КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (5), 2019
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2019.5.6172
УДК 004.056

Борсуковський Юрій Володимирович
кандидат технічних наук , професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
OrcID:0000-0003-1973-2386
Y.Borsukovskyi@kubg.edu.ua

ВИЗНАЧЕННЯ ВИМОГ ЩОДО ПОБУДОВИ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ. ЧАСТИНА 1

Анотація. В даній статті проведено аналіз останніх тенденцій реалізації кіберзагроз та сформульовані базові вимоги щодо формування концепції інформаційної безпеки в умовах гібридних загроз. Наведено ключові тенденції реалізацій у кіберпросторі принципів гібридної війни. Визначено, що передумовами виникнення таких гібридних війн стає зростання зацікавленості урядових структур в отриманні інформації, яка може бути використана протиборчими сторонами в світовій конкурентній і політичній боротьбі, а також можливість ефективної монетизації шкідливих впливів на інформаційні та автоматизовані системи організацій. Визначено необхідність адаптивного формування напрямків проведення превентивних заходів з інформаційної і кібернетичної безпеки. Акцентовано увагу на відсутності, у більшості випадків, стратегії забезпечення безпеки щодо захисту ключових інформаційних систем у відповідності до існуючих ризиків. Звернено увагу на те, що концепція інформаційної безпеки в умовах гібридних загроз повинна враховувати можливість повної компрометації систем інформаційної та кібернетичної безпеки при цілеспрямованій атаці на інформаційні активи структурних підрозділів державних, банківських та приватних організацій. Розглянуто можливу структуру концепції інформаційної безпеки в умовах гібридних загроз з метою забезпечення ефективності функціювання інформаційних та автоматизованих систем забезпечення інформаційної та кібернетичної безпеки в умовах обмеженого фінансування. Наведена структура та зміст концепції інформаційної безпеки в умовах гібридних загроз. Визначено, що концепція інформаційної безпеки в умовах гібридних загроз повинна визначати основні цілі та завдання, а також загальну стратегію побудови ІТ і системи управління інформаційною безпекою організації. Сформовані вимоги та базові підходи до її реалізації. Визначено, що одним із шляхів оптимізації фінансових ресурсів, що витрачаються на системи ІТ і системи інформаційної та кібернетичної безпеки, у відповідності до визначених ризиків, може стати використання кращих світових практик, а також чітке узгодження вимог забезпечення інформатизації та цифрової трансформації з боку бізнесу і створення узгоджених регулятивних вимог до певних напрямків бізнесу з точки зору інформаційної та кібернетичної безпеки.

Ключові слова: загрози, ризики, класифікація, кібербезпека, стратегія, концепція**.**

1. ВСТУП

Постановка проблеми. Розгорнутий аналіз тенденцій розвитку кіберзагроз показує, що кількість атак проти державних, банківських і приватних організацій країн світу постійно зростає, а самі атаки стають дедалі досконалішими 0.

Відділ ФБР, що займається кіберзлочинністю (IC3), опублікував звіт «2018 Internet Crime Report», згідно з яким за минулий рік втрати від злочинів в кіберпросторі склали 2 700 000 000 доларів США. Згідно із цими ж даними, в період з 2014 до 2018 року злочини в цифровому світі стали причиною втрати $ 7,45 млрд. 0.

Така ситуація вимагає динамічної адаптації інформаційних систем і систем інформаційної безпеки до поточного ландшафту загроз, а також впровадження в технологічну мережу організації декількох типів рішень безпеки з метою знизити загрозу зовнішніх та (або) внутрішніх кібератак, здатних пошкодити або відключити її. Це, у свою чергу, потребує коригування концепції інформаційної безпеки з метою визначення пріоритетних напрямків проведення превентивних заходів із планування та розгортання ІТ, систем інформаційної та кібернетичної безпеки відповідно до поточного ландшафту загроз в інформаційній сфері 0.

Аналіз останніх досліджень і публікацій. У жовтні 2017 року Європейська Рада зобов'язала уряди країн ЄС посилити питання кібербезпеки. Останні рішення, прийняті Європейською Радою, вказують на необхідність виділення всіма країнами-членами ЄС потрібних ресурсів та інвестиції для боротьби із кіберзлочинністю 0.

Створення та поширення перспективних інформаційних систем та технологій сприяє появі нових форм кібератак, що піддають державні, банківські та приватні інформаційні ресурси загрозам, з якими вони не готові мати справу. Кібератаки можуть становити критичну загрозу для тих економік, держав і суспільств, у яких недостатньо розвинуте співробітництво і відсутня ефективна система інформаційного та кібернетичного захисту. Результати аналізу векторів кібератак говорять про те, що у кіберпросторі сформувалася стійка тенденція свого роду гібридної війни. Головною передумовою такої тенденції стало перш за все зростання зацікавленості урядових структур в отриманні інформації, яка може бути використана протиборчими сторонами в світовій конкурентній і політичній боротьбі 0.

Як приклад, можна навести статистику звернень у відділ IC3 боротьби із кіберзлочинами ФБР США. IC3 почав свою роботу в травні 2000 року і з цього моменту отримав 4 415 870 скарг на кіберзлочини - це близько 300 000 скарг щорічно. У 2018 році відділ ФБР отримував більше 900 скарг на день 0.

Запобігти витоку даних або захистити інформаційні системи від злому дуже складно, тому що в світі існує величезна кількість ризиків кібербезпеки. Значним каталізатором цих процесів є можливість ефективної монетизації, через електронні гаманці пірінгових платіжних систем, результатів шкідливих впливів на інформаційні та автоматизовані системи управління (ІАСУ) 0. Тим не менш, якщо вживати системних і адекватних заходів захисту, це допоможе значно знизити ризики успішних реалізацій зовнішніх та внутрішніх атак.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Враховуючи викладене, особливо важливо прийняти зважене рішення, щодо напрямків і пріоритетів захисту ключових інформаційних та автоматизованих систем управління в державних, банківських та приватних організаціях. При цьому треба враховувати тенденції багатовекторності та швидкозмінності схем атак, орієнтованих на невідомі вразливості або відсутності ефективних систем захисту від них на фоні обмеженого фінансування в сферах ІТ та ІБ. Це особливо актуально в економічних умовах, в яких сьогодні знаходиться Україна. Тут ми постійно стикаємося з низкою проблем, які потребують пріоритетного розгляду при прийнятті рішень 0, 0, 0.

Твердження 1. Запобігти витоку даних або захистити ІАСУ від злому дуже складно, тому що в світі існує величезна кількість ризиків кібербезпеки. Формально багато організацій мають ретельно прописані ІТ-політики, які забезпечують додатковий

захист, але, як показує практика, їх дуже часто не дотримуються. Це може бути пов'язано з тим, що персонал Організації недостатньо обізнаний про те, чим загрожують потенційні вразливості ІАСУ. Поставити під загрозу цілісність даних і інформаційну безпеку ІТ-ІБ систем можуть також сторонні ділові партнери, які не приділяють пильної уваги питанням безпеки. Кіберзлочинці націлені на отримання максимальної вигоди і постійно вдосконалюють методи атак. По такому принципу потрібно підходити до концепції інформаційної безпеки в умовах гібридних загроз ІАСУ. Вона повинна адаптивно змінюватися, відповідно до нових викликів та загроз, що формуються в кіберпросторі.

Твердження 2. Концепція інформаційної безпеки в умовах гібридних загроз повинна враховувати той факт, що при цільовій атаці зловмисники досягнуть 100% успіху. Ґрунтуючись на даній аксіомі повинні бути внесені відповідні зміни в інфраструктуру ІТ та ІБ, а також, з дуже високим ступенем імовірності, і в деякі бізнес процеси, які можуть виявитися критичними в разі успішної кібератаки. Крім того, концепція інформаційної безпеки в умовах гібридних загроз повинна враховувати організаційну структуру компанії і її міжструктурний інформаційний обмін. Це означає, що концепція інформаційної безпеки в умовах гібридних загроз повинна враховувати розподілену структуру Організації і те, що будь який елемент ІАСУ може бути успішно атакований зловмисниками. Іншими словами, концепція інформаційної безпеки в умовах гібридних загроз повинна враховувати можливість побудови уточнених моделей безпеки та використання додаткових посилених засобів захисту для ключових структурних елементів Організації. Але це не повинно бути стандартизовано і не приводити до хаосу при побудові СУІБ в цілому.

Твердження 3. Оскільки інформаційні та кібернетичні атаки стають все більш витонченими і до того ж можуть бути цілеспрямованими, компанії не повинні покладатися на один або два типи превентивного захисту - необхідно застосовувати більш широку стратегію застосування рівнів безпеки залежно від структури і цілей організації, а також значення в забезпеченні неперервності бізнесу як компанії в цілому, так і окремих її структурних підрозділів.

Твердження 4. Концепція інформаційної безпеки в умовах гібридних загроз повинна бути орієнтована на підвищення обізнаності персоналу. Внутрішні порушники, зовнішні атаки, нові інфраструктурні сервіси та бізнес-додатки вже складають багатовимірну множину активів і ризиків. Швидке адаптування концепції інформаційної безпеки до поточного ландшафту інформаційних та кібернетичних загроз є достатньо проблематичним відносно врахування кращих світових практик, якості управлінських рішень і ефективності налаштувань систем кібербезпеки в цілому. Особливо це стає критичним відносно до ключових складових функціювання бізнесу в сучасних умовах швидких змін та багатовекторності ландшафту загроз.

Твердження 5. Управління вимогами до ІТ з боку бізнесу вимагає створення узгоджених регулятивних вимог до певних напрямків бізнесу з точки зору ІБ. При вироблені узгоджених вимог повинно бути розуміння не тільки завдань бізнесу, а і розуміння проблем ІТ та ІБ для того, щоб амортизувати корпоративні тертя і оптимізувати часові та фінансові витрати при виробленні спільного ефективного рішення до захисту ключових складових функціонування бізнесу.

Твердження 6. Формування повноцінної концепції інформаційної безпеки в умовах гібридних загроз дозволяє в цілому сформулювати підходи до визначення загроз безпеки інформації, реалізація яких може призвести до порушення штатних режимів

функціонування інформаційних та автоматизованих систем управління виробництвом та забезпечення неперервності функціонування бізнесу.

Об’єднуючи всі ці твердження, ми можемо сформулювати мінімальні умови, при яких ми можемо, на основі аналізу сучасних загроз і оцінок власних ризиків, сформулювати вимоги до структури та змісту концепції інформаційної безпеки в умовах гібридних загроз з метою оптимізації та підвищення ефективності побудови процесів забезпечення ІТ та ІБ ІАСУ державних та приватних організацій.

Концепція інформаційної безпеки в умовах гібридних загроз повинна визначати:

- **Основні принципи формування переліку критичних активів ІАСУ**, що потребують захисту, який формується в процесі проведення аудиту ІТ, ІБ і аналізу ризиків. Даний перелік повинен включати в себе опис фізичних, програмних і інформаційних активів з визначенням вартості активів і ступеня їх критичності для Організації.
- **Основні принципи захисту**, що визначають стратегію забезпечення ІТ та ІБ, і перелік правил та вимог, якими необхідно керуватися при побудові системи управління інформаційною безпекою ІАСУ Організації.
- **Основні підходи до організації робіт із захисту інформації** в державних та приватних організаціях, розподіл ролей і порядок взаємодії підрозділів державних та приватних організацій при здійсненні заходів щодо забезпечення інформаційної безпеки ІАСУ, розробку та узгодження організаційно-розпорядчих документів.
- **Порядок класифікації інформації**, що підлягає захисту, і основні підходи до забезпечення безпеки різних категорій інформаційних активів ІАСУ.
- **Модель порушника безпеки**, яка визначається на основі обстеження активів ІАСУ і способів їх використання.
- **Модель загроз безпеки і основні підходи до оцінки ризиків**, пов'язаних з їх здійсненням, що формуються на основі переліку критичних активів ІАСУ і моделі порушника, яка включає визначення ймовірностей загроз і способів їх здійснення, а також оцінок можливих збитків.
- **Вимоги безпеки** для кожної з основних підсистем ІАСУ та інформаційної безпеки, що визначаються за результатами оцінки ризиків.
- **Заходи забезпечення безпеки організаційного і програмно-технічного рівня**, що вживаються для реалізації перерахованих вимог.
- **Відповідальність** співробітників державних та приватних організацій і прирівняних до них осіб за дотримання встановлених вимог інформаційної безпеки ІАСУ при експлуатації інформаційних та безпекових систем Організації.

На основі вищевказаних визначень можна сформулювати базові вимоги до структури концепції інформаційної безпеки в умовах гібридних загроз:

- Терміни та визначення
- Загальні положення
- Нормативні посилання
- Опис об'єкта захисту
- Основні фактори, що впливають на інформаційну безпеку організації
- Основні принципи забезпечення інформаційної безпеки

- Організаційна структура служби інформаційної безпеки
- Організація робіт із захисту інформації
- Заходи управління інформаційною безпекою
- Розподіл відповідальності і порядок взаємодії
- Порядок класифікації інформації що підлягає захисту
- Модель порушника безпеки
- Модель загроз безпеки
- Вимоги щодо забезпечення інформаційної безпеки ІАСУ
- Технічні вимоги до суміжних підсистем
- Відповідальність співробітників за порушення вимог щодо забезпечення інформаційної безпеки
- Аудит і звітність
- Механізм реалізації концепції
- Історія змін

Розглянемо послідовно орієнтовні вимоги до змісту концепції інформаційної безпеки в умовах гібридних загроз. Звертаю увагу, що наведені базові вимоги є не догмою, а керівництвом до дій, що рекомендується враховувати при розроблені концепції інформаційної безпеки ІАСУ Організації.

ТЕРМІНИ ТА ВИЗНАЧЕННЯ – вводяться з метою однозначного трактування визначень та понять в документі. Враховуємо те, що документ орієнтований на керівний склад Організації, який може не володіти термінологією що використовується в ІТ та ІБ.

При визначені термінів пріоритетними повинні бути терміни та визначення, що даються в нормативних документи ДССЗЗІ та діючих Державних стандартах України 0, 0, 0. Посилання на документи ІСО/ІЕС з метою уточнень термінів та визначень буде тільки вітатися 0, 0.

Термін		Визначення
Адміністративна мережа	-	Локальна обчислювальна мережа, яка використовується для налаштування і управління активним мережевим обладнанням корпоративної мережі і мережевими засобами захисту інформації
Аутентифікація	-	перевірка приналежності суб'єкту доступу пред'явленого їм ідентифікатора; підтвердження автентичності. Найчастіше аутентифікація виконується шляхом набору користувачем свого пароля на клавіатурі комп'ютера
Внутрішня мережа	-	внутрішня ділянка корпоративної мережі, відділена від зовнішньої мережі (мережі Інтернет) і DMZ міжмережним екраном. Внутрішня мережа об'єднує виробничі, тестові і адміністративні мережі
Демілітаризована зона (DMZ)	-	ділянка корпоративної мережі, розташована між зовнішнім МЕ і зовнішнім маршрутизатором, що використовується для підключення корпоративної мережі до мережі телекомунікаційних провайдерів (мережі Інтернет). У DMZ розміщуються сервери, які використовуються для взаємодії і надання мережевих

		сервісів зовнішнім користувачам корпоративної мережі, а також сервери, які з міркувань інформаційної безпеки недоцільно розміщувати у внутрішній мережі Організації
Захищений канал передачі даних	-	логічні і фізичні канали мережевої взаємодії, захищені від прослуховування потенційними зловмисниками засобами шифрування даних (засобами VPN), або шляхом їх фізичної ізоляції і розміщення на території, що охороняється
Ідентифікація	-	присвоєння суб'єктам доступу (користувачам, процесам) і об'єктам доступу (інформаційним ресурсам, пристроям) ідентифікатора та (або) порівняння пред'явленого ідентифікатора із переліком присвоєних ідентифікаторів
Інформаційна система (ІС)	-	сукупність програмного забезпечення і технічних засобів, що використовуються для зберігання, обробки і передачі інформації, з метою вирішення бізнес завдань підрозділів Організації. У Організації можуть використовуватися різні типи інформаційних систем для вирішення виробничих, управлінських, облікових та інших бізнес завдань
Інформаційний актив	-	матеріальний або нематеріальний об'єкт, який: є інформацією або містить інформацію, служить для обробки, зберігання або передачі інформації, має цінність для організації
Інформація з обмеженим доступом (ІзОД)	-	інформація, доступ до якої обмежено Організацією і яка може поширюватися у визначеному Організацією порядку, відповідно до діючого законодавства і передбаченими Організацією умовами
ІТ		Інформаційні технології
Корпоративна мережа Організації	-	об'єднання інформаційних систем, комп'ютерного, телекомунікаційного та офісного обладнання всіх підрозділів Організації, за допомогою їх підключення до єдиної комп'ютерної мережі передачі даних з використанням різних фізичних і логічних каналів зв'язку
Критична інформація	-	інформація, порушення доступності, цілісності, або конфіденційності якої, може мати негативний вплив на функціонування підрозділів Організації, призвести до заподіяння Організації матеріального, іміджевого чи іншого виду шкоди
Локальна обчислювальна мережа (ЛОМ)	-	група ЕОМ, а також периферійне устаткування, об'єднані одним або декількома автономними високошвидкісними каналами передачі цифрових даних в межах одного або декількох довколишніх кампусів (будівель)

Міжмережевий екран (МЕ)	-	програмно-апаратний комплекс, який використовується для контролю доступу між ЛОМ, що входять до складу корпоративної мережі, а також між корпоративною мережею та зовнішніми мережами (мережею Інтернет)
Несанкціонований доступ (НСД)	-	доступ до інформації, що порушує встановлені правила розмежування доступу
Користувач інформаційної системи	-	співробітник Організації (штатний, тимчасовий, який працює за контрактом і т.п.), а також інші особи (підрядники, аудитори і т.п.), зареєстровані в корпоративній мережі Організації у встановленому порядку і які отримали права на доступ до ресурсів корпоративної мережі відповідно до своїх функціональних обов'язків
Принцип мінімізації привілеїв	-	один з основних керівних принципів, який використовується при призначенні повноважень користувачам і адміністраторам мережі, а також при розробці списків контролю доступу. Відповідно до цього принципу користувачам надаються тільки ті повноваження і сервіси, які є необхідними для виконання ними своїх службових обов'язків
Виробнича мережа	-	основна частина корпоративної мережі, яка використовується для роботи бізнес-підрозділів Організації, що є об'єднанням ЛОМ різних підрозділів Організації
Реєстраційний (обліковий) запис користувача	-	включає в себе ім'я користувача і його унікальний цифровий ідентифікатор, що однозначно ідентифікує даного користувача в операційній системі (мережі, базі даних, додатку і т.п.). Реєстраційний запис створюється адміністратором при реєстрації користувача в операційній системі комп'ютера, в системі управління базами даних, в мережевих доменах, додатках і т.п. Він також може містити такі відомості про користувача, як П.І.Б., назву підрозділу, телефони, E-mail і т.п.
Мережеві (інформаційні) сервіси	-	мережеві додатки, що надають різні види сервісів для внутрішніх і зовнішніх користувачів корпоративної мережі, включаючи DNS, FTP, HTTP, Telnet, і інші
СІТ	-	служба інформаційних технологій
СлІБ	-	служба інформаційної безпеки
Список контролю доступу (ACL)	-	правила фільтрації мережевих пакетів, що настроюються на маршрутизаторах, комутаторах і МЕ, які визначають критерії фільтрації і дії, що здійснюються над пакетами

Тестова мережа	-	спеціальний тип ЛОМ організований фахівцями СІТ з метою апробації ІТ та ІБ рішень перед введенням їх в експлуатацію, порівняльного тестування програмних та апаратних продуктів різних виробників, нових версій програмних продуктів та в інших тестових цілях

ЗАГАЛЬНІ ПОЛОЖЕННЯ - концепція інформаційної безпеки в умовах гібридних загроз повинна визначати основні цілі та завдання, а також загальну стратегію побудови комплексної системи управління інформаційною безпекою Організації, основні вимоги та базові підходи до її реалізації.

Система управління інформаційною безпекою (СУІБ) являє собою сукупність заходів організаційного та програмно-технічного рівня, спрямованих на захист інформаційних активів ІАСУ Організації від загроз безпеці. Заходи захисту організаційного рівня реалізуються шляхом проведення відповідних заходів, передбачених документованою політикою безпеки. Заходи захисту програмно-технічного рівня реалізуються за допомогою відповідних програмно-технічних засобів і методів захисту.

Економічний ефект від впровадження СУІБ ІАСУ повинен проявлятися в зниженні величини можливого матеріального, морального та інших видів шкоди, що завдається ІАСУ Організації, за рахунок заходів, спрямованих на формування та підтримання заданого режиму інформаційної безпеки. Ці заходи покликані забезпечити:

- **Конфіденційність інформації** (стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, які мають на неї право).
- **Цілісність інформації** (стан інформації, при якому відсутня будь-яка її зміна або зміна здійснюється тільки навмисно суб'єктами, що мають на це право).
- **Доступність інформації** (можливість за прийнятний час отримати доступ до інформації авторизованими користувачами).
- **Неможливість відмови від авторства (неспростовності)** (здатність засвідчувати, чи мала місце дія чи подія так, що ці події або дії не могли бути пізніше відкинуті).
- **Дійсність (автентичність)** (властивість, яка гарантуватиме, що суб'єкт або ресурс ідентичні заявленим).

Концепція інформаційної безпеки в умовах гібридних загроз ІАСУ Організації повинна визначати склад критичних інформаційних активів і основні принципи їх захисту. Принципи забезпечення ІТ та ІБ обумовлюють необхідність застосування певних методів і технологій захисту. Визначення способів реалізації цих принципів шляхом застосування конкретних програмно-технічних засобів захисту інформації (ЗЗІ) та системи організаційних заходів, є предметом конкретних проектів і політик безпеки, що розробляються на основі даної концепції.

Концепція повинна переглядатися в міру виявлення нових методів і технологій здійснення атак на інформаційні активи. Подібний перегляд також повинен проводитися в міру розвитку інформаційних систем (ІС) Організації. Рекомендований термін перегляду концепції становить три роки (за умови відсутності корінних змін в структурі системи, в технологіях управління і передачі інформації).

Підготовка концепції, внесення в неї змін і загальний контроль виконання співробітниками Організації вимог до ІТ та ІБ ІАСУ здійснюється СлІБ.

Відповідальність за виконання вимог ІТ та ІБ, які визначаються концепцією та іншими організаційно-розпорядчими документами Організації, що розроблені відповідно до неї, покладається на керівників структурних підрозділів, а також адміністраторів і користувачів корпоративної мережі Організації.

Перелік необхідних заходів захисту інформації визначається за результатами аудиту безпеки ІАСУ Організації і аналізу ризиків з урахуванням співвідношення витрат на захист інформації з можливим збитком від її розголошення, втрати, знищення, перекручення, порушення доступності інформації і працездатності технічних засобів, що обробляють цю інформацію.

Стратегія системи управління ІТ та ІБ ІАСУ повинна будуватися відповідно до чинного законодавства в сфері захисту інформації, вимог міжнародних, галузевих, промислових і інтернет стандартів, а також врахування напрацьованих галузевих практик щодо захисту ІАСУ.

Все це, з урахуванням кращих світових практик, дозволяє достатньо ефективно сформувати концепцію інформаційного та кібернетичного захисту критичних інформаційних активів ІАСУ в умовах гібридних загроз ресурсам ІТ та ІБ. Розроблена та затверджена концепція інформаційної безпеки в умовах гібридних загроз ІАСУ дозволяє бізнесу орієнтуватися на оцінки ключових ризиків і розроблену стратегію захисту/мінімізації від їх реалізації і на цій основі приймати планові рішення щодо мінімізації ризиків і оптимізації фінансових витрат на ІТ та ІБ ІАСУ Організації.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Сучасні проблеми глобалізації та висока ефективність перспективних ІТ технологій підвищує імовірність реалізації сучасних інформаційних і кібернетичних загроз і, як наслідок, це може сприяти виникненню загального світового колапсу. Кібератаки все частіше стають інструментом швидкого досягнення необхідних результатів як в економічній, так і політичній сферах.

На даний час питання цифрової трансформації і забезпечення безпеки ключових інформаційних активів в державних та приватних організаціях стоїть досить гостро у цілому світі. Сформовані вимоги до складових та змісту концепції інформаційної безпеки в умовах гібридних загроз та вимоги щодо прикладних аспектів побудови стратегії захисту в умовах обмежених фінансових ресурсів можуть бути використані при розробці політик захисту ІАСУ державних та приватних організацій.

Враховуючи те, що шкідливі програми і кібератаки з кожним роком удосконалюються, повинна вдосконалюватися і стратегія по їх запобіганню. Потрібно не просто купувати найсучасніші ІТ та ІБ засоби, а й постійно стежити за ефективністю їх використання, що дозволить державним та приватним організаціям забезпечити максимальний захист та оптимізувати фінансові витрати.

Подальші дослідження варто зосередити на формуванні інших розділів концепції інформаційної безпеки в умовах гібридних загроз ІАСУ, створенні та впровадженні на її основі типових політик, процедур та рекомендацій щодо захисту інформаційних активів державних і приватних організацій як опорних точок для побудови оптимізованих по ефективності, вартості і функціоналу систем ІТ та систем інформаційної і кібернетичної безпеки ІАСУ.

ISSN 2663 - 4023

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1].FBI online Internet Crime Complaint Center(IC3). [Електронний ресурс]. Режим доступу: https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf/ [Перевірено 06 жовтня 2019]
[2].Борсуковський Ю.В., Борсуковська В.Ю., Бурячок В.Л. «Напрямки формування політик кібербезпеки для державного, банківського та приватного секторів», Modern Methodologies, Innovations, and Operational Experience on the Field of Technical Science: Conference proceedings, December 27-28, 2017, Radom, Republic of Poland, с. 8-11
[3].Борсуковська В. Ю., Борсуковський Ю. В. «Безперервність бізнесу: новий тренд або необхідність», Економіка. Менеджмент. Бізнес. - 2017, № 2(20), с. 48-52
[4].Борсуковський Ю.В., Бурячок В.Л., Борсуковська В.Ю. «Базові напрямки забезпечення кібербезпеки державного та приватного секторів», Сучасний захист інформації, - 2017, № 2(30), с. 85-89
[5].Державна служба спеціального зв'язку та захисту інформації. [Електронний ресурс]. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index [Перевірено 25 вересня 2019]
[6].Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості». [Електронний ресурс]. Режим доступу: http://uas.org.ua/ua/ [Перевірено 25 вересня 2019]
[7].БУДСТАНДАРТ Online - Сервіс нормативних документів. [Електронний ресурс]. Режим доступу: http://online.budstandart.com/ua/ [Перевірено 25 вересня 2019]
[8].Міжнародна організація по стандартизації (International Organization for Standardization). [Електронний ресурс]. Режим доступу: https://www.iso.org [Перевірено 25 вересня 2019]
[9].Міжнародна електротехнічна комісія (International Electrotechnical Commission). [Електронний ресурс]. Режим доступу: https://www.iec.ch/ [Перевірено 25 вересня 2019]
[10].Хакер. [Електронний ресурс]. Режим доступу: https://xakep.ru/2019/10/03/ransomware-attacks-medical/ [Перевірено 06 жовтня 2019]

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (5), 2019
ISSN 2663 - 4023

Yurii V. Borsukovskyi
PhD in technical sciences, professor of the Department of Information and cyber security
Borys Grinchenko Kyiv University, Ukraine
OrcID: 0000-0003-1973-2386
Y.Borsukovskyi@kubg.edu.ua

DEFINING REQUIREMENTS TO DEVELOP INFORMATION SECURITY CONCEPT N HYBRID THREATS CONDITIONS. PART 1

Abstract. Current article provides the analysis of recent trends in realization of cyber threats and collects the basic requirements for development of information security concept in hybrid threats conditions. It covers the key tendencies of realization at cyber space of principles of hybrid war. Envisages that preconditions for occurrence of such hybrid wars constitute the interest of governmental agencies in information that might be used by opposing parties in world`s competition and political battles, as well the possibility of effective monetization of harmful impact at information and automated systems of companies. The article defines the necessity in adaptive development of directions in application of preventive actions at information and cyber security. It underlines the absence, at most cases, of strategy to ensure security of the key information systems considering the existing risks. Article emphasize that the information security concept in hybrid threats conditions shall consider the possibility of complete compromising of systems of information and cyber security in case of targeted attack at information resources of structural units of state, banking and private organizations. It considers the model structure of information security concept in hybrid threats conditions to ensure the effectiveness of functioning of information and automated systems of information and cyber security in conditions of limited financing. It provides structure and content of the concept of information security in hybrid threats conditions. Article defines that the information security concept at hybrid threats conditions shall cover the main tasks and objectives, and the general strategy for development of IT and system for managing of information security within the company. It formulates the requirements and basic approaches to its implementation. The article defines that the possible way to optimize the financial resources assigned for IT systems and information and cyber security systems according to the risks defined, might be the use of the best world practices, as well the strict coordination of requirements to ensure the informatization and digital transformation from business and development of coordinated regulatory requirements to the certain businesses from information and cyber security perspective.

Keywords: threats, risks, classification, cyber security, strategy, concept.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1].FBI online Internet Crime Complaint Center(IC3). [Online]. Available: https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf/ [Accessed: Oktober 06, 2019]
[2].Borsukovskii Y.V., Borsukovska V.Y., Buriachok V.L. «Directions for creation of informational security policies for the state, banking and private sectors», Modern Methodologies, Innovations, and Operational Experience on the Field of Technical Science: Conference proceedings, December 27-28, 2017, Radom, Republic of Poland, p. 8-11
[3].Borsukovska V.Y., Borsukovskii Y.V. «Business Continuity: new trend or necessity», Economy. Management. Business. - 2017, № 2(20), c. 48-52
[4].Borsukovskii Y.V., Buriachok V.L., Borsukovska V.Y. «Basic ways to ensure cyber security of state and private sectors», Modern Information Security, - 2017, № 2(30), c. 85-89
[5].State Service of Special Communication and Information Protection of Ukraine. [Online]. Available: http://www.dsszzi.gov.ua/dsszzi/control/uk/index [Accessed: September 25, 2019]
[6].Ukrainian Research and Training Center of Standardization, Certification and Quality. [Online]. Available: http://uas.org.ua/ua/ [Accessed: September 25, 2019]
[7].Budstandard Online - Document service. [Online]. Available: http://online.budstandart.com/ua/ [Accessed: September 25, 2019]
[8].International Organization for Standardization. [Online]. Available: https://www.iso.org [Accessed: September 25, 2019]

[9].International Electrotechnical Commission. [Online]. Available: https://www.iec.ch/ [Accessed: September 25, 2019]
[10].Хакер.ru [Online]. Available: https://xakep.ru/2019/10/03/ransomware-attacks-medical/ [Accessed: October 06, 2019]