

АНАЛІЗ БЕЗПЕКИ АВТОМАТИЗОВАНОГО РОБОЧОГО МІСЦЯ ТА ПЕРЕДАЧІ ДАНИХ ВІД РЕЄСТРАТОРА РОЗРАХУНКОВИХ ОПЕРАЦІЙ ДО ДЕРЖАВНОЇ ФІСКАЛЬНОЇ СЛУЖБИ

Невід'ємною частиною автоматизованого робочого місця касира є реєстратор розрахункових операцій (РРО). Порядок передачі інформації до органів доходів і зборів по каналах зв'язку встановлюється органами доходів і зборів на базі технології, розробленої Національним банком України та погодженої центральним органом виконавчої влади, що реалізує державну податкову політику. Одним з основних компонентів РРО є модем, призначений для передачі копії сформованих РРО розрахункових документів і фіскальних звітних чеків в електронній формі по каналах зв'язку, до складу якого входить пам'ять для тимчасового зберігання цих копій[1].

При дослідженні безпеки експлуатації автоматизованого робочого місця касира необхідно врахувати наступні загрози: фальсифікація даних клієнта в ПЗ з подальшим їх використанням; проникнення шкідливого коду; цілеспрямовані хакерські атаки і, як наслідок, отримання несанкціонованого доступу до даних; будь-які дії, що призводять до викрадення, спотворення, зміни або знищення інформації в інформаційній системі та вразливості оточення. Під вразливістю оточення маємо на увазі інфраструктурні діри, пов'язані з організацією віддаленого доступу до інформації, помилками конфігурації мережевого обладнання, механізмами встановлення оновлень прикладного і системного програмного забезпечення, організаційні аспекти доступу до обслуговування і технічної підтримки POS-терміналів. Останній пункт потребує особливої уваги оскільки, торгові точки які не мають достатньо ресурсів для самостійного обслуговування POS-терміналів наймають стороннього підрядника. Це дає можливість недобросовісним підрядникам підключати мережеві вузли, які мають безпосередній доступ та з'єднання POS-терміналів до Інтернет, що дає зловмиснику поле для злодіянь. Багато POS-терміналів використовують статичну RAM для зберігання інформації про кредитні картки. Після переповнення RAM записи перезаписуються новими даними, та, як показує практика, відключення живлення (різке чи штатне) не дозволяє очистити пам'ять від надлишкових даних. Деякі моделі POS-терміналів використовують спеціальні комбінації кодів що дозволяють переглянути історію транзакцій, чим часто користуються зловмисники. POS-термінали, що використовують Compact Flash (CF) надають досить гнучкий механізм створення резервних копій і відновлення даних через окремий ПК.

Вище наведені факти підтверджують актуальність обраної теми досліджень у зв'язку з необхідністю удосконалення систем автоматизації управління підприємствами.

Література

1. Закон України «Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг» №265/95-ВР редакція від 19.07.2017 [Електронний ресурс] <http://zakon.rada.gov.ua/laws/show/64/95-вр>.