КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№2 (6), 2019
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2019.6.112121
УДК 004.056

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

ВИЗНАЧЕННЯ ВИМОГ ЩОДО ПОБУДОВИ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ. ЧАСТИНА 2

Анотація. В даній статті розглянуто тенденції ландшафту гібридних загроз на 2020 і послідуючі роки. Наведено ключові аспекти реалізації у кіберпросторі гібридних загроз та шляхів протидії їм, які тісно пов'язані із постійною зміною напрямів кібератак, підвищення їх ефективності і швидкості реалізації, використанням систем штучного інтелекту для забезпечення безпеки інформаційних ресурсів і створення адаптивних систем несприятливості до інформаційних і кібернетичних загроз, використання методів машинного навчання для більш повного уявлення про поточний стан загроз, застосування принципів штучного інтелекту і сценаріїв реагування для передбачення кібератак, розробки індивідуальних планів дій з опорою на системи штучного інтелекту з метою поліпшення розкриття загроз і пришвидшення реагування, використання можливостей контррозвідки і контр-методів з метою оперативного реагування на будь-які шпигунські прийоми до початку активних дій, посилення зв`язків між правоохоронними органами з метою формування єдиного підходу для взаємодії між правоохоронними органами міжнародного і місцевого рівнів, урядовими організаціями, корпоративним сектором та експертами в галузі безпеки. Визначена необхідність розробки валідованих експертами стратегій для захисту від інформаційних та кібернетичних нападів злочинців. Розглянуто опис об'єкта захисту із визначенням призначення і основних функцій системи, групи завдань, що вирішуються в системі, визначена класифікація користувачів системи, організаційна структура обслуговуючого персоналу, структура і склад комплексу програмно-технічних засобів, види інформаційних активів, що зберігаються і обробляються в системі, структура інформаційних потоків, характеристики каналів взаємодії з іншими системами і точок входу. Сформульовані основні принципи забезпечення безпеки при розробці концепції інформаційної та кібернетичної безпеки в умовах гібридних загроз, а саме простоти архітектури, апробованості рішень, керованості, простоти експлуатації, ешелонування оборони, безперервності захисту в просторі і часі, рівноміцності оборони в усіх напрямках, проактивного захисту, мінімізації привілеїв, розподілу обов'язків, економічної доцільності, спадковості і безперервності вдосконалення. Визначено базові критерії щодо вибору програмно-технічних рішень для забезпечення інформаційної та кібернетичної безпеки.

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

1. ВСТУП

Постановка проблеми. В частині один [9] були розглянуті структура та загальні положення щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Далі послідовно розглянемо базові вимоги щодо опису об'єкта захисту та основних принципів інформаційного та кібернетичного захисту Організації. Для кращої інтерпретації дослідження та компактного викладу матеріалу буде, як приклад, наводитись ряд посилань та тверджень щодо умовної Організації, для якої повинна бути розроблена та затверджена концепція інформаційної безпеки [1-3].

©Ю. В. Борсуковський, 2019.

Аналіз останніх досліджень і публікацій. Аналіз ландшафту загроз на 2020 і послідуючі роки, що був підготовлений командою експертів FortiGuard Labs [10], показує, що успіх зловмисників при проведенні кібератак тісно пов'язаний із постійно зростаючою множиною векторів атак, а також наявністю значних прогалин в кібербезпеці, викликаних цифровою трансформацією у всіх сферах життя суспільства.

Висновки дослідження потребують уже зараз враховувати наступні гібридні загрози [10]:

- Постійна зміна напрямів кібератак і як наслідок підвищення їх ефективності і швидкості реалізації.
- Еволюція штучного інтелекту для забезпечення безпеки і створення адаптивних систем несприятливості до загроз.
- Використання розподіленого машинного навчання для більш повного уявлення про поточний стан загроз.
- Застосування досягнень штучного інтелекту і сценаріїв реагування з метою передбачення кібератак і розробки індивідуальних планів дій з опорою на системи штучного інтелекту для поліпшення розкриття потенційних загроз і пришвидшення реагування на них.
- Можливості контррозвідки і контр-методів з метою оперативного реагування на будь-які шпигунські прийоми до початку активних дій із збереженням за собою переваг в контролі.
- Посилення зв’язків між правоохоронними органами з метою формування єдиного підходу для взаємодії між правоохоронними органами міжнародного і місцевого рівнів, урядовими організаціями, корпоративним сектором та експертами в галузі безпеки.

Фахівці також фіксують кібератаки для впливу і моніторингу рівня технологічної безпеки. Все це потребує розроблення та дотримування ефективних (валідованих експертами) стратегій для захисту Організацій від інформаційних та кібернетичних нападів злочинців.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

НОРМАТИВНІ ПОСИЛАННЯ

Вимоги до концепції інформаційної безпеки в умовах гібридних загроз повинні бути розроблені на основі наступних нормативних документів в області інформаційної безпеки [4-8]:

- Конституція України.
- Закон України "Про інформацію".
- Закон України "Про захист персональних даних".
- Цивільний кодекс України.
- Господарський кодекс України.
- Кримінальний процесуальний кодекс України.
- Кодекс про адміністративні порушення України.
- Керівні документи ДССЗЗІ України.
- ДСТУ ISO/IEC 27000. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд і словник.
- ДСТУ ISO/IEC 27001. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.

- ДСТУ ISO/IEC 27002. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
- ISO/IEC 27003. Information security management system implementation guidance (Керівництво по реалізації системи менеджменту інформаційної безпеки)
- ISO/IEC 27004. Information security management — Measurement (Менеджмент інформаційної безпеки. Вимірювання).
- ДСТУ ISO/IEC 27005. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки.
- ДСТУ ISO-IEC 27006. Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою.
- ISO/IEC 27007. Guidelines for information security management systems auditing (Керівні принципи аудиту систем управління інформаційною безпекою).
- ISO/IEC 27011. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (Настанови щодо управління захистом інформації організацій, що пропонують телекомунікаційні послуги, на основі ISO /IEC 27002).

ОПИС ОБ'ЄКТА ЗАХИСТУ

Призначення і основні функції системи. ІС об'єкта захисту призначена для створення інформаційної інфраструктури Організації, надання співробітникам структурних підрозділів різних видів інформаційних сервісів, автоматизації фінансової діяльності та бізнес процесів.

Групи завдань, що вирішуються в системі. Групи завдань, що вирішуються в системі, визначаються наступним чином:

- Автоматизація робочих місць співробітників Організації.
- Надання співробітникам Організації доступу до спільно використовуваних файлових ресурсів ЛВС і серверів БД.
- Надання співробітникам Організації інформаційних сервісів і доступу до внутрішніх і зовнішніх WEB-ресурсів.
- Надання послуг електронної пошти та можливостей колективної роботи з документами.
- Зберігання інформації, необхідної для здійснення діяльності Організації.
- Надання співробітникам Організації мобільного доступу до інформаційних ресурсів та інформаційних систем.
- Надання авторизованого і контрольованого гостьового доступу до інформаційних ресурсів та інформаційних систем.
- Автоматизація діяльності фінансової служби, забезпечення процесів здійснення платежів через банківські установи.
- Архівування інформації, яка використовувалася для здійснення діяльності Організації і може знадобитися в майбутньому.
- Знищення інформації, яка використовувалася для здійснення діяльності Організації і не знадобиться в майбутньому.

Вирішення перерахованих завдань реалізується на базі інформаційної інфраструктури ЛВС з використанням спеціалізованих додатків, загальнодоступних мережевих сервісів і успадкованих додатків. До спеціалізованих програм відносяться система M.E.Doc, системи обліку 1С, системи IT-підприємство, системи EPM Oracle,

Ліга Закон і ін. До загальнодоступних сервісів ЛВС відносяться - електронна пошта (MS Exchange - внутрішня пошта, SMTP - зовнішня пошта), файловий сервіс на основі протоколів Microsoft Distributed File System (DFS), система обміну даними бізнес-підрозділів на базі FTP, сервіс надання захищених термінальних сесій RDP APP, система колективної роботи Microsoft, система самообслуговування користувачів MS System Center і т.д. Базова серверна інфраструктура Організації повинна бути побудована на затвердженій до використання віртуальній платформі (наприклад, VMware) і повинна являти собою відмовостійкий серверний комплекс. До успадкованих додатків відносяться автоматизовані робочі місця користувачів і керівників, що працюють на базі IT-розробок поза контуром спеціалізованих додатків.

Класифікація користувачів системи. Користувачем ІС є будь-який співробітник Організації, зареєстрований в мережі відповідно до встановленого порядку, якому надається доступ до інформаційних ресурсів ЛВС і додатків відповідно до його функціональних обов'язків. Особливу категорію користувачів ЛВС становить керівництво Організації, робочі станції якого підключені до ЛВС. Дана категорія користувачів потребує використання додаткових заходів забезпечення інформаційної та кібернетичної безпеки (ІКБ) для захисту їхніх робочих місць. Користувачем ІС можуть бути співробітники підрядних організацій на період виконання узгоджених робіт. Доступ таких користувачів до інформаційних ресурсів ЛВС Організації надається в особливому порядку, який повинен узгоджуватися із СлІБ.

Організаційна структура обслуговуючого персоналу. Адміністративно-технічна підтримка ІС Організації здійснюється службами інформаційних технологій відповідних підрозділів. Служби інформаційних технологій в частині впровадження та експлуатації систем ІКБ підпорядковуються керівнику СлІБ і використовують у своїй роботі нормативні документи, розроблені співробітниками СлІБ.

Структура і склад комплексу програмно-технічних засобів. Структура і склад комплексу програмно-технічних засобів включає в себе:

- Локальну обчислювальну мережу (ЛВС) (в складі: сервери, системи зберігання даних, робочі станції, мобільні пристрої, лінії зв'язку та мережеве обладнання).
- Магістральні засоби передачі даних.
- Корпоративну телефонну систему.
- Серверну групу ЛВС Організації складають корпоративні сервери, що працюють під управлінням затверджених до використання ОС (наприклад, Windows Server і Linux). Функціонально вони поділяються на сервери підтримки спеціалізованих додатків, сервери підтримки загальнодоступних сервісів і сервери, що підтримують технологічні служби ЛВС.
- До мережі підключені робочі станції користувачів, що функціонують на базі затверджених до використання клієнтських ОС (Microsoft, Linux, MAC).
- Основу ЛВС Організації складає мережеве обладнання затвердженого до використання Виробника(ів).
- Виділені магістральні канали обміну даними використовуються для забезпечення зовнішніх інформаційних взаємодій ЛВС.
- Схема використання корпоративного каналу - «телефонія + дані». Інформаційна взаємодія по каналу включає - обмін інформацією між бізнес-підрозділами, обмін повідомленнями електронної пошти, IP-телефонію, різні мережеві сервіси та доступ до мережі Інтернет.
- Телефонний зв'язок всередині Організації забезпечується з використанням IP АТС, розміщеної в головному вузлі системи корпоративного зв'язку Організації.

ISSN 2663 - 4023

- Внутрішній телефонний зв'язок здійснюється між бізнес-підрозділами по захищеному VPN каналу.
- Для забезпечення зовнішніх телефонних з'єднань використовується підключення IP АТС до міських ліній.
- Управління даної IP АТС здійснюється централізовано з головного вузла корпоративного зв'язку Організації.

Види інформаційних активів, що зберігаються і обробляються в системі. В ІС Організації зберігаються і обробляються різні види відкритої та конфіденційної інформації (інформація з обмеженим доступом). До конфіденційної інформації, що циркулює в ЛВС, відносяться:

- Персональні дані співробітників Організації і партнерів, збережені в БД і передаються по мережі.
- Електронні листи і інформація БД, що містять службові відомості, інформацію про діяльність Організації і т.п.
- Конструкторська і технологічна документація, перспективні плани розвитку, модернізації виробництва, реалізації продукції та інші відомості, що становлять науково-технічну і технологічну інформацію, пов'язану з діяльністю Організації.
- Фінансова документація, бухгалтерська звітність, аналітичні матеріали досліджень про конкурентів і ефективність роботи на фінансових ринках і інші відомості, що становлять ділову інформацію про внутрішню діяльність Організації.

До строго конфіденційної інформації, яка потенційно може циркулювати в ЛВС, відносяться відомості стратегічного характеру, розголошення яких може привести до зриву виконання функцій Організації, які прямо впливають на її життєдіяльність і розвиток, нанести непоправної шкоди діяльності та престижу, зірвати вирішення стратегічних завдань, порушити виконання затверджених політик і, в кінцевому рахунку, привести до її краху. До категорії відкритої відноситься вся інша інформація, яка не належить до конфіденційної або строго конфіденційної інформації. Для зберігання інформаційних активів в ЛВС використовуються файлові сервери, бази даних і захищені сховища. Вони використовуються для централізованого зберігання інформації про Замовників, Партнерів та іншої виробничої, фінансової та довідкової інформації.

Структура інформаційних потоків. Усередині ЛВС можна виділити наступні інформаційні потоки:

- Передача файлів між файловими серверами і призначеними для користувача робочими станціями.
- Ділове листування.
- Передача юридичної і довідкової інформації між серверами БД і призначеними для користувача робочими станціями.
- Передача звітної інформації.
- Передача повідомлень електронної пошти.
- Передача фінансової інформації між призначеними для користувача робочими станціями і сервером БД в рамках облікових фінансових систем.

Виділяються наступні зовнішні інформаційні потоки:

- Передача звітних документів (виробничі дані) по каналах корпоративної мережі.
- Передача платіжних документів в Банки.
- Передача фінансових і статистичних звітних документів.
- Внутрішньовідомчий і міжвідомчий обмін електронною поштою.

- Передача інформації по комутованих каналах віддаленим користувачам.
- Різні види інформаційних обмінів між ЛВС і мережею Інтернет.

Характеристика каналів взаємодії з іншими системами і точок входу. У центральній ІС Організації використовується два канали взаємодії з зовнішніми мережами:

- Виділена лінія зв'язку з мережею Інтернет Оператора#1.
- Виділена лінія зв'язку з мережею Інтернет Оператора#2.

Для взаємодії бізнес-підрозділів з центральною ІС Організації використовуються виділені канали зв'язку Інтернет. Для передачі інформації між бізнес-підрозділами та головною (центральною) ІС Організації використовуються VPN тунелі. VPN тунелі створюються на базі мережевого устаткування затвердженого до використання Виробника(ів). Захист зовнішніх мереж центральної ІС Організації здійснюється за допомогою МЕ затвердженого Виробника(ів). В даний час для користувачів ЛВС відкритий доступ до Інтернет через проксі-шлюз з використанням URL-фільтрації. Для управління взаємодією бізнес-підрозділів з корпоративною мережею використовується мережеве обладнання затвердженого до використання Виробника(ів). Для управління взаємодією з мережею Інтернет використовуються мережеве обладнання затвердженого до використання Виробника(ів).

ОСНОВНІ ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Побудова архітектури СУІБ Організації має базуватися на дотриманні наступних основних принципів забезпечення ІБ:

- **Простота архітектури.** Мінімізація та спрощення зв'язків між компонентами, уніфікація і спрощення компонентів, використання мінімального числа протоколів мережевої взаємодії. Система повинна містити лише ті компоненти зв'язку, які необхідні для її функціонування (з урахуванням вимог надійності та перспективного розвитку).
- **Апробованість рішень.** Орієнтація на рішення, можливі ризики для яких і заходи протидії цим ризикам пройшли всебічну теоретичну і практичну перевірку.
- **Надійність, готовність і обслуговуванність.** Побудова системи з компонентів, що володіють високою надійністю, готовністю і обслуговуванністю.
- **Керованість.** Можливість збору реєстраційної інформації про всі компоненти і процеси, наявність засобів раннього виявлення порушень інформаційної безпеки, нештатної роботи апаратури, програм і користувачів.
- **Простота експлуатації.** Автоматизація максимального числа дій адміністраторів мережі.
- **Ешелонування оборони.** Для кожного каналу витоку інформації і для кожної загрози безпеки повинно існувати кілька захисних рубежів. Створення захисних рубежів здійснюється з урахуванням того, щоб для їх подолання потенційному зловмисникові були потрібні професійні навички в декількох невзаємопов'язаних областях.
- **Безперервність захисту в просторі і часі.** Неможливість обходу захисних засобів - системи повинні перебувати в захищеному стані протягом усього часу їх функціонування. Відповідно до цього принципу вживаються заходи щодо недопущення переходу систем в незахищений стан.

- **Рівноміцність оборони в усіх напрямках.** Здійснюється регламентація і документування всіх способів доступу до ресурсів корпоративної мережі. Відповідно до цього принципу забороняється створювати несанкціоновані підключення до корпоративної мережі та іншими способами порушувати встановлений порядок надання доступу до інформаційних ресурсів, який визначається регламентуючими документами ІКБ Організації.
- **Проактивний захист.** Заснований на профілактиці порушень безпеки. У більшості випадків для Організації економічно виправданим є вжиття запобіжних заходів щодо недопущення порушень безпеки на відміну від заходів по реагуванню на інциденти, пов'язаних з прийняттям ризиків здійснення загроз інформаційній безпеці. Однак це не виключає необхідності застосування заходів по реагуванню на інциденти і відновленню пошкоджених інформаційних активів. Відповідно до цього принципу повинен проводитися аналіз ризиків, що спирається на модель загроз безпеки і модель порушника, що визначаються справжньою концепцією. Багато ризиків можна зменшити шляхом прийняття превентивних заходів захисту.
- **Мінімізація привілеїв.** Політика безпеки повинна будуватися на основі принципу «все, що не дозволено, заборонено». Права суб'єктів повинні бути мінімально достатніми для виконання ними своїх службових обов'язків.
- **Розподіл обов'язків.** Між адміністраторами корпоративної мережі розподіл обов'язків має визначатися посадовими інструкціями і регламентами адміністрування.
- **Економічна доцільність.** Забезпечення відповідності цінності інформаційних активів Організації і величини можливого збитку (від їх розголошення, втрати, витоку, знищення та спотворення) рівню витрат на забезпечення інформаційної безпеки. Використовувані заходи і засоби забезпечення безпеки інформаційних активів не повинні помітно погіршувати економічні показники роботи автоматизованих систем Організації, в яких ця інформація циркулює.
- **Спадковість і безперервність вдосконалення.** Забезпечення постійного вдосконалення заходів і засобів захисту інформаційних активів та інформаційної інфраструктури на основі наступності організаційних і технічних рішень, кадрового апарату, аналізу функціонування систем захисту з урахуванням змін в методах і засобах перехоплення інформації, нормативних вимог щодо її захисту, досягнутого передового вітчизняного та зарубіжного досвіду в цій галузі.

При виборі програмно-технічних рішень щодо забезпечення ІКБ перевага має надаватись рішенням, що забезпечують дотримання основних принципів ІКБ, а також задовольняють наступним критеріям:

- Підтримка міжнародних, національних, галузевих промислових і інтернет стандартів (перевага віддається міжнародним стандартам).
- Підтримка найбільшою мірою інтеграції з корпоративними програмно-апаратними платформами і використовуваними СЗІ.
- Уніфікація розробників і постачальників використовуваних продуктів.
- Уніфікація засобів і інтерфейсів управління підсистемами ІКБ.
- Мінімізація вартості впровадження та експлуатації.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Сучасні проблеми розвитку кіберпростору та висока ефективність перспективних ІТ технологій підвищує імовірність реалізації сучасних інформаційних і кібернетичних загроз. Кібератаки стають реальним інструментом швидкого досягнення необхідних результатів як в економічній, так і політичній сферах.

Враховуючи те, що інформаційні і кібернетичні атаки з кожним роком удосконалюються, повинна вдосконалюватися і стратегія по їх запобіганню. Очевидно, шо розроблення та дотримування ефективних стратегій для захисту від інформаційних та кібернетичних атак злочинців є напрямом, який дозволить будувати результативні системи протидії на основі використання сучасних технологій та кращих світових практик.

Подальші дослідження варто зосередити на:

- визначенні базових факторів, що впливають на інформаційну та кібернетичну безпеку, а також основних принципів забезпечення інформаційної безпеки при формуванні концепції інформаційної безпеки в умовах гібридних загроз ІАСУ;
- створенні та впровадженні типових політик, процедур та інструкцій щодо захисту інформаційних активів державних і приватних структур;
- побудові та модернізації оптимізованих по ефективності, вартості і функціоналу систем ІТ та ІКБ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] 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

[2] Борсуковська В. Ю., Борсуковський Ю. В. «Безперервність бізнесу: новий тренд або необхідність», Економіка. Менеджмент. Бізнес. - 2017, № 2(20), с. 48-52

[3] 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

[4] Державна служба спеціального зв'язку та захисту інформації. [Електронний ресурс]. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index [Перевірено: 6 грудня 2019]

[5] Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості». [Електронний ресурс]. Режим доступу: http://uas.org.ua/ua/ [Перевірено: 6 грудня 2019]

[6] БУДСТАНДАРТ Online - Сервіс нормативних документів. [Електронний ресурс]. Режим доступу: http://online.budstandart.com/ua/ [Перевірено: 6 грудня 2019]

[7] Міжнародна організація по стандартизації (International Organization for Standardization). [Електронний ресурс]. Режим доступу: https://www.iso.org [Перевірено: 6 грудня 2019]

[8] Міжнародна електротехнічна комісія (International Electrotechnical Commission). [Електронний ресурс]. Режим доступу: https://www.iec.ch/ [Перевірено: 6 грудня 2019]

[9] Борсуковський Ю. В. «Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 1», Кібербезпека, освіта, наука, техніка, - 2019, №1(5), с. 61-72

[10] Threat Landscape Report. [Online]. Available: https://www.fortinet.com [Accessed: 6 December 2019]

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (6), 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 2

Annotation. Current article provides the trends of the hybrid threats landscape for 2020 and further. The key aspects of the implementation of hybrid threats and ways of counteracting them in cyberspace, which are closely related to the constant change of directions of cyber-attacks, improving their efficiency and speed of implementation, the use of artificial intelligence systems to ensure the security of information resources and the creation of adaptive systems of adversity to information and cyber threats , the use of machine learning techniques for a better understanding of the current state of threats, the application of artificial intelligence principles and responsive scenarios for predicting cyberattacks, developing customized action plans that rely on artificial intelligence systems to improve threat detection and response speed, utilize counterintelligence and counter-methods to respond quickly to any spyware before initiating active action, enhancing communication between law enforcement agencies to form a unified approach for interaction between law enforcement agencies at international and local levels, government organizations, the corporate sector and experts in the field of security.

The article defines the necessity for development of experts validated strategies to protect against information and cyber-attacks by criminals. The article describes the object of protection with determination of purpose and basic functions of the system, group of tasks solved in the system, classification of users of the system, organizational structure of service personnel, structure and composition of a complex of software and hardware, types of information assets stored and processed in system, structure of information flows, characteristics of channels of interaction with other systems and entry points.

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

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] 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
[2] Borsukovska V.Y., Borsukovskii Y.V. «Business Continuity: new trend or necessity», Economy. Management. Business. - 2017, № 2(20), c. 48-52
[3] 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
[4] State Service of Special Communication and Information Protection of Ukraine. [Online]. Available: http://www.dsszzi.gov.ua/dsszzi/control/uk/index [Accessed: 6 December 2019]
[5] Ukrainian Research and Training Center of Standardization, Certification and Quality. [Online]. Available: http://uas.org.ua/ua/ [Accessed: 6 December 2019]
[6] Budstandard Online - Document service. [Online]. Available: http://online.budstandart.com/ua/ [Accessed: 6 December 2019]
[7] International Organization for Standardization. [Online]. Available: https://www.iso.org [Accessed: September 25, 2019]
[8] International Electrotechnical Commission. [Online]. Available: https://www.iec.ch/ [Accessed: 6 December 2019]

[9] Borsukovskyi Y.V., «Defining requirements to develop information security concept n hybrid threats conditions. Part 2», Cybersecurity: education, science, technique, - 2019, №1(5), p. 61-72 . . [Online]. Available: https://doi.org/10.28925/2663-4023.2019.5 [Accessed: 6 December 2019].

[10] Threat Landscape Report. [Online]. Available: https://www.fortinet.com [Accessed: 6 December 2019]

This work is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.