МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
«Cybersecurity in Ukraine: Legal and Organizational Issues»

Матеріали
Міжнародної науково-практичної конференції
17 листопада 2023 року

Одеса
ОДУВС
2023

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Всі матеріали надані в авторській редакції та виражають персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 17 листопада 2023 р. Одеса : ОДУВС, 2023. -- - 168 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 17 листопада 2023 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов’язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад’юнктам), здобувачам вищої освіти першого та другого півня освіти.

Як видно з аналізу Стратегії [1], ефективність її реалізації визначатиметься через чітку систему індикаторів стану кібербезпеки, яка буде включати базові індикатори стану кібербезпеки, індикатори розвитку, національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури [1], що дасть змогу комплексно оцінювати результативність та ефективність реалізації Стратегії та прогрес, якого досягли суб'єкти забезпечення кібербезпеки в її виконанні. Упровадження індикаторів стану кібербезпеки забезпечить покращення процесу координації діяльності із забезпечення кібербезпеки, а також моніторингу виконання Стратегії у реальному часі.

Аналіз позитивного зарубіжного досвіду показує, що найбільш ефективним є багаторівневі системи оцінювання ризиків і загроз, коли відповідний аналіз проводиться як на національному , так і на регіональному або місцевому рівні з використанням сучасних веб-ресурсів (онлайн-платформ), що свідчить про прозорість вжитих заходів для суспільства і держави.

Література:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.21 р. №477. URL: https://www.president.gov.ua/documents/4472021-40013
2. Національні системи оцінювання ризиків і загроз: кращі світові практикти,нові можливості для України: аналіт. доп. / Резнікова О.О., Войтовський К.Є., Лепіхов А.В., за заг. ред.. О.О. Резнікової. Київ:НІСД, 2020. 84 с.
3. Про основні засади забезпечення кібербезпеки України: Закон україни від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Про національну безпеку України : Закон України від 21.06.18 р. № 2469- VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
5. Priority assessment of threats and risks: which issues require extra focus. URL: https://english.nctv.nl/topics/national-security-strategy/priority- assessment of threats and risks

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ У КОНТЕКСТІ СУЧАСНИХ ЗАГРОЗ

Балтовський Олексій Анатолійович
доктор технічних наук, доцент
професор кафедри кібербезпеки
та інформаційного забезпечення
Одеський державний університет внутрішніх справ
Кузаков Дмитро Олександрович
слухач 2 курсу магістратури ІПБ
спеціальність 124 «Системний аналіз»
Одеський державний університет внутрішніх справ

Розвиток сучасних інформаційних технологій та загальна комп'ютеризація, а також значне збільшення кількості інформаційно-комунікаційних систем (далі - ІКС), призвели до того, що інформаційна безпека стала не лише обов'язковою їх складовою, але й однією з характеристик інформаційних систем.

Проблеми інформаційної безпеки України в сучасних умовах, принципи забезпечення захисту інформації є надзвичайно актуальними і вимагають поглибленого вивчення. Сьогодні ведеться дискусія щодо цього питання, зокрема щодо оцінки критеріїв інформаційної безпеки, характеристик ймовірних небезпек та їх структури, а також принципів побудови надійної системи захисту національних інтересів саме в інформаційній сфері від зовнішніх та внутрішніх загроз як для самої держави (суспільства), так і для конкретної людини.

Мета захисту інформації в ІКС полягає у запобіганні негативному впливу на інформаційні ресурси з метою збереження конфіденційності, цілісності та доступності. Цей процес включає в себе заходи знищення, викрадення, зниження ефективності функціонування або несанкціонованого доступу до інформації.

Побудова надійного і ефективного захисту інформаційної системи неможлива без

знання можливих загроз безпеці інформаційним ресурсам. Під загрозами безпеці інформаційним ресурсам розуміють дії, які можуть призвести до спотворення, несанкціонованого використання або навіть руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

З урахуванням проведеного аналізу існуючих загроз інформаційним ресурсам, їх можна класифікувати за наступними критеріями:

За інформаційною безпекою (загрози конфіденційності даних і програм, загрози цілісності даних, програм, апаратури, загрози доступності даних, загрози відмови виконання операцій), які впливають на безпеку інформаційних ресурсів та порушують основні властивості інформації, зберіганої і оброблюваної в інформаційній системі, зокрема на її компоненти, такі як інформаційні ресурси, персональні дані, програмні засоби, апаратні засоби, програмно-апаратні засоби.

За способами здійснення (випадкові виходи з ладу апаратних чи програмних засобів, помилкові дії працівників або її користувачів, навмисні помилки в програмному та програмно-апаратному забезпеченні і т. д.; навмисні мають на меті завдання збитків інформаційній системі або користувачам і можуть бути реалізовані шляхом тривалої масованої атаки несанкціонованими запитами або вірусами тощо, їх наслідки призведуть до руйнування (втрати) інформації, модифікації (зміни інформації на помилкову, яка коректна за формою і змістом, але має інший зміст), ознайомлення з нею сторонніх осіб, дії природного і техногенного характеру).

За розташуванням джерела загроз (внутрішні і зовнішні).

Для створення ефективної системи безпеки інформації та розробки та вдосконалення існуючих методів її захисту, важливо враховувати актуальні загрози безпеці, спрямовані проти інформаційних ресурсів у сучасних інформаційно-комунікаційних системах. Ці загрози включають:

Незаконний збір і використання інформації.

Порушення технології обробки інформації.

Впровадження в апаратні та програмні засоби компонентів, які реалізують функції, не передбачені документацією на такі вироби.

Розробка і поширення програм, які порушують нормальне функціонування інформаційних та інформаційно-телекомунікаційних систем, зокрема систем захисту інформації.

Радіоелектронний вплив з метою виведення з ладу, пошкодження або руйнування засобів і систем обробки інформації, телекомунікації.

Вплив на парольно-ключові системи захисту автоматизованих систем обробки та передачі інформації.

Витік інформації технічними каналами.

Впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, зберігання та передачі інформації через засоби зв'язку, а також у службові приміщення органів державної влади, підприємств, установ та організацій усіх форм власності.

Знищення, пошкодження, руйнування або розкрадання машинних та інших носіїв інформації.

Перехоплення інформації в мережах передачі даних та лініях зв'язку, дешифрування цієї інформації та нав'язування помилкової інформації.

Використання незасвідчених вітчизняних та зарубіжних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікаційних засобів при створенні і розвитку інформаційної інфраструктури України.

Несанкціонований доступ до інформації, яка знаходиться в банках і базах даних.

Порушення законних обмежень на поширення інформації.

Для організації ефективного та надійного захисту інформації необхідно керуватися системою принципів, яка дозволяє ефективно організувати роботу з захисту інформаційних ресурсів ІКС. Принципи захисту інформації включають основні ідеї та найважливіші

рекомендації з організації та виконання робіт для ефективного захисту інформаційних ресурсів ІКС і можуть бути розділені на дві основні групи [4, 5].

Література:

1. Денисюк С. В., Сидоренко В.В. Інформаційна безпека в інформаційно-комунікаційних системах: сучасні тенденції та підходи. *Вісник Національного університету «Львівська політехніка». Серія: Інформаційні технології*, 2021, № 187, стор. 17-26.

2. Кириченко О. В. Методи захисту інформації в інформаційно-комунікаційних системах. *Науковий вісник Херсонського державного університету. Серія: Інформатика*, 2022, № 3, стор. 12-17.

3. Олексенко В. М., Смірнова О. В. Технології захисту інформації в інформаційно-комунікаційних системах. *Вісник Національного університету «Львівська політехніка». Серія: Інформаційні технології,* 2023, № 192, стор. 14-22.

4. Сидорчук В. А., Чурило, О. В. Захист інформації в інформаційно-комунікаційних системах на основі штучного інтелекту. *Вісник Національного університету «Львівська політехніка». Серія: Інформаційні технології*, 2021, № 186, стор. 27-34.

5. Шульгів О. В. Захист інформації в інформаційно-комунікаційних системах на основі блокчейну. *Вісник Національного університету «Львівська політехніка». Серія: Інформаційні технології,* 2022, № 189, стор. 19-26.

ДОСЛІДЖЕННЯ ХМАРНИХ ТЕХНОЛОГІЙ ЯК СЕРВІСІВ ДЛЯ РІЗНОМАНІТНИХ СИСТЕМ

Самойлов Станіслав Вадимович
кандидат юридичних наук, начальник 3-го управління інформаційних технологій
та програмування Департаменту кіберполіції НПУ
Кузаков Дмитро Олександрович
студент 2 курсу ОПП «Кримінальний аналіз» відділення підготовки
студентів заочної форми навчання інституту права та безпеки
Одеський державний університет внутрішніх справ

У зв’язку з безперечними перевагами хмарних технологій як зручність, надійність, зберігання даних та інші інфраструктурні ресурси за потребою треба звернуту увагу на збільшення використання різноманітних систем господарства. Паралельно з цим треба аналізувати та поліпшувати безпеку використання хмарних технологій з урахуванням використання їх в різних галузях підприємств.

Хмарні технології - це підхід до обчислення та зберігання даних, коли вони не розміщуються локально на окремому пристрої чи сервері, а замість цього обробляються та зберігаються на віддалених серверах в Інтернеті, що називаються «хмарними серверами». Організації та користувачі можуть отримати доступ до цих ресурсів через інтернет.

Основні аспекти хмарних технологій включають:

1. Зберігання даних. Дані зберігаються на серверах у великих центрах обробки даних замість локальних пристроїв.
2. Обчислення. Віддалені сервери можуть обробляти дані, втратити обчислення та надавати доступ до програм і сервісів.
3. Доступність. Дані можуть бути доступні з будь-якого пристрою, підключеного до інтернету, що дозволяє користувачам працювати з ними з будь-якої точки світу.
4. Масштабованість. Можливість легко розширити обсяги даних чи обчислювальні можливості шляхом зміни підписаного обсягу послуг.
5. Еластичність. Можливість зміни обсягу обчислення або зберігання даних поза межами потреби користувача.
6. Безпека. Загальні хмарні сервіси мають захист даних, включаючи шифрування та інші методи безпеки для захисту користувачів інформації.
7. Спільний доступ. Можливість спільно працювати над даними чи проектами з різних місць [1].