

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський
політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій
«Індустрія 4.0» ім. П.М. Платонова

XXIII Всеукраїнська науково-технічна конференція
молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ
ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції



Одеса

20-21 квітня 2023 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 20-21 квітня 2023 р. - Одеса, Видавництво ОНТУ, 2023 р. – 449 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

Збірник буде корисним як для фахівців і працівників фірм, зайнятих в області ІТ, так і для викладачів, магістрів і студентів вищих навчальних закладів, які навчаються за напрямками і спеціальностями програмного забезпечення, обчислювальної техніки і автоматизованих систем, прикладної математики та обробки інформації, буде корисним професіоналам з комп'ютерного моделювання та розробки комп'ютерних ігор.

Результати досліджень у збірнику представляють собою своєрідний зріз сучасного стану справ в перерахованих галузях знань, який може допомогти як фахівцям, так і студентам університетів скласти загальну картину розвитку інформаційних технологій та пов'язаних з ними питань.

Наукові праці згруповані за напрямками роботи конференції та наведені в алфавітному порядку прізвищ авторів.

Матеріали (тези доповідей) друкуються в авторській редакції. Відповідальність за якість та зміст публікацій несе автор.

Матеріали подано українською та англійською мовами.

Редактор збірника Котлик С.В.

7. Порівняльний аналіз сучасних шляхів діагностики складних технічних виробничих систем. Лактіонов О. (Національний університет «Полтавська політехніка») 93	93
8. Optimization of paths, taking into account the significance of intermediate points. Мазурок І.Є., Веремйов К.В. (Одеський національний університет ім. Мечникова) 95	95
9. Методика навчання фахівців із інформаційної безпеки соціальної інженерії з використанням OSINT і мови SIEVE. Міронов І. В., Болтач С. В. (Одеський національний технологічний університет) 97	97
10. Дослідження факторів впливу на безпеку мобільних застосунків на прикладі клієнтської частини кіберфізичної системи розумної парковки. Павлова О.О., Авсієвич В.Р., Кузьмін А.А. (Хмельницький національний університет) 98	98
11. Парсинг тексту: використання потужностей NLP задля підвищення точності отримуваних даних. Пелович Д. В., Смиш О. Р. (Національний університет «Києво-Могилянська академія») 100	100
12. Захист підприємств від кібератак на корпоративні мережі. Петрук Д. С. (Волинський національний університет імені Лесі Українки) 102	102
13. Використання мобільних застосунків у роботі з документацією ТОВ "Агрона Фрут Україна". Погоріла Ю. В. (Донецький національний університет імені Василя Стуса) 103	103
14. Технологія HDR у моніторах. Романюк О. Н., Захарчук М. Д., Романюк О.В., Коробейнікова Т. І. (Вінницький національний технічний університет, Національний університет «Львівська політехніка») 105	105
15. Проектування інформаційної системи управління сегрегаційним комплексом збору відходів оперативної поліграфії. Сторожук Д.І. (Українська академія друкарства) 107	107
16. Дослідження методів перетворення повідомлень у бортових автомобільних системах. Чайковський О.Р., Селіванова А.В. (Одеський національний технологічний університет) 109	109
17. Процес безпечної передачі інформації у мобільному додатку “Студент ЧДТУ” з Використанням Spring Security на основі JWT. Куницька С.Ю., Архіпов М.О., Чоповенко В.М. (Черкаський державний технологічний університет) 110	110
18. Захист даних та вихідних файлів від несанкціонованого доступу та копіювання комп’ютерних відеоігор. Шаповал В.В. (Київський національний університет імені Тараса Шевченка) 112	112
19. Програмне забезпечення для забезпечення безпеки резервного архівування даних у хмарних системах. Шевчук Р.П., Заріцький О.І. (Західноукраїнський національний університет) 114	114
20. Вплив війни в Україні на кібербезпеку. Шередега Р.О., Бутенко Т.А. (Харківський державний біотехнологічний університет) 116	116
21. Дослідження застосування стандартів PAPERLESS у закладах вищої освіти. Чіклікчі О.С., Лукашенко Д.О., Ольшевська О.В. (Одеський національний технологічний університет) 117	117
22. 3-D візуалізація авторадіограмм радіоактивних частинок. Новіков А.М. (Інститут проблем безпеки атомних електростанцій Національної академії наук України) 119	119
Розділ 3: Нові інформаційні технології в освіті	
1. Development of a methodology for evaluating the efficiency of ship operator model. Nosov P.S., Masonkova M.M., Diahyleva P.S., Solovey O.S. (Херсонська державна морська академія) 121	121
2. Optimization of management processes for maritime transport personnel qualification. Nosov P.S., Ponomaryova V.P., Diahyleva O.S., Ben A.P. (Херсонська державна морська академія) 123	123
3. Using SolidWorks in modern education and science. Rudyk O.Yu., Baranov I.I., Gereta M.M., Dytynyuk V.O., Fedoryshyn S.I. (Хмельницький національний університет) 125	125

ЗАХИСТ ПІДПРИЄМСТВ ВІД КІБЕРАТАК НА КОРПОРАТИВНІ МЕРЕЖІ

ПЕТРУК Д. С. (petrukyana513@gmail.com)

Волинський національний університет імені Лесі Українки

Сучасний світ стає все більш цифровим, а корпоративні мережі стають невід'ємною частиною успішного бізнесу. У зв'язку з цим інформаційна безпека є одним з головних пріоритетів для організацій усіх рівнів. Кібератаки можуть призвести до значних втрат, погіршення репутації та збоїв у роботі корпоративних мереж. Тому актуальність дослідження та розробки шляхів захисту корпоративних мереж від кібератак важко переоцінити.

Метою даної роботи є вивчення сучасних методів захисту корпоративних мереж і розробка нового підходу, який допоможе покращити захист від кібератак.

Завданням дослідження є аналіз сучасних методів захисту, визначення їх переваг і недоліків, розробка нових методів та їх практичне впровадження в мережах підприємств.

Щоб забезпечити ефективний захист корпоративних мереж, необхідно розуміти типи кібератак, з якими може зіткнутися організація. Кібератаки можна класифікувати за кількома критеріями, зокрема: атаки на доступність мережі: атаки DoS (відмова в обслуговуванні) і DDoS (розподілена відмова в обслуговуванні) перешкоджають користувачам отримати доступ до мережі або ресурсів; атаки на конфіденційність даних: віруси, трояни, шпигунські програми, які викрадають або витікають конфіденційну інформацію; атаки на цілісність інформації: програми-вимагачі, пошкодження даних та інші атаки, призначені для знищення або зміни даних без згоди власника. Однак, існує безліч способів захисту корпоративних мереж від кібератак. Ці підходи можна згрупувати за фізичним, логічним і управлінським рівнями:

- Методи захисту фізичного рівня: брандмауери, системи виявлення та запобігання вторгненням (IDS/IPS), моніторинг мережевого трафіку та блокування атак на мережевому рівні.

- Методи захисту логічного рівня: антивірусне програмне забезпечення, методи шифрування для захисту даних від несанкціонованого доступу та зміни.

- Методи захисту на адміністративному рівні: політики безпеки, обмеження доступу, процедури резервного копіювання та відновлення даних, регулярні аудити. [1]

На основі аналізу сучасних підходів до захисту корпоративних мереж пропонується розробка нового підходу, який враховуватиме недоліки існуючих підходів та забезпечуватиме більш ефективний захист від кібератак. Новий підхід має ґрунтуватися на таких фундаментальних принципах: превентивний захист: раннє виявлення можливих загроз і блокування їх на початковому етапі; багаторівневий захист: поєднує фізичні, логічні та адміністративні методи захисту для досягнення максимальної ефективності; адаптивність: здатність нових методів швидко адаптуватися до змін сценарію кібератаки та постійного вдосконалення. [2] Щоб запровадити новий підхід до захисту корпоративних мереж, організаціям необхідно: оновити існуючі системи безпеки, включаючи брандмауери та антивірусні програми, а також розглянути можливість впровадження нових технологій і рішень; впровадити процес моніторингу та аналізу мережевого трафіку для виявлення аномалій і можливих загроз; забезпечити регулярні аудити безпеки та аналіз ефективності нових методів захисту для подальшого вдосконалення; розробити процедури реагування на інциденти, щоб забезпечити швидке й ефективне відновлення мережі та зменшити шкоду від можливих кібератак.

Завдяки дослідженню сучасних методів захисту корпоративних мереж і розробці нових методів на основі аналізу їх сильних і слабких сторін я можу запропонувати більш ефективний спосіб захисту корпоративних мереж від кібератак. Практична реалізація нового підходу з його кількома рівнями захисту, адаптивності, прозорості та контролю дозволяє краще захистити корпоративні мережі від потенційних загроз. Важливо постійно вдосконалювати та оновлювати свої методи захисту, оскільки кіберзлочинці постійно

розвиваються та вдосконалюють свої методи атак. Впровадження нових підходів у поєднанні з регулярним аудитом, навчанням і моніторингом може стати ключовим фактором для підвищення організаційної інформаційної безпеки та забезпечення стійкості корпоративних мереж проти кібератак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Репозитарій Національного Авіаційного Університету: Home. URL: https://er.nau.edu.ua/bitstream/NAU/51948/1/ФККП_2021_123_БасокБО.pdf
2. Шморгун О. М. Методи захисту корпоративних мереж від комп'ютерних атак : Вісник Черкаського університету. Серія: Економічні науки. Випуск 2. Черкаси. 56 с. URL: <https://econom-ejournal.cdu.edu.ua/article/view/2856/2906>

УДК 004.735:621.395.721.5]:658.114.4:338.432

ВИКОРИСТАННЯ МОБІЛЬНИХ ЗАСТОСУНКІВ У РОБОТІ З ДОКУМЕНТАЦІЄЮ ТОВ «АГРАНА ФРУТ УКРАЇНА»

ПОГОРІЛА Ю. В. (yuliya23pogorelaya@gmail.com)
Донецький національний університет імені Василя Стуса

Анотація. У роботі було визначено важливість використання мобільних застосунків для аграрного сектору. Було визначено, що використання застосунків для ТОВ «АгрANA Фрут Україна» допоможе покращити роботу підприємства в цілому.

Ключові слова: мобільні застосунки, аграрний сектор.

Abstract. The paper determined the importance of using mobile applications for the agricultural sector. It was determined that the use of applications for «Agrana Fruit» LLC will help improve the work of the enterprise as a whole.

Keywords: mobile applications, agricultural sector.

Проблематика. Сучасне уявлення про організацію документації на підприємствах аграрного сектору дещо відрізняється від минулого бачення цього процесу. На зміну паперовій документації поступово приходить електронна, яку людина краще сприймає за рахунок машинного набору тексту, яку швидше можна створити та опрацювати та яка має більш мобільний характер, адже полегшує обмін документами всередині підприємства та за його межами. Підприємства будь-якої спеціалізації використовують мобільні застосунки, встановлюють додатки на власні смартфони та відкривають вкладки у браузерях для того, аби проконтролювати робочий процес, сповістити колег про заплановану подію або ж створити документ.

Основним завданням є обрання найбільш ефективних мобільних застосунків, які допоможуть підприємству «АгрANA Фрут Україна» досягнути кращих результатів в роботі з електронними документами.

Виклад основного матеріалу. Українське товариство з обмеженою відповідальністю «АгрANA Фрут» – не виняток. Підприємство активно впроваджує інформаційні технології не лише шляхом автоматизації процесів виробництва соків та консервування фруктових культур, а й за рахунок використання мобільних застосунків.