

**Міністерство освіти і науки України
Херсонська обласна державна адміністрація
Херсонський державний аграрно-економічний університет
Херсонський обласний центр перепідготовки та підвищення кваліфікації
працівників органів державної влади, органів місцевого самоврядування,
державних підприємств, установ і організацій
Навчально-науковий центр «Інститут післядипломної освіти та
дорадництва»
Херсонська державна морська академія
Громадська організація «Глобальний погляд»**

**ЗБІРНИК ТЕЗ
IV Всеукраїнської науково-практичної Інтернет-конференції
«Публічне управління та адміністрування
у процесах економічних реформ»
з дистанційною участю**

Том II



11 листопада 2020 року

м. Херсон

Оргкомітет конференції

Кирилов Юрій Євгенович – доктор економічних наук, професор, ректор Херсонського державного аграрно-економічного університету;

Бутрій Дмитро Степанович – перший заступник голови Херсонської обласної державної адміністрації

Грановська Вікторія Григорівна – доктор економічних наук, доцент, перший проректор, проректор з науково-педагогічної роботи Херсонського державного аграрно-економічного університету;

Аверчев Олександр Володимирович – доктор сільськогосподарських наук, професор, проректор з наукової роботи та міжнародної діяльності Херсонського державного аграрно-економічного університету;

Крикунова Вікторія Миколаївна – кандидат економічних наук, декан економічного факультету Херсонського державного аграрно-економічного університету;

Потравка Лариса Олександрівна – доктор економічних наук, професор, завідувач кафедри публічного управління та адміністрування Херсонського державного аграрно-економічного університету;

Вольська Олена Михайлівна – доктор наук з державного управління, професор кафедри публічного управління та адміністрування Херсонського державного аграрно-економічного університету;

Білорусов Сергій Георгійович – кандидат технічних наук, доцент, заслужений працівник освіти України, директор Херсонського обласного центру перепідготовки та підвищення кваліфікації працівників органів державної влади, органів місцевого самоврядування, державних підприємств, установ і організацій;

Грицук Ігор Валерійович – доктор технічних наук, професор кафедри експлуатації суднових енергетичних установок Херсонської державної морської академії;

Булгаков Микола Петрович – кандидат технічних наук, доцент кафедри експлуатації суднових енергетичних установок Херсонської державної морської академії;

Абсава Людмила Олександрівна – кандидат економічних наук, доцент, голова Громадської організації «Глобальний погляд»;

Карташова Ольга Григорівна – кандидат економічних наук, доцент, доцент кафедри публічного управління та адміністрування Херсонського державного аграрно-економічного університету.

УДК 35: 33.021.8

Публічне управління та адміністрування у процесах економічних реформ: збірник тез доповідей IV Всеукраїнської науково-практичної Інтернет-конференції з дистанційною участю, Том II, 11 листопада 2020 р. – Херсон: ДВНЗ «ХДАУ», 2020. – 79 с.

У матеріалах конференції висвітлені передові науково-практичні результати досліджень, отримані в галузі публічного управління та адміністрування. Для студентів, аспірантів, науковців та фахівців.

© Колектив авторів, 2020

© ДВНЗ «ХДАУ», 2020

МОЛОЧНОЇ ГАЛУЗІ В УКРАЇНІ	51
Мул В.В.,Пічура В.І.	
ДОСЛІДЖЕННЯ АГРОЕКОЛОГІЧНОГО СТАНУ ҐРУНТІВ ХЕРСОСЬКОЇ ОБЛАСТІ ЗА РЕЗУЛЬТАТАМИ ЇХ ЕКОЛОГОАГРОХІМІЧНОГО ОБСТЕЖЕННЯ	54
СЕКЦІЯ «ЕЛЕКТРОННЕ УРЯДУВАННЯ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА»	61
Лобода О. М.	
ЗАХИСТ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ	61
СЕКЦІЯ « СУЧАСНІ КОМУНІКАЦІЇ ТА МОВНА ПОЛІТИКА У ПУБЛІЧНОМУ УПРАВЛІННІ»	64
Володченко В.Г.,Володченко С.В.	
СУЧАСНІ ЗАСОБИ КОМУНІКАЦІЇ В ПУБЛІЧНОМУ УПРАВЛІННІ	64
Панкратьєва Т.Л.	
КОМУНІКАТИВНА КУЛЬТУРА У СФЕРІ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ	67
Рудік Н.М.	
ДЕЦЕНТРАЛІЗАЦІЯ В ЗАБЕЗПЕЧЕННІ РОЗВИТКУ СІЛЬСЬКИХ ТЕРИТОРІЙ ТА КОНКУРЕНТОСПРОМОЖНОСТІ РЕГІОНІВ	70
Відомості про авторів	76

**«ЕЛЕКТРОННЕ УРЯДУВАННЯ В УМОВАХ РОЗВИТКУ
ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА»**

Лобода Олена Миколаївна,

доцент кафедри менеджменту та

інформаційних технологій, к.т.н., доцент

Херсонський державний аграрно-економічний університет

м. Херсон

ЗАХИСТ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ

На сьогоднішній день збільшується кількість нових автоматизованих систем, існуючі мережі розширюються, зростає число користувачів цих мереж і систем. Зростають також і вимоги, пропоновані до переданому трафіку, пропускну здатності, протяжності (масштабності), захисту інформації (передачі даних) та вартості розробки і розгортання автоматизованої системи, причому безпека інформації і вартість автоматизованої системи є одними з головних чинників при її побудові. Справа в тому, що на сьогоднішній день інформація є найціннішим товаром, тобто має ціну, може купуватись і продаватись, загалом представляє інтереси багатьох груп людей, бізнесу, може цікавити конкурентів, опонентів тощо. При володінні певною інформацією та вмілому користуванню нею можна досить сильно впливати на події в сучасному світі. Тому не лише великі корпорації типу Tesla, Microsoft чи Facebook намагаються всіма силами захистити корпоративні мережі, а й звичайні користувачі досить сильно занепокоєні безпекою власних даних.

Міністерство оборони США у книзі «Критерії оцінки безпеки комп'ютерів», [1] (Оранжева книга, 1998р.), визначило сім рівнів безпеки комп'ютерних та мережевих систем. Ця розробка стала загальноприйнятою в

світі для класифікації ступеня захищеності системи. Існують різноманітні методи виявлення атак, але найпопулярнішими та найбільш ефективними є методи аналізу мережної інформації і, зокрема, статистичний метод, який має на увазі, що спочатку для всіх суб'єктів аналізованої системи визначаються профілі. Будь-яке відхилення використовуваного профілю від еталонного вважається несанкціонованою діяльністю та експертні методи (наприклад, застосування штучного інтелекту).

У фінансових установах існує два підходи до захисту інформації: автономний - направлений на захист конкретної ділянки або частини інформаційної системи, яка як правило є найбільш вразливою або може бути джерелом зловживань; комплексний - захищає інформаційну систему в цілому, всі її складові частини, приміщення, персонал тощо. [2]

Найпростіший і надійний спосіб захисту інформації від загроз несанкціонованого доступу (НСД) - режим автономного використання ПК одним користувачем у спеціально виділеному приміщенні при відсутності сторонніх осіб. У цьому випадку роль замкненого контуру захисту виконує виділене приміщення, а фізичний захист – вікна, стіни, підлога, стеля, двері. Якщо стіни, стеля, підлога і двері міцні, підлога не має люків, які з'єднуються з іншими приміщеннями, вікна і двері обладнані охоронною сигналізацією, то стійкість захисту буде визначатись технічними характеристиками охоронної сигналізації при відсутності користувача в неробочий час.

Апаратні засоби захисту - це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку тощо. Засоби захисту портів виконують декілька захисних функцій, а саме:

- «звірка коду». Комп'ютер захисту порту звіряє код санкціонованих користувачів з кодом у запиті;

- «камуфляж». Деякі засоби захисту портів камуфлюють існування портів на лінії телефонного зв'язку шляхом синтезування людського голосу, який відповідає на виклик абонента;

- «дзвінок назустріч». У пам'яті засобу захисту портів зберігаються не тільки коди доступу, але й ідентифікаційні номери телефонів;

- ведення автоматичного «електронного журналу» доступу в комп'ютерну систему з фіксацією основних дій користувача. [3]

Підводячи підсумки, слід підкреслити, що деякі фахівці з банківської безпеки пов'язують надійність фінансових інформаційних систем з засобами їх зовнішнього захисту, тобто системою паролів для входу не тільки у саму комп'ютерну мережу, а й до різних рівнів інформації системи, залежно від допуску користувачів. Коло працівників, які за технологією виконання банківських операцій мають доступ до широкого діапазону такої інформації, дуже великий. Тому система захисту, яка базується на кодуванні входів до різних видів інформації, малоефективна. Потрібно знайти принципово нові підходи для розробки та впровадження відносно надійних систем захисту банківської діяльності від комп'ютерних злочинів. Така система повинна будуватися згідно із технологією банківського документообігу та особливостями форм розрахунково-кредитних операцій.

Література

1. Information Systems Security – Washington: Headquarters Department of the Army, 1998. 49 с. (Army Regulation; вип. 380).

2. Олійник А. В. Інформаційні системи і технології у фінансових установах. Львів: Новий світ- 2000, 2006. 436 с.

3. Войнаренко М. П. інформаційні системи та технології в управлінні організацією [Електронний ресурс]. Едельвейс і К, 2015. Режим доступу до ресурсу: https://pidruchniki.com/74227/informatika/bezpeka_informatsiynih_sistem.