

Державна служба України з надзвичайних ситуацій  
Львівський державний університет безпеки життєдіяльності  
Навчально-науковий інститут цивільного захисту  
Кафедра управління інформаційною безпекою

«Допущено до захисту»  
Начальник кафедри УІБ  
\_\_\_\_\_ Ростислав ТКАЧУК  
“ \_\_\_\_ ” \_\_\_\_\_ 2021 року

## ДИПЛОМНА РОБОТА МАГІСТРА

на тему «Розроблення моделі та методу оцінки надійності персоналу у  
забезпеченні інформаційної безпеки організації»

Виконала:  
студент VI курсу, групи КБ61м  
спеціальності 125 «Кібербезпека»  
(шифр і назва спеціальності)  
\_\_\_\_\_ Христина Явин \_\_\_\_\_  
(прізвище та ініціали)  
Керівник \_\_\_\_\_ Наталія Кухарська \_\_\_\_\_  
(прізвище та ініціали)  
Рецензент \_\_\_\_\_ Іван Дияк \_\_\_\_\_  
(прізвище та ініціали)

Львів – 2021 року

## АНОТАЦІЯ

Явин Х.Р. «Розроблення моделі та методу оцінки надійності персоналу у забезпеченні інформаційної безпеки організації». Дипломна робота магістра за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 4 розділи, 91 с., 10 рис., 65 джерел.

Об'єкт – процес управління персоналом, метою якого є забезпечення інформаційної безпеки організації.

Мета роботи – підвищення рівня інформаційної безпеки організації за рахунок розроблення науково-методичного забезпечення внутрішнього аудиту персоналу.

Основним методом дослідження є математичне моделювання, що базується на використанні апарату математичної статистики, теорії інформаційної безпеки, методів управління персоналом.

На захист виносяться:

- метод багатофакторної оцінки надійності персоналу в забезпеченні інформаційної безпеки організації;
- модель багатофакторної оцінки надійності персоналу в забезпеченні інформаційної безпеки організації;
- рекомендації щодо застосування розроблених методу та моделі забезпечення інформаційної безпеки організації.

Розроблені метод і модель можуть бути застосовані в системі управління інформаційною безпекою організації для оцінки співробітників і визначення тих хто є найбільшою потенційною загрозою інформаційної безпеки організації. Завчасне виявлення таких співробітників дозволить оптимізувати заходи щодо забезпечення інформаційної безпеки. В тому числі, розроблені метод і модель можуть застосовуватися при прийнятті рішення про допуск співробітника до інформації з обмеженим доступом, або при прийнятті рішення про необхідність додаткового спостереження за діяльністю співробітника.

ІНФОРМАЦІЙНА БЕЗПЕКА, ПЕРСОНАЛ, ОЦІНКА НАДІЙНОСТІ  
СПІВРОБІТНИКІВ, МОДЕЛЬ МЕЙЄР-АЛЛЕН.

## ЗМІСТ

ВСТУП.....	7
Розділ 1. РОЛЬ ПЕРСОНАЛУ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ.....	10
1.1. Актуальність протидії інсайдерам в умовах стрімкого розвитку інформаційних технологій.....	10
1.2. Класифікація порушників інформаційної безпеки: інсайдери і їх види.....	17
1.3. Джерела загроз інформаційної безпеки.....	19
1.4. Зв'язок джерел загроз інформаційної безпеки та напрямків роботи з персоналом.....	23
1.5. Зв'язок організаційної прихильності персоналу та інформаційної безпеки організації.....	26
Висновки до розділу.....	31
Розділ 2. ОГЛЯД СУЧАСНИХ МЕТОДІВ МОДЕЛЮВАННЯ І ОЦІНКИ ОРГАНІЗАЦІЙНОЇ ПРИХИЛЬНОСТІ ПЕРСОНАЛУ.....	32
2.1. Поняття організаційної прихильності в роботах зарубіжних авторів.....	32
2.2. Модель організаційної прихильності Мейєр-Аллен.....	34
Висновки до розділу.....	44
Розділ 3. МЕТОД І МОДЕЛЬ ОЦІНКИ НАДІЙНОСТІ ПЕРСОНАЛУ....	45
3.1.                   Метод                   оцінки                   надійності персоналу.....	45
3.2. Побудова моделі оцінки.....	50
3.3. Принципи оцінки факторів.....	54
3.4. Оцінка рівня підготовки співробітника.....	56
3.5. Оцінка організаційної прихильності співробітника на основі об'єктивних факторів .....	57
3.6. Оцінка організаційної прихильності співробітника на основі	65

суб'єктивних факторів .....	
3.7. Оцінка надійності співробітника на основі специфічних факторів.....	68
3.8. Загальна оцінка надійності співробітника.....	73
Висновки до розділу.....	74
Розділ 4. ПЕРЕВІРКА РОЗРОБЛЕНОГО МЕТОДУ І МОДЕЛІ.....	76
4.1. Апробація моделі оцінки організаційної прихильності.....	76
4.2. Рекомендації щодо практичного застосування розроблених методу та моделі.....	80
Висновки до розділу.....	83
ЗАГАЛЬНІ ВИСНОВКИ.....	84
СПИСОК ДЖЕРЕЛ.....	ВИКОРИСТАНИХ 85

## ЗАГАЛЬНІ ВИСНОВКИ

У результаті проведеного дослідження, основною метою якого є підвищення рівня інформаційної безпеки організації за рахунок розробки науково-методичного забезпечення внутрішнього аудиту персоналу, була вирішена нова наукова задача, пов'язана з розробленням методу і моделі оцінки надійності персоналу.

Розглянуто роль персоналу організації в забезпеченні її інформаційної безпеки. Проведено аналіз джерел загроз інформаційної безпеки і визначено роль персоналу в реалізації загроз у залежності від їх джерела. Проаналізовано напрямки оцінювання співробітника з точки зору його надійності. Визначено місце аудиту персоналу в процесі забезпечення інформаційної безпеки організації. Розглянуто історію розвитку методів і моделей оцінки організаційної прихильності персоналу. Вивчено приклади їх адаптації до національних особливостей деяких країн.

Розроблено метод і модель оцінки надійності персоналу в забезпеченні інформаційної безпеки організації. Проведено апробацію розробленої моделі, проведена експертна оцінка розроблених методу та моделі.

Розроблено рекомендації щодо їх застосування та подальшого вдосконалення.

Таким чином, в дипломній роботі вирішена нова наукова задача щодо підвищення рівня інформаційної безпеки організації за рахунок розробки науково-методичного забезпечення внутрішнього аудиту персоналу.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аверченков В.И., Рытов М.Ю. Организационная защита информации. Учебное пособие // Москва.: ФЛИНТА. – 2011. – 184 с.
2. Амелин Р.В. Информационная безопасность. Электронный учебник. [Электронный ресурс] // Учебный центр «Новые технологии в образовании» ММФ СГУ. – URL: [http://nto.immpu.sgu.ru/sites/default/files/3/\\_\\_\\_77037.pdf](http://nto.immpu.sgu.ru/sites/default/files/3/___77037.pdf)
3. Асаул А.Н. Организация предпринимательской деятельности. Учебник СПб.: АНО ИПЭВ. – 2009. – 336 с.
4. Баранская С.С. Методика измерения лояльности [Электронный ресурс] // Психологические исследования: электрон. науч. Журн. – 2011. – N 1(15). – URL: <http://psystudy.ru>
5. Батурина О.В. Лояльность сотрудников: причины и преимущества // Кадровый менеджмент. – 2003.– № 3.
6. Бойдало М.К. Анализ данных нарушения государственных нормативно-правовых актов в сфере защиты государственной тайны. // Научная Перспектива. –2014. – №5(51). – С.28-30.
7. Бойдало М.К. Модель поиска потенциальных инсайдеров посредством оценки активности сотрудников в информационной системе организации. // Научная Перспектива. – 2015. – №5(63). – С.160-162.
8. Бойдало М.К. Политика информационной безопасности в государственных органах и коммерческих организациях США в XXI веке. // Научная Перспектива. – 2013. – №7(41). – С.39–43.
9. Бойдало М.К. Построение модели оценки надежности персонала в интересах информационной безопасности, как модели оценки сложной системы. // «МНИ «Educatio». Ежемесячный научный журнал». – Новосибирск — 2015. – №7(14), Часть 2. – С.11-13.
10. Бойдало М.К. Роль персонала в обеспечении информационной безопасности. // Материалы X Международной научно-практической конференции «Фундаментальные и прикладные исследования в современном мире». – СПб –2015. – С.116-118.

11. Бойдало М.К., Жигулин Г.П. Метод и модель оценки профессионального соответствия персонала в вопросах обеспечения информационной безопасности. // Научно-технический вестник Поволжья. – 2014. – №3. – С.66-71.

12. Бойдало М.К., Жигулин Г.П. Персонал организации как уязвимость в системе информационной безопасности: атаки и противодействие им. // Научно-технический вестник Поволжья. – 2015. – №3. – С.89-91.

13. Бойдало М.К., Жигулин Г.П. Практическая проверка метода и модели оценки профессионального соответствия персонала в вопросах обеспечения информационной безопасности. // Научно-технический вестник Поволжья. – 2015. – №3. – С.86-88.

14. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С.121-124).

15. Власенко М.Н. Лояльность сотрудников безопасность компании. Сайт менеджеров-профессионалов [Электронный ресурс] // М. 2004. – URL: <http://eexecutive.ru/knowledge/announcement/339998>

16. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України. Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів “Проблеми та перспективи розвитку системи безпеки життєдіяльності” (м. Львів, 23-24 березня 2017 р.). [в 2 ч.]. Ч. 2. – Львів: ЛДУ БЖД, 2017. С. 11–12.

17. Войтович В.С., Гриник Р.О. Необхідність створення комплексної системи захисту інформації. Зб. тез доповідей II Міжвузівської науково-практичної конференції студентів і курсантів “Захист інформації в інформаційно-комунікаційних системах” (м. Львів, 24 листопада 2017 р.). Львів: ЛДУ БЖД, 2017. С. 10–11.



18. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція “Інформаційна безпека в сучасному суспільстві” (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24.

19. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности. Учебное пособие // СПб.: ИТМО. – 2009. – 84 с.

20. Германов И.А., Плоникина Е.Б. Измерение организационной лояльности персонала (Опыт апробации методики Мейер-Аллен) // Вестник пермского университета. – 2011. – №3(7). – С.106-111.

21. Дейнека О.С. Экономическая психология: Учеб. Пособие. // СПб: Изд-во С-Петербур. Ун-та.– 2000. — 160 с.

22. Джуэлл Л. Индустриально-организационная психология. Учебник для вузов // СПб.: Питер. – 2001. – 720 с.

23. Довганич М. О. Методи та засоби захисту персонального інформаційного простору в контексті мережевої розвідки / М. О. Довганич, В. І. Ящук // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С. 79-81).

24. Доминяк В. И. Феномен лояльности в разработках зарубежных исследователей. // Персонал-Микс. – 2003. – №1. – С.107-111.

25. Доминяк В.И. Измерение лояльности: действующая модель. // Персонал-Мик. – 2004. – №2. – С. 114-119.

26. Доминяк В.И. Измерение лояльности: действующая модель. // Персонал-Мик. – 2004. – №3. – С. 105-108.

27. Доминяк В.И. Организационная лояльность: основные подходы. // Менеджер по персоналу. – 2006, №4. – С. 34-40.

28. Жигулин Г.П., Бузинов А.С., Шабает Р.И. Моделирование и прогнозирование информационных угроз. // СПб.: СПб ГУ ИТМО.– 2011.

29. Жигулин Г.П., Серебров А.И., Яковлев А.Д. Прогнозирование устойчивости и функционирования объектов с использованием теории игр и исследования операций. // СПб.: СПбГУ ИТМО.– 1994.

30. Злышко О.В. Специфика мотивации персонала в современных условиях // Фундаментальные исследования. – 2009. – №3. – 3 с.

31. Кухарська Н.П., Полотай О.І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13), pp. 126-136.

32. Макринова Е.И., Мухина М.Г. Методика комплексной оценки управленческого персонала в организациях потребительской кооперации // Фундаментальные исследования. – 2012. – №3. – С.696-701.

33. Математическое моделирование информационной и экономической безопасности на предприятиях малого и среднего бизнеса / Иванченко П.Ю., Кацура Д.А., Медведев А.В., Трусков А.Н. – Фундаментальные исследования. – 2013. – №10. – С.2860-2863.

34. Полотай О., Деменко В. Особливості оцінки ризиків загроз інформаційної безпеки. Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. (Київ, 18 березня 2016 року) : у2 ч. Ч. 2. – Київ: Нац. акад. СБУ, 2016. – С. 204-205.

35. Прасолов В.И. Технологии обеспечения лояльности персонала в структуре политики безопасности фирмы. [Электронный ресурс] // Материалы конференции «Создание системы корпоративной безопасности. Практические подходы». (Москва, 15.04.2005) – Москва, 2005. – URL: <http://it2b.ru/blog/arhiv/651.html>

36. Симоненко В.Н. Симоненко Н.Н., Старкова Е.Ю. Организационные меры по совершенствованию мотивации персонала предприятий // Фундаментальные исследования. – 2012. – №11. – С.785-789.

37. Соловейчик А.В. Лояльность персонала и факторы, характеризующие организацию / А. В. Соловейчик // Известия Российского

государственного педагогического университета имени А.И. Герцена. – 2010. – № 125. – С. 93-98.

38. Харский К.В. Благонадежность и лояльность персонала. // СПб.: Питер.– 2003.– 496 с.

39. Чистякова Т. Н., Моисеенко Н. В. О лояльности, организационных конфликтах и развитии организации (заметки на полях исследования). // Новая перспектива. – 2000.

40. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).

41. Abdulkadir Kirmizi dr., Orkun Deniz The organizational commitment of IT professionals in private banks. // European and Mediterranean Conference on Information Systems 2009.

42. Adamek S. Human Resources Information Security Standarts // Wokingham Borough Council. – April 2010. – 10 pages.

43. Affective, continuance, and normative commitment to the organization: A metaanalysis of antecedents, correlates, and consequences. / Meyer, J. P., Stanley D. J., Herscovitch L., Topolnytsky L. – Journal of Vocational Behavior. – 2002. – No61. – P. 20.

44. Best Practices Against Insider Threats in All Nations [Электронный ресурс] / Flynn L., Hurth C., Trzeciak R., Buttles P. – Technical Note CMU/SEI-2013-TN-023: Software Engineering Institute, August 2013, 16 pages. Internet URL:

[http://resources.sei.cmu.edu/asset\\_files/TechnicalNote/2013\\_004\\_001\\_59084.pdf](http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_59084.pdf)

45. Buchanan B. Building organizational commitment: The socialization of managers in work organizations. // Administrative Science Quarterly. – N19. – 1974.– P. 533-546.

46. Capelli D., Moore A., Trzeciak R. The CERT Guide to Insider Threats. // USA.: Pearson Education, Inc. – January 2012. – 389 pages.

47. Common Sense Guide to Mitigation Insider Threats 4th Edition / Silowash G., Cappelli D., Moore A., Trzeciak R., Shimeall T.J., Flynn L. – Technical Report CMU/SEI-2012-TR-012. – Carnegie Mellon University. – December 2012, 121 pages.

48. Fink O. Attack vs. Defense on an Organizational Scale [Электронный ресурс]: SANS Institute Reading Room, November 2007. URL: [http://www.sans.org/reading\\_room/whitepapers/hackers/attack-vs-defenseorganizational-scale\\_2016](http://www.sans.org/reading_room/whitepapers/hackers/attack-vs-defenseorganizational-scale_2016)

49. Human Behavior, Insider Threat, and Awareness: An Empirical Study of Insider Threat Behavior. / Caputo D. D., Stephens G., Stephenson B., Kim M. – Research Report No. 16. – Institute for Information Infrastructure Protection, July 2009. – 5 pages.

50. Insider Attack and Cyber Security. Beyond the Hacker. / Stolfo S.J., Bellovin S.M., Hershkop S, Keromytis A.D. Sinclair S., Smith S.W. – Springer Science + Business Media, LLC. – 2008. – 228 pages.

51. Insider Threats in Cyber Security / Probst S.W., Hunker J., Gollmann D., Bishop M. – Springer Science + Business Media, LLC. – 2010. – 248 pages.

52. Jaros S. Meyer and Allen model of Organizational Commitment: Measurement Issues. // The ICFAI Journal of Organization Behavior. – 2007. – Vol. VI, No. 4. – P. 8-25.

53. Khan R. Practical Approaches to Organizational Information Security Management [Электронный ресурс]: SANS Institute Reading Room, August 10th, 2010. URL: <http://www.sans.org/reading-room/whitepapers/leadership/practical-approachesorganizational-information-security-management-33568>

54. Kipp S. P. Espionage and the Insider [Электронный ресурс] – SANS Institute Reading Room, 2001. URL: [http://www.sans.org/reading\\_room/whitepapers/basics/espionage-insider\\_426](http://www.sans.org/reading_room/whitepapers/basics/espionage-insider_426)

55. Li F. A detailed Analysis of an Advanced Persistent Threat Malware [Электронный ресурс]: SANS Institute Reading Room, October 13, 2011. URL:

<http://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-advancedpersistent-threat-malware-33814>

56. Meyer J.P. Building Commitment in an Era of Change // Rx for HRM.- 2000.

57. Montelibano J., Moore A. Insider Threat Security Reference Architecture // Technical Report CMU/SEI-2012-TR-007. – Software Engineering Institute. – April 2012.

58. Mowday R.T., Porter L.W., Steers R.M. Employee-organization linkages. // New York: Academic Press. – 1982.

59. Okedji A.A. Influence of organizational culture on organizational commitment among workers [Электронный ресурс]: Nnamdi Azikawe University Awka, September 27, 2012. URL: <http://naudigitallibrary.wordpress.com/2012/09/27/influence-of-organizational-cultureon-organizational-commitment-among-workers/>

60. Schmitt N. Uses and Abuses of Coefficient Alpha // Psychological Assessment. – 1996, – Vol. 8, – No 4, – p. 350-353.

61. Sinclair M., Jr. The influence of Trust and Affective Organizational Commitment on Intetnt to Leave // Doctoral Study Submitten in Partial Fullfillment of the Requirements for the Degree of Doctor of Business Administration. – Walden University. – March 2013. – 194 page.

62. Todd M. The insider threat to organizational information security: A structural model and empirical test: A Dissertation of the Requirements for the Degree of Doctor of Philosophy. – Auburn, Alabama, 2007.

63. Warren K.V. Security Controls in Service Management [Электронный ресурс]: SANS Institute Reading Room, December 17, 2010. URL: <http://www.sans.org/reading-room/whitepapers/iso17799/security-controls-servicemanagement-33558>

64. Weiland R.M., Moore A.P., Cappelli D.M., Trzeciak R.F., Spooner D., Spotlight On: Insider Threat from Trusted Business Partners // Carnegie Mellon

University. – 2010, 15 pages. Internet URL:  
[http://resources.sei.cmu.edu/asset\\_files/TechnicalNote/2013\\_004\\_001\\_59084.pdf](http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_59084.pdf)

65. Wright C.S. Rationally opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls [Электронный ресурс]: SANS Institute Reading Room, September 5th, 2011. URL:  
<http://www.sans.org/readingroom/whitepapers/awareness/rationally-opting-insecure-alternative-negativeexternalities-selection-securit-33779>