

Стоянова-Коваль С. С.

*д.е.н., професор,
викладач кафедри забезпечення військ (сил),
Військова академія м. Одеса*

Космін А.О.

*ОПП «Речове забезпечення військ (сил)» 4 курс бакалаврат,
Військова академія м. Одеса*

ОРГАНІЗАЦІЯ СИСТЕМИ ВНУТРІШНЬОГО КОНТРОЛЮ ТА УПРАВЛІННЯ РИЗИКАМИ РЕЧОВИХ СЛУЖБ ЗСУ

В умовах російської агресії проти України, коли збройні сили мужньо відстоюють кордони держави, питання їх своєчасного забезпечення, у тому числі і речового, мають нагальне значення. З початком широкомасштабного вторгнення і від так, різким збільшенням особового складу, виникла нагальна потреба у забезпеченні великої кількості новоприбулих воїнів спеціальним одягом, білизною, взуттям, спорядженням, касками та іншими засобами, необхідними для належного виконання службових обов'язків. Такі потреби закривалися як за рахунок держави так і за рахунок волонтерських зборів. Зазначимо, що своєчасне і повне забезпечення особового складу усім необхідним пов'язане не тільки зі значними фінансуванням, а й з ризиками щодо збереження і ефективного використання такого майна. В таких умовах питанням організації внутрішнього контролю та управління ризиками приділяється велика увага.

Внутрішній контроль є одним з найважливіших аспектів управління у будь-якій компанії, як приватній так і бюджетній. Так як він об'єктивно оцінює ефективність та результативність діяльності, законність та обґрунтованість господарських операцій, достовірність звітності і забезпечує виявлення та усунення відхилень у системі бухгалтерського обліку.

Загальні прийоми внутрішнього контролю використовуються як в цивільній сфері діяльності, так і у військовій сфері, це незамінна частина єдиного механізму управління. Розглянемо особливості внутрішнього контролю та управління ризиками на прикладі речової служби військової частини.

Внутрішній контроль – це комплекс заходів, які застосовує начальник речової служби для забезпечення законного та ефективного використання бюджетних коштів, досягнення результатів відповідно до встановленої мети, завдань, планів і вимог щодо діяльності речової служби [1].

Найбільшої ефективності внутрішній контроль може досягти за умови системного підходу. Так, під системою внутрішнього контролю речової служби розуміється комплекс заходів, що направлений на виконання завдань, що поставлені перед службою і виконуються організовано та ефективно щодо забезпечення збереження майна та ресурсів, виявлення, виправлення та запобігання помилкам і викривленням інформації стосовно речової служби, підготовка і подання достовірних звітів, включаючи фінансову та бухгалтерську звітність служби. Важливим показником ефективності внутрішнього контролю у військових частинах є ступінь досягнення цілей (визначених можливостей) при

оптимізації внутрішнього контролю. Ключовим показником ефективності системи управління ризиками є ступінь перевищення результатів контрольних процедур і заходів з управління ризиками над витратами на них [2].

Начальник речової служби організовує свою роботу щодо внутрішнього контролю підпорядкованого йому особового складу та здійснення господарських операцій речової служби згідно з Положенням про внутрішній контроль військової частини (далі Положення), що затверджене наказом командира. Дане Положення визначає: порядок здійснення внутрішнього контролю; опис всіх елементів контролю, з урахуванням специфіки речової служби військової частини; посадових осіб відповідальних за здійснення заходів внутрішнього контролю у речовій службі військової частини; інформацію про можливі ризики та план управління ризиками на відповідний рік, а також порядок проведення моніторингу внутрішнього контролю за речовою службою.

Головною метою організації внутрішнього контролю є робота з управління ризиками. Управління ризиками – це діяльність суб'єкта внутрішнього контролю з метою виявлення на якомога більш ранній стадії потенційних порушень, недоліків і неефективного використання ресурсів при виконанні своїх функціональних обов'язків і процесів по речовій службі.

Управління ризиками діяльності речової служби починається з ідентифікації ризиків з метою визначення найбільш ризикованих форм поведінки (подій), які можуть перешкодити досягненню законності та ефективності; зосередження наявних ресурсів на зменшенні найбільш значущих ризиків; визначення відповідальних осіб з особового складу, що виконують процеси або операції, пов'язані з ризиком. Наприклад, несвоєчасне внутрішнє інформування речової служби призводить до виникнення ризиків несвоєчасних розрахунків, або навпаки - до зайвих втрат ресурсів речового майна [3].

Важливою ланкою в управлінні ризиками є інформування і комунікація, що передбачає збір, документування, аналіз, передачу та використання інформації вищим керівництвом для належного виконання та оцінки функцій та завдань. Зазначимо, що ручне (паперове) ведення бухгалтерського та оперативного обліку військового майна на всіх рівнях управління, створює ризики неналежного інформування та комунікації, що, в свою чергу, може призвести до викривлення інформації про фінансово-майновий стан як військових частин, так і органів управління, отож цифровізація і перехід на автоматизований облік має велике значення для поліпшення роботи речової служби.

Наразі, впровадження внутрішнього контролю має забезпечити ефективне та раціональне використання ресурсів. Заходи контролю мають реалізовуватися керівниками та офіцерами на всіх рівнях управління зберігаючи принцип, що вигоди від внутрішнього контролю повинні бути співмірними витратам на його розробку та впровадження, включаючи витрати на додаткові заходи контролю для зменшення ризиків.

Список використаних джерел:

1. Про затвердження Порядку організації в системі Міністерства оборони України та Збройних Сил України внутрішнього контролю та управління ризиками: наказ М –ва оборони України від 02 квіт. 2019 р. № 145
2. Методичний посібник Організація внутрішнього контролю та управління ризиками. К. Кустріч, С.Бреус та інш. 2021 с.275 URL: [https://www.mil.gov.ua/content/pdf/vnytr_control/Dod2_TKP_8-00\(199\)01.02.pdf](https://www.mil.gov.ua/content/pdf/vnytr_control/Dod2_TKP_8-00(199)01.02.pdf)
3. Перелік типових ризиків в системі організації внутрішнього контролю військової частини: методич. посіб. В. А. Тіора та ін. Житомир, 2021. 50 с.

Тарасенко В.В.

ОПП «Банківський бізнес», 4 курс бакалаврат

Київський національний економічний університет імені Вадима Гетьмана

Науковий керівник – к.е.н., доцент,

професор кафедри банківської справи та страхування

Білошапка В.С.

СЦЕНАРІЙ ПЛАТІЖНОГО ШАХРАЙСТВА ТА ПРОТИДІЯ ЙОМУ ЯК ЕЛЕМЕНТ ФІНАНСОВОЇ БЕЗПЕКИ БАНКІВ

Шахрайство пов'язане з платежами дуже поширене явище не тільки в Україні, а й в усьому світі. Воно може вирізнятись за схемами, мотивами, масштабами та наслідками, але найбільше це торкається банківської системи. Фінансова безпека банку залежить від того, чи зможе він вчасно виявити шахрайські дії та протидіяти їм. В іншому випадку банки наражають себе на небезпеку та втрату довіри зі сторони клієнтів.

З початком повномасштабного вторгнення в Україну питання фінансового шахрайства почало набирати все більших обертів. Так, за даними НБУ кількість незаконних дій з платіжними картками у 2023 році зросла на 25%, і спричинило збитки за 272 тисячам операцій, що становить приблизно 833 млн гривень, тобто це на 73% більше порівняно з минулим роком. В середньому незаконні операції зросли на 39% від початку війни, і на 91,5% порівнюючи з 2021 роком (рис.1).

Слід зазначити, що з лютого 2022 року банківська система стикається з періодичними DDoS-атаками зі сторони РФ, де особливе напруження припадає на періоди підвищеного онлайн-трафіку. Паралельно із цим відбуваються фішингові атаки, спроби несанкціонованого доступу, хакерські атаки на платіжні системи, а також різні способи платіжного шахрайства. Найпоширенішими сценаріями, що привели до великих фінансових втрат стали: 1) фішингові SMS-повідомлення про державну допомогу, де клієнти перейшовши за фейковим посиланням вводили свої конфіденційні дані, і тим самим дозволяли шахраям привласнити кошти; 2) дублювання електронних або фізичних SIM-карт для отримання доступу до номера телефону, що прив'язаний до різних застосунків: починаючи від мобільного банкінгу, і закінчуючи спробами оформлення онлайн-