпека» — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».

Виклад основного матеріалу. Нові виклики часу та нові напрями розвитку суспільства проникнення найновіших технологій в усі сфери життя вимагають зрозуміти ключові проблеми та питання безпеки освітнього процесу в цифровому просторі, зокрема безпеку усіх безпосередніх учасників, організаторів освіти, держави, а також безпеку змісту навчання. Відповідно, значення кібербезпеки вийшло на рівень компетентності з питань безпеки життєдіяльності людини, стало невід'ємною частиною цифрової компетентності, насамперед, усіх учасників навчального процесу. Ці тенденції зміни парадигми навчання пред'являють додаткові вимоги як до суб'єктів навчання (як вчителів, так і учнів), так і до засобів навчання, особливо в синтетичному навчальному середовищі. Навчання із застосуванням технічних засобів, насамперед електронних, набуває все більше характеру операторської праці, під час якої зовнішні та внутрішні фактори, що діють на людину, впливають на когнітивні можливості останньої. До того ж вихід проблем кібербезпеки на

рівень одного з найбільш актуальних питань людства в цілому, як це було зазначено, зокрема, під час обговорень на міжнародному Форумі в Давосі в січні 2019 р., ставить питання ефективності, безпечності та "людиноцентричного" характеру електронних засобів навчання.

Глобальна культура кібербезпеки – це шлях вирішення проблеми підвищення рівня кіберзахисту особи і суспільства з використанням соціальних заходів на міжнародному і національному рівнях. Актуальність цієї проблеми обумовлена наявними і прогнозованими тенденціями збільшення кількості кримінальних правопорушень у кіберпросторі у зв'язку зі значним поширенням технологій електронної економіки та урядування, безпрецедентними масштабами комунікації у кіберпросторі спільнот національного і міжнародного виміру. Основною метою формування глобальної культури кібербезпеки є досягнення такого стану соціальної взаємодії між суб'єктами інформаційної діяльності, коли заходи із забезпечення кібербезпеки стають повсякденною звичкою кожного користувача сервісів кіберпростору.

Світова практика. Формування глобальної культури кібербезпеки та реалізації зазначених принципів базується на рекомендаціях міжнародних організацій та національних ініціативах, насамперед, шляхом: інформування (формуванням обізнаності) широких верств населення, фахівців державних і приватних установ відносно існуючих загроз, заходів попередження їх реалізації, виявлення та реагування; формування та підтримки ринку засобів та послуг кіберзахисту, проведення відповідного навчання. Національні стратегії кібербезпеки передбачають механізми взаємодії та відповідальності в рамках приватно-державного партнерства при реалізації заходів формування глобальної культури кібербезпеки. Заходи формування обізнаності громадян з питань забезпечення кібербезпеки відбуваються шляхом інформування співробітників організацій та установ різних форм власності: в засобах масової інформації; на веб-ресурсах державних і приватних структур; на конференціях, семінарах та тренінгах; при реалізації освітніх програм в середніх і вищих навчальних закладах. Формування та підтримка ринку засобів і послуг із забезпечення кібербезпеки передбачає: заходи нормативно-правового регулювання сфери технічного і криптографічного захисту інформації; створення громадських організацій для надання правової і технічної допомоги громадянам для забезпечення їх кібербезпеки; розбудову національної системи оповіщення про кібератаки та кіберінциденти; започаткування механізмів страхування ризиків та інших інструментів управління кібербезпекою.

Висновки. Проблеми кібербезпеки не зводяться лише до технічних аспектів захисту інформаційних ресурсів, у повному обсязі вони мають включати такі види захисту: правові, технічні, інформаційні, організаційні та психологічні. Важливим аспектом формування компетентності людини в цифровому просторі має бути культура кібербезпеки, яка є складником цифрової компетентності.

Література

1. Биков В.Ю., Спірін О.М., Пінчук О.П. Проблеми та завдання сучасного етапу інформатизації освіти: Інститут інформаційних технологій і засобів навчання НАПН України. 2017

2. Довгань О.Д. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія / О.Д. Довгань, І.М. Доронін. (НДІ інформатики і права НАПрН України К.: Видавничий дім "АртЕк"

МІЖГАЛУЗЕВА СУТНІСТЬ ТЕОРІЇ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Горпинич О.В. к.філос.н., доц.
Державний університет телекомунікацій
м. Київ, Україна

Становлення інформаційного суспільства має як безсумнівні позитивні, так і певні негативні наслідки. З одного боку, пришвидшилася передача інформації значного обсягу, прискорилась її обробка та впровадження. З іншого – серйозне занепокоєння викликає поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблематики, свідчить, що дуже часто інформаційна безпека підприємництва зводиться тільки до інвестицій у технічні засоби захисту інформації, нерідко без будь-яких виправдань та обмежень, без чіткого усвідомлення її сутності та змісту як соціального явища.

Інформаційна безпека - це комплекс нормативних документів з усіх аспектів використання засобів обчислювальної техніки для обробки та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації та профілактики комп'ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо [1].

З точки зору когнітивного підходу, різні автори, переважно на основі базового освітнього світогляду, по-різному подають визначення інформаційної безпеки, спираючись на ті чи інші критерії (умови, чинники). В умовах формування інформаційного суспільства специфічним предметом правовідносин є інформація у формі даних, сигналів в автоматизованих (комп'ютерних) системах, електронних телекомунікаціях, в Інтернеті тощо [2].

З точки зору теорії гіперсистем права, провідна системна проблема інформаційної безпеки як процесу інформаційної діяльності — це підтримка (збереження, охорона і захист) суспільних інформаційних відносин від негативних впливів (загроз інтересам суб'єктів суспільних відносин): соціальних (соціогенних, антропогенних, у їх складі криміногенних), техногенних та природних (стихійних). Зазначені чинники логічно зумовлюють необхідність визначення інформаційної безпеки як міжгалузевого комплексного наукового інституту [2].

Однак багатоаспектність та багатофункціональність категорії «інформаційна безпека» дає можливість проводити дослідження в різних наукових напрямах гуманітарного (у тому числі правового, соціологічного) та технічного спрямування.

Визначним у проблематиці теорії організації інформаційної безпеки як соціо-технічного явища є з'ясування її напрямів на засадах комплексного підходу. Умовно можна визначити такі аспекти: правові, управлінські, інженерно-технологічні. У складі останніх, наприклад, щодо комп'ютерних систем як автономні визначаються програмно-математичні (комп'ютерні програмні) засоби безпеки.

Щодо інформаційної безпеки як наукового напряму існує необхідність виділення двох частин її теорії: загальної частини (фундаментальних, загальних положень) та особливої частини (відносин щодо окремих напрямів, функцій на основі загальних положень). Можливе виділення спеціальної частини, наприклад, інформаційної безпеки підприємництва тощо.

На загальнотеоретичному рівні можна визначитися у наступних ключових для потреб практики, особливих проблемах інформаційної безпеки:

1) щодо організаційного аспекту підтримки функціонування інформаційних систем (їх збереження, охорони та захисту);

2) як міжгалузевого комплексного інституту, що формується на межі соціальної кібернетики (теорії автоматизації управління соціальними системами), інформаційного права та правової інформатики.

До першої групи можна віднести такі проблеми:

• забезпечення доступу до даних (відомостей, повідомлень, сигналів);

• забезпечення цілісності даних щодо загроз, які можуть спричинити порушення життєдіяльності суб'єкта інформаційних правовідносин;

• організації комплексного контролю за потоками сигналів у відповідному середовищі їх функціонування (циркуляції інформаційних ресурсів), відповідно до матеріальних носіїв, а саме: людських (соціальних, антропологічних), людино-машинних (людино-технічних, соціо-технічних) та технологічних;

• організації сумісності систем підтримки (збереження, охорони та захисту) даних, у тому числі в автоматизованих (комп'ютеризованих) системах з іншими системами забезпечення відповідної організаційної структури;

• виявлення можливих каналів несанкціонованого витоку інформації (фізичних, соціо-технічних, соціальних);

• блокування (протидії) несанкціонованого витоку інформації;

•організації виявлення, кваліфікації, документування порушень інформаційної безпеки (як фактів щодо визначеного стану: у визначеному просторі, часі і колі осіб), а також правове формулювання відповідальності, санкцій та організація притягнення винних до відповідальності (дисциплінарної, цивільної, адміністративної, кримінальної) за порушення інформаційної безпеки.

Ураховуючи міжгалузеву сутність теорії організації інформаційної безпеки в умовах формування глобальної кіберцивілізації, в ній поєднуються методи пізнання традиційних фундаментальних наук: соціології та фізики, які концентруються у такій науці, як кібернетика. Це зумовлено безпосередньо предметом теорії: людино-машинними (соціо-технічними) системами, провідними яких є комп'ютеризовані інформаційні системи, в тому числі телекомунікаційні, та необхідність керування їх діяльності.

Через наявність людського фактору як провідного теорія організації інформаційної безпеки як система знань має предметний гіперзв'язок з такими фундаментальними гуманітарними науками, як соціологія, соціальна психологія, правознавство тощо.

У даному аспекті визначається також напрям теорії щодо оцінки, характеристики зловмисників, які посягають на безпеку інформаційної системи. У цьому аспекті теорія безпеки має зв'язок з кримінологією, в тому числі її складовими вченнями: віктимологією, теорією формування соціально-психологічного портрету зловмисника тощо.

Література

1. Золотар О. Інформаційна безпека людини: теорія і практика. URL: http://ippi.org.ua/sites/default/files/informaciyna_bezpeka_lyudini_print.pdf

2. Медвідь Ф. Інформаційна безпека України: виклики і загрози. URL: https://nato.pu.if.ua/old/journal/2009-2/2009-2-28.pdf

СЕКЦІЯ 8. ЗАКОНОДАВЧА Й НОРМАТИВНА ОСНОВА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

КОНЦЕПТУАЛЬНІ ПОГЛЯДИ НА ЗМІСТ НОРМАТИВНИХ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

Дзюба Т.М.
Державний університет телекомунікацій,
м. Київ, Україна

Відповідно до Стратегії національної безпеки України [1], формування стійкості, як здатності суспільства та держави швидко адаптуватися до змін безпекового середовища й підтримувати стале функціонування, зокрема шляхом мінімізації зовнішніх і внутрішніх уразливостей, є однією з основних засад забезпечення національної безпеки.

Очевидно, що кіберстійкість має відображати сутність стійкості, як однієї з засад національної безпеки, в сфері кібербезбеки, тим більше, що кібербезпека є невід'ємною складовою національної безпеки України, а Стратегія кібербезпеки відповідно до Закону України «Про національну безпеку України» має деталізувати положення Стратегії національної безпеки України у сфері використання кіберпростору [2].

Однак, в основних нормативно-правових актах національного законодавства, які визначають сферу кібербезпеки: Законі України «Про основні засади забезпечення кібербезпеки України» [3] та Стратегії кібербезпеки України [4], категорія кіберстійкості відсутня взагалі, лише визначені деякі шляхи і пріоритети забезпечення кібербезпеки, які можна віднести до формування кіберстійкості:

підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

проведення навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;

розвиток мережі команд реагування на комп'ютерні надзвичайні події;

створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій тощо.

Термін «кіберстійкість» в системі нормативно-правових актів України визначений тільки в банківській сфері і стосується використання платіжних систем: «Кіберстійкість платіжної системи – це спроможність платіжної організації, учасників платіжної системи, операторів послуг платіжної інфраструктури та розрахункового(их) банку(ів) цієї платіжної системи запобігати, протистояти, стримувати та оперативно відновлюватися після кіберінцидентів та кібератак на неї» (Постанова Національного банку України від 28.11.2014 № 755 «Про затвердження Положення про нагляд (оверсайт) платіжних систем та систем розрахунків в Україні»).

Очевидним є висновок щодо необхідності вдосконалення чинного законодавства, яке визначає та регулює сферу кібербезпеки, шляхом виокремлення кіберстійкості, як окремого напряму забезпечення кібербезпеки, і деталізації відповідних правових механізмів. Однак, всіх можливих проблем це не вирішить.

На мій погляд, сьогодні можна визначити три основні проблеми розвитку системи кібербезпеки України, зокрема формування кіберстійкості:

1. Штучне відокремлення сфери інформаційної безпеки (в якій загрози визначаються за змістом інформації, що розповсюджується) від сфери кібербезпеки (в якій загрози визначаються за формами та способами використання інформації, інформаційних систем та технологій без урахування змісту самої інформації). Як наслідок, маємо дві різні сфери національної безпеки, які, обидві, стосуються використання інформаційного простору

(сьогодні різниця між поняттями «інформаційний простір» та «кіберпростір» вже фактично відсутня).

2. Неврахування системо утворюючої ролі інформаційної сфери, яка полягає в тому, що інформаційні процеси та відносини відбуваються в усіх, без виключення, сферах життєдіяльності держави та суспільства, і, відповідно, стосуються усіх сфер національної безпеки України. Як наслідок, не враховуються особливості реалізації кіберзагроз в сферах зовнішньо і внутрішньополітичної безпеки, енергетичної, економічної, соціальної, воєнної безпеки тощо.

3. Реактивний (часто навіть пасивний) підхід до забезпечення кібербезпеки, тобто реагування та дії передбачаються тільки за наявності видимої загрози. Це обумовлює недостатнє використання можливостей для збільшення власного впливу на процеси, які відбуваються в інформаційному просторі і, як наслідок, формування стійкого базису для забезпечення власної кібербезпеки.

Слід зазначити, що перша Доктрина інформаційної безпеки [5], прийнята в 2009 році враховувала комплексний характер загроз інформаційній безпеці і специфічність прояву цих загроз в різних сферах життєдіяльності держави та суспільства. Так, в ній окремо розглядались загрози і відповідні напрями державної політики у зовнішньополітичній сфері, сфері державної безпеки, воєнній, внутрішньополітичній, економічній, соціальній і гуманітарній, науково-технологічній і екологічній сферах. Однак, розроблення комплексної державної політики, яка б враховувала всі особливості кожної зі сфер і передбачала активний вплив на світовий інформаційний простір, в цьому документі теж не було визначено.

З огляду на зазначене, сьогодні, при розробленні концептуальних та доктринальних документів у сфері інформаційної безпеки та кібербезпеки доцільно:

1. Дослідити можливості вироблення єдиних поглядів на забезпечення національної безпеки України в інформаційному просторі без штучного розділення сфер інформаційної безпеки та кібербезпеки;

2. При формуванні системи нормативно-правових актів, які регулюють сфери інформаційної та кібербезпеки, зокрема визначають механізми формування кіберстійкості, обов’язково вивчати особливості прояву відповідних загроз в усіх, без виключення, сферах життєдіяльності держави і суспільства;

3. Змінити реактивний підхід реагування на загрози інформаційній та кібербезпеці на проактивний, який грунтується на розширенні національного інформаційного простору, збільшенні власних можливостей впливу на світовий інформаційний простір, зокрема на інформаційний простір Російської Федерації, як держави-агресора, інших держав, міждержавних утворень та окремих суб’єктів, які є джерелами загроз національній безпеці України.

Література

1. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037
2. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
3. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text
5. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року N 514/2009. URL: https://zakon.rada.gov.ua/laws/show/514/2009#Text.

ПОНЯТТЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ. ОСОБИСТІ НЕМАЙНОВІ ТА МАЙНОВІ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Костроміна М.О.
Державний університет телекомунікацій
м.Київ,Україна

Розглянуто поняття права інтелектуальної власності. Досліджена різниця між поняттями «суб'єктивна новизна» та «об'єктивна новизна». Установлено необхідні дії для того щоб результати творчої, інтелектуальної діяльності, що мають об'єктивну новизну, були визнані суспільством як об'єкти права інтелектуальної власності. Визначено що розуміють під особистими немайновими та майновими правами інтелектуальної власності.

В сучасному світі інтелектуальна, творча діяльність набуває все більшого значення майже в усіх сферах цивільно-правових відносин, пов'язаних із розвитком суспільства. Зазвичай поняття «інтелектуальна власність» розуміється в значенні, наданому в Конвенції, що засновує Всесвітню організацію інтелектуальної власності. Ст. 2 цієї Конвенції визначає, що «інтелектуальна власність» містить права, що відносяться до:

- літературних, художніх і наукових творів;
- виконавчої діяльності артистів, звукозапису, радіо – і телевізійних передач;
- винаходів у всіх сферах діяльності людини;
- наукових відкриттів;
- промислових зразків;
- торговельних марок, фірмових найменувань і комерційних позначень;
- захисту від недобросовісної конкуренції, а також всі інші права, які є результатом інтелектуальної діяльності в промисловій, науковій, літературній та художній сферах [3].

У ст. 418 Цивільного кодексу України надано наступне визначення інтелектуальної власності: «Право інтелектуальної власності – це право особи на результат інтелектуальної, творчої діяльності або на інший об'єкт права інтелектуальної власності, визначений цим Кодексом та іншим законом» [2].

Таким чином, під інтелектуальною власністю слід розуміти не продукт інтелектуальної діяльності людини як такий, а право власності на результат інтелектуальної діяльності, що, з одного боку, заслуговують правової охорони, а з іншого боку мають інтелектуальний, творчий характер.

Діяльність людини може бути репродуктивною та творчою. Репродуктивна діяльність – це процес, який виконується за детальним алгоритмом і в результаті якого створюється продукт, що не має новизни як для самого суб'єкта діяльності (суб'єктивна новизна), так і для інших членів суспільства (об'єктивна новизна) [1]. Творча діяльність відрізняється від репродуктивної тим, що це діяльність без алгоритму, кінцевим результатом якої є продукт, який має об'єктивну або суб'єктивну новизну [1].

І саме право на результати творчої, інтелектуальної діяльності, що мають об'єктивну новизну, є інтелектуальною власністю як такою. Але для того щоб ці результати були визнані суспільством як об'єкти права інтелектуальної власності, необхідна їх формалізація у будь-який спосіб. Процес формалізації є передумовою набуття прав інтелектуальної власності в установленому законом порядку [1].

Врегульовані законом суспільні відносини щодо володіння, користування і розпорядження результатами інтелектуальної, творчої діяльності складають закріплений Конституцією України інститут права інтелектуальної власності. Згідно ст. 418 Цивільного кодексу України право інтелектуальної власності становлять особисті немайнові та (або) майнові права інтелектуальної власності [2]. При цьому вони можуть бути різними для різних об'єктів права інтелектуальної власності і встановлюються на законодавчому рівні.

Загалом під особистими немайновими правами інтелектуальної власності розуміють:

- право на визнання людини творцем (автором, виконавцем, винахідником тощо) об’єкта права інтелектуальної власності;
- право перешкоджати будь-якому посяганню на права інтелектуальної власності, здатному завдати шкоди честі чи репутації творця об’єкта права інтелектуальної власності [1].

А до майнових прав інтелектуальної власності зазвичай відносять:

- право на використання об’єкта права інтелектуальної власності;
- виключне право дозволяти використання об’єкта права інтелектуальної власності;
- виключне право перешкоджати неправомірному використанню об’єкта права інтелектуальної власності, в тому числі забороняти таке використання [1].

Таким чином, інтелектуальна власність – це формалізований результат творчої, інтелектуальної діяльності, що надає його автору або особі, визначеній чинним законодавством, право власності на цей результат, яке набувається, здійснюється та захищається відповідно до законодавчо встановлених норм і правил. Право інтелектуальної власності визнається державою шляхом закріплення його в законі; право інтелектуальної власності охороняється та захищається у встановленому законодавством порядку; це право пов’язується з відповідними об’єктами (результати інтелектуальної, творчої діяльності, а також деякі інші прирівняні до них об’єкти права), які визначаються законодавством України, в тому числі і міжнародно-правовими актами.

Література

1. Жаров В.О. Захист прав інтелектуальної власності: норми міжнародного і національного законодавства та їх правозастосування. Практичний посібник. 2017. С. 18-20. URL: http://www.nsj.gov.ua/files/1378882678IPR%20Manual%20UKR.pdf
2. Загальні положення про право інтелектуальної власності. Стаття 418. URL: https://i.factor.ua/ukr/law-54/section-299/article-5641/
3. Конвенция, учреждающая Всемирную организацию интеллектуальной собственности. URL: https://zakon.rada.gov.ua/laws/show/995_169#Text

НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Горпинич Л.І.
Національна академія внутрішніх справ,
м. Київ, Україна

Одним із головних стратегічних пріоритетів є розвиток інформаційного суспільства та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя і в діяльність органів державної влади. Саме цим зумовлена актуальність забезпечення інформаційної безпеки України з метою задоволення національних інтересів людини (громадянина), суспільства та держави в інформаційній сфері.

Згідно ст. 30 "Інформація з обмеженим доступом "Закону України "Про інформацію", інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденціальну і таємну [1].

Конфіденційна інформація - це, відповідно до Закону, відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов. Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого,

банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їхнього професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї систем захисту. Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України та інформація, приховування якої є загрозою для життя і здоров'я людей. До таємної належить інформація, що містить відомості, які становлять державну або іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Відповідно до змісту ч. 2 ст. 30, конфіденційною інформацією з волі вповноваженої особи може бути визнана будь-яка інформація. Однак ч. 4 статті 28 Закону передбачає, що не підлягає необґрунтоване її віднесення до категорії інформації з обмеженим доступом. Оскільки інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну, згідно ст. 28 не допускається необґрунтоване віднесення інформації до конфіденційної, що суперечить ст. 30 [3, с. 43-45].

Згідно тексту ч. 4 ст. 30 Закону України "Про інформацію", інформація комерційного та банківського характеру не може бути визнана конфіденційною, тому в цій частині ст. 30 потребує коригування [1].

Ст. 30 Закону України "Про інформацію" фактично не розмежовує конфіденційну та таємну інформацію, що негативно відбивається й на інших нормах чинного інформаційного законодавства [1].

Ст. 30 у визначенні таємної інформації передбачає, що її розголошення завдає шкоди особі, суспільству і державі. Але власник встановлює для інформації режим обмеженого доступу, відносячи її до категорії конфіденційної також з урахування того, що повідомлення такої інформації третім особам може завдати йому інтересам шкоди. Так само і державні юридичні особи, що володіють інформацією на праві повного господарського відання або оперативного управління (як і іншою державною власністю), тобто титульні володільці згідно змісту ст. 30 можуть відносити таку інформацію до категорії конфіденційної, якщо її розголошення може зашкодити державі. Крім того заподіяння шкоди окремому суб'єкту правовідносин одночасно є заподіянням шкоди правопорядку в цілому, тобто шкода завдається не лише окремій особі, а й суспільству та державі. Таким чином, завдання розголошення інформації шкоди певним інтересам не може вважатися підставою для класифікації інформації. Однак такі підстави мають бути виявлені і зазначені в законі [1].

Закон охороняє як таємну, так і конфіденційну інформацію, тому неможливо говорити про захист першої за допомогою закону, а іншої - засобами власника.

Для визнання інформації конфіденційною необхідно мати певне право на таку інформацію. Держава ж, визнаючи інформацію таємною, керується своїми повноваженнями щодо захисту публічних інтересів, а не правом на інформацію. Звісно, можна зазначити, що встановлення в законі можливості віднесення інформації до категорії конфіденційної також захищає публічні інтереси, тобто всіх, а не окремої особи. Однак норми щодо віднесення інформації до категорії конфіденційної є диспозитивними, що ж стосується віднесення інформації до категорії таємної, тут мають місце імперативні норми - держава наказує визнавати таємною інформацію певного характеру. Різним є також момент отримання інформацією рівня захисту згідно режиму обмеженого доступу: таємною інформація визнається з моменту свого виникнення, конфіденційною ж - з моменту відповідного рішення власника [2, с. 23-24].

Віднесення інформації до категорії конфіденційної є реалізацією повноважень власника, тобто права власності як абсолютного. У той же час визнання інформації таємною являє собою безпосереднє виключення з права на інформацію, передбаченого чинним Законом та Конституцією. Виходячи з цього, закон має передбачати вичерпний перелік видів інформації, що становить "іншу, передбачену законом таємницю", оскільки не встановлення в законі та віднесення до компетенції "відповідних державних органів" визначення порядку її

обігу та захисту призводить до незаконних обмежень права на інформацію. Такий перелік, як і принципи "обґрунтованого віднесення" до інформації з обмеженим доступом, зокрема до категорії конфіденційної, є необхідним. Що стосується конфіденційної інформації, встановлення вичерпного переліку її видів є неможливим, оскільки власник, згідно закону, уповноважений відносити до категорії конфіденційної будь-яку інформацію, крім встановлених законом обмежень. Але якщо закон встановить окремі види конфіденційної інформації та характер відомостей, що до них належать, з метою визначення порядку її обігу та функціонування, це не означатиме вичерпності видів такої інформації та порушення диспозитивності норми. До того ж неможливою є конфіденційність a priori, тобто вимога держави на рівні закону щодо обов'язковості визнання певної інформації конфіденційною.

Разом з тим, стаття 46 закону України "Про інформацію" [1], визначаючи, яка інформація не підлягає розголошенню, відмежовує державну та "іншу передбачену законом таємницю" від лікарської таємниці, таємниці грошових вкладів, прибутків від підприємницької діяльності, усиновлення, листування, телефонних розмов і телеграфних повідомлень, очевидно, не вважаючи зазначені "таємниці" таємною інформацією. Ці непорозуміння мають бути ліквідовані шляхом чіткого окреслення меж та критеріїв різних категорій інформації з обмеженим доступом.

Література

1. Про інформацію: Закон України від 02.10.1992 р. *Закони України*. К. 1996. Т.4. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. URL: http://veche.kiev.ua/journal/598/
3. Шилан Н.Н., Кривонос Ю.М., Бирюков М.Г. Компьютерные преступления и проблемы защиты информации. URL: https://it-crime.at.ua/index/vidpovidalnist_quot_insajderiv_quot/0-36