МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ОНОФРІЙЧУК ОЛЕКСАНДР ЛЕОНІДОВИЧ

УДК 004.632.2/5

Дослідження вразливостей автоматизованого робочого місця касира та передачі даних до Державної фіскальної служби

Спеціальність 125 «Кібербезпека»

Автореферат

дипломної роботи на здобуття освітньо-кваліфікаційного рівня «магістр»

Тернопіль — 2018

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, зав. кафедри кібербезпеки
Загородна Наталія Володимирівна
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: кандидат технічних наук, доцент
Золотий Роман Захарійович
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 26 грудня 2018 р. о 9.00 годині на засіданні екзаменаційної комісії №32 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 806.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. Проблема захищеності інформації що обробляється АРМ особливо актуальна у період комп'ютеризації підприємств. Аналітична обробка економічної інформації дуже трудомістка сама по собі і вимагає великого обсягу різноманітних обчислень. З переходом до ринкових відносин потреба в аналітичній інформації значно збільшується. Це пов'язано перш за все з потребою розробки та обгрунтування перспективних бізнес-планів підприємств, комплексної оцінки ефективності короткострокових і довгострокових управлінських рішень. У зв'язку з цим автоматизація аналітичних розрахунків стала об'єктивною необхідністю. Збільшення АРМ веде за собою збільшення вразливостей їх компонентів, у тому числі банківських терміналів та реєстраторів розрахункових операцій, саме тому їх дослідження є актуальним.

Мета і завдання дослідження. Дослідити вразливості АРМ касира та безпеки передачі даних до Державної фіскальної служби, сформувати загальні рекомендації для розробки КСЗІ підприємства в частині, що стосується функціональних обов'язків касира. Провести пошук вразливостей та запропонувати шляхи їх усунення для ФОП Бойко А.М. Магазин «Смаколик».

Для досягнення поставленої мети, необхідно вирішити наступні задачі:

- Огляд літературних джерел;
- Опис АРМ касира;
- Аналіз існуючих загроз;
- Дослідити безпеку передачі даних від РРО до ДФС;
- Розробити список рекомендацій щодо усунення вразливостей АРМ;
- Розробити список обов'язків персоналу що працює на АРМ.

Об'єктом дослідження є автоматизоване робоче місця продавця-касира.

Предметом вразливості АРМ касира та його компонент (РРО, POS,) та безпека процесу передачі даних до ДФС.

Методи дослідження. методи забезпечення конфіденційності, цілісності, доступності інформації, аутентифікації користувачів.

Нормативно-правовою базою дослідження є Закон України " Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг ".

Наукова новизна роботи полягає у тому, що досліджено вразливості АРМ касира та передачі даних до ДФС на прикладі магазину «Смаколик», сформовано ряд рекомендацій для розробки КСЗІ підприємства в частині, що стосується функціональних обов'язків касира та забезпечення властивостей інформації.

Практичне значення дослідження полягає наданні рекомендацій щодо покращення системи захисту автоматизованого робочого місця.

Апробація результатів дипломної роботи. Основні положення дослідження доповідалися й обговорювалися на науково-практичній конференції: VI Науково-технічна конференція "Інформаційні моделі, системи та технології" (12-13 грудня 2018 року).

Структура роботи. Дипломна робота складається із вступу, семи розділів, висновків, списку використаних джерел із 102 найменувань. Робота містить 22 рисунків, 1 таблицю і 12 формул. Обсяг основного тексту становить 99 сторінок, перелік використаних джерел 2 сторінка, додатки 2 сторінок. Загальний обсяг дипломної роботи складає 127 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність проблеми, визначено об'єкт і предмет дослідження, сформульовано його мету, завдання, розкрито теоретичну та методологічну основу, методи дослідження; висвітлено наукову новизну, практичне значення роботи; подані відомості про апробацію результатів дослідження.

У першому розділі — *"Автоматизоване робоче місце"* — проаналізовано визначення поняття автоматизованого робочого місця, коротко описано історію виникнення поняття. Розгляну три варіанти реалізації автоматизованого робочого місця касира: АРМ що складається з комп'ютера або ноутбука та периферії, АРМ що складається з електронного контрольно-касового апарату та периферії та POS-система. Також описано кільки інноваційних методів реалізації АРМ , таких як: каси самообслуговування та аптечний робот. Розглянуто такі режими роботи АРМ: одиничний, груповий, мережевий.

У другому розділі — " Практична імплементація фіскальної політики в Україні **" —** я описав основну сферу застосування реєстраторів розрахункових операцій, суть фіскальних функцій. Розглянув принципи класифікації реєстраторів розрахункових операцій, дослідив їх компоненти та функції компонентів. Також було описано тестову систему електронного касового апарату E-Receipt, яка в даний час працює в тестовому режимі. Також розглянув нормативно-правові акти що застосовуються до РРО в Україні.

У третьому розділі − "*Вразливості АРМ касира*"− детально описано та проаналізовано процес передачі даних від реєстратора розрахункових операцій до Державної фіскальної служби, розглянуто процес персоналізації та фіскалізації пристроїв, процес формування контрольної стрічки в електронному форматі, обмін інформацією між еквайєром на ДФС. Розглянуто вразливості АРМ, вразливості терміналів безготівкових розрахунків. Досліджено вразливості АРМ на прикладі магазину «Смаколик». Розроблено рекомендації щодо побудови системи захисту АРМ, описано приблизний зміст обов'язків користувача АРМ та відповідальної за роботу АРМ особи. На прикладі реального АРМ досліджено його вразливості, розроблено ряд рекомендацій для КСЗІ, що стосуються інформаційної безпеки та обов'язків персоналу.

У спеціальній частині розглянуто Українські стандарти шифруванн ГОСТ 28147-89 та «Калина».

У розділі «Економічне обгрунтування» описано орієнтованиі витрати для придбання основних компонентів автоматизованого робочого місця касира, розраховано витрати на створення безпечного автоматизованого робочого місця, розраховано (поточні) експлуатаційні витрати, оцінено збитки від атак на вузол або

сегменти АРМ касира, розраховано ефект від реалізаціїсистеми інформаційної безпеки.

У розділі Охорона праці описано правила безпеки поводження на АРМ а також мектоди захисту від іонізуючого випромінення.

У розділі екологія описано вимоги до моніторів та пеом а також гости і стандарти на монітори та ПЕОМ.

У результаті проведених досліджень запропоновано методи уникнення та усунення вразливостей АРМ, Point of sale-терміналів, розроблено перелік рекомендацій які реалізують ці методи. Проведено аналіз АРМ касира на прикладі двох господарських одиниць магазину «Смаколик» (ФОП Бойко А.М.)

ВИСНОВКИ

У результаті виконання дипломної роботи було проаналізовано та досліджено принципи роботи автоматизованого робочого місця касира та реєстратора розрахункових операцій як його складової. Детально описано функції, можливості та режими роботи АРМ. Закріплено теоретичні аспекти автоматизованого робочого місця та РРО. Розгляну кілька варіантів реалізації автоматизованого робочого місця касира. Описано такі режими роботи АРМ: одиночний, груповий та мережевий. Описано метод касового самообслуговування та роботу аптечного робота. Наведено приклад реалізації АРМ з POS-системою, класичним комп'ютером до якого підключено периферійні пристрої так касовим апаратом.

У ході виконання дипломної роботи розглянуто завдання фіскального обліку та реєстраторів розрахункових операцій в цілому. Детально описано класифікацію РРО. Визначено сфери застосування електронних контрольно-касових реєстраторів та електронних контрольно-касових апаратів. Описано переваги і інноваційні рішення ЕККР. Досліджено компоненти та їх функції реєстраторів розрахункових операцій, еволюцію ЕККА, розглянуто систему електронного касового апарату E-Receipt. В даний час система знаходиться на стадії тестування із дуже обмеженими функціями. Проаналізовано нормативно правові акти, закони, та накази, що застосовуються до РРО в Україні згідно з якими визначено вимоги до РРО та їх недоліки.

Результатом дипломної роботи було визначення загроз та вразливостей АРМ та передачі даних до ДФС. Тому детально розглянуто та описано процес передачі даних від РРО до ДФС з сторін відправника та отримувача, описано поняття інформаційного еквайєру, його роль у процесі передачі даних. Розглянуто процеси ініціалізації модуля безпеки РРО, персоналізації. Визначено вразливості автоматизованого робочого місця, детально описано відомі вразливості терміналів безготівкових розрахунків та вразливості їх запам'ятовуючих пристроїв. Визначено та проаналізовано вразливості двох АРМ на прикладі магазину «Смаколик». Описано рекомендації щодо усунення вразливостей, сформовано принципи побудови системи захисту автоматизованого робочого місця, визначено цілі яких необхідно прагнути при цьому. Запропоновано заходи вживання яких забезпечить безпеку інформації від НСД, зменшення кількості помилок персоналу, розроблено ряд організаційних

рішень для ЗІ. Сформовано внутрішні обов’язки обслуговуючого АРМ персоналу та користувачів АРМ.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Онофрійчук О.Л. Аналіз безпечності автоматизованого робочого місця та передачі даних від реєстратора розрахункових операцій до Державної фіскальнї служби/ Тези доповіді на VII Міжнародній науково-технічній конференції молодих учених та студентів “Актуальні задачі сучасних технологій” 28-29 листопада 2018 року. – Том ІІ. – Тернопіль, 2018. – С. 139 ст.
2. Онофрійчук О.Л. Аналіз безпечності автоматизованого робочого місця та передачі даних від реєстратора розрахункових операцій до Державної фіскальнї служби / Тези доповіді VI Науково-технічна конференція "Інформаційні моделі, системи та технології", 12-13 грудня 2018 року. – Том ІІ. – Тернопіль, 2018. – С. ст.

АНОТАЦІЇ

Дослідження вразливостей автоматизованого робочого місця касира та безпеки передачі даних до Державної фіскальної служби // Дипломна робота ОР «Магістр» // Онофрійчук Олександр Леонідович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2018 // С. , рис. – , табл. – , кресл. – , додат. – , бібліогр. – .

Ключові слова: АВТОМАТИЗОВАНЕ РОБОЧЕ МІСЦЕ, ЕЛЕКТРОННИЙ КОНТРОЛЬНО-КАСОВИЙ АПАРАТ, ЕЛЕКТРОННИЙ КОНТРОЛЬНО-КАСОВИЙ РЕЄСТРАТОР, POS-СИСТЕМА, РЕЄСТРАТОР РОЗРАХУНКОВИХ ОПЕРАЦІЙ, ВРАЗЛИВОСТІ, БЕЗПЕКА.

У даній дипломній роботі було досліджено фактори, які впливають на захищеність автоматизованого робочого місця касира, безпеку передачі даних від реєстратора розрахункових операцій до Державної фіскальної служби.

У першому розділі було проведено дослідження діяльності продавця-касира та особливості організації його автоматизованого робочого місця. Запропоновано та розглянуто три методи реалізації автоматизованого робочого місця. Описано режими роботи АРМ.

У другому розділі було проаналізовано роботу реєстраторів розрахункових операцій. Описано практичну імплементацію, класифікацію, а також детально досліджено функції компонентів реєстраторів розрахункових операцій. Крім того розглянуто інноваційний метод електронного касового апарату E-Receipt. Розглянуто

нормативно-правові акти, що регламентують порядок застосування та опломбування реєстраторів розрахункових операцій.

У третьому розділі було проведено аналіз загроз інформаційної безпеки автоматизованого робочого місця, досліджено вразливості POS-терміналів із різним типом пам’яті та описано повний процес передачі даних від реєстратора розрахункових операцій до Державної фіскальної служби. Проведено аналіз інформаційної безпеки двох різних типів реалізації АРМ на прикладі двох господарських одиниць магазину «Смаколик» (ФОП Бойко А.М.). Розроблено ряд рекомендацій щодо усунення вразливостей.

У спеціальній частині розглянуто Українські стандарти шифруванн ГОСТ 28147-89 та «Калина».

У розділі «Економічне обгрунтування» описано орієнтованиі витрати для придбання основних компонентів автоматизованого робочого місця касира, розраховано витрати на створення безпечного автоматизованого робочого місця, розраховано (поточні) експлуатаційні витрати, оцінено збитки від атак на вузол або сегменти АРМ касира, розраховано ефект від реалізаціїсистеми інформаційної безпеки.

У розділі Охорона праці описано правила безпеки поводження на АРМ а такж мектоди захисту від іонізуючого випромінення.

У розділі екологія описано вимоги до моніторів та пеом а також гости і стандарти на монітори та ПЕОМ.

Основною метою даної дипломної роботи є дослідити вразливості АРМ касира та безпеки передачі даних до ДФС, сформувати загальні рекомендації для розробки КСЗІ підприємства в частині, що стосується функціональних обов’язків касира. Провести пошук вразливостей та запропонувати шляхи їх усунення для двох господарських одиниць магазину «Смаколик» (ФОП Бойко А.М.).

Об’єктом дослідження є автоматизоване робоче місце продавця-касира та фактори, які впливають на його захищеність

Предметом дослідження є вразливості АРМ касира та його компонент (РРО, POS,) та безпека процесу передачі даних до ДФС.

У результаті проведених досліджень запропоновано методи уникнення та усунення вразливостей АРМ, Point of sale-терміналів, розроблено перелік рекомендацій які реалізують ці методи. Проведено аналіз АРМ касира на прикладі двох господарських одиниць магазину «Смаколик» (ФОП Бойко А.М.)

In this thesis, the factors influencing the security of the automated workplace of the cashier, the security of data transmission from the settlement operations registrar to the State fiscal service were investigated.

In the first section was conducted research of the seller's work in the automated workplace. Three methods of implementing an automated workplace are proposed and considered. The modes of work of the workstation are described.

The second section analyzed the work of settlement operations registrars. Practical implementation, classification, as well as detailed analysis of the functions of the components of payment transaction loggers are described. Also, an innovative method of

electronic cash register E-Receipt was considered. The normative-legal acts regulating the order of application and sealing of payment transaction loggers are considered.

In the third section - "Vulnerability of workstation of cashier" - detailed description and analysis of the process of data transfer from the settlement operations registrar to the State fiscal service, the process of personalization and device fiscal, the process of forming a control tape in electronic format, and the exchange of information between the acquirer on the State fiscal department is considered. Considered the vulnerability of automated workplace, the vulnerability of non-cash payment terminals. The vulnerability of automated workplacewas studied on the example of the shop "Smakolyk". Recommendations on the construction of the protection system of workstation have been developed, the approximate maintenance content of the user of the workstation and the person responsible for the work of the workstation are described. workstation

In special parts the Ukrainian standards of encryption GOST 28147-89 and "Kalina" are considered.

The "Economic Situation" section describes the estimated costs of acquiring the main components of the automated location, developed costs for creating secure automated sites, calculated for operating costs, estimated from the act on coal or the segments of the automated workplace security.

The Security section describes the security rules that apply to workstation and other media protection.

The "Ecology" section describes the requirements for monitoring and information, as well as standards and standards for monitors and PCs.

The main purpose of this thesis is to: investigate the vulnerability of the workstation of cashier and the security of the data transfer to the State fiscal service; formulate general recommendations for the development of the system of information security of the enterprise in terms of the functional responsibilities of the cashier. Search for vulnerabilities and propose ways to eliminate them for Boiko A.M. The shop "Smakolyk".

The object of the research is the automated workplace of the cashier-seller and factors that influence its security.

The subject of the study is the vulnerability of the ARM cashier and its component (cashregister, POS) and the security of the data transfer process to the State fiscal department.

As a result of the conducted researches, methods of avoiding and eliminating the vulnerabilities of automated workplace, Point of sale-terminals are proposed, and a list of recommendations that implement these methods is developed. An analysis of the cashier's AWM was carried out on the example of two business units of the shop "Smakolyk" (FOP Boiko A.M.)

Keywords: WORKSTATIONS, AN ELECTRONIC CASH REGISTERS, ELECTRONIC CASH REGISTERS RECORDER, POS-SYSTEM COMPONENTS PPO, WORKSTATIONS VULNERABILITY, THE VULNERABILITY OF POS-TERMINALS, WORKSTATIONS DEFENSE, SECURITY OF WORKSTATIONS.