УДК 004.056:336.71

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКИХ УСТАНОВАХ

Брайко В.С., Мартинчук О.О.
e-mail: vladyslav.braiko@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна

The study examines comprehensive approaches to information security in banking institutions. The proposed model integrates physical, technical, and administrative protection methods, providing a multi-level security system adaptable to emerging threats. The research analyzes the economic efficiency of implementing advanced security solutions, including Next-Generation Firewalls, SIEM systems, and behavior analytics tools. The developed implementation plan enables banking institutions to systematically enhance their security posture while meeting regulatory requirements. Results demonstrate the importance of proactive security measures and continuous monitoring to reduce cyber incidents and financial losses in the banking sector.

Сучасна банківська сфера стикається з постійно зростаючими кіберзагрозами, що потребує впровадження ефективних методів захисту інформації. У цій статті розглядається комплексний підхід до забезпечення інформаційної безпеки банківських установ з урахуванням актуальних викликів. Визначається важливість відповідності нормативним вимогам НБУ, GDPR та міжнародним стандартам (ISO 27001, PCI DSS). Аналізуються наслідки недотримання вимог безпеки, що включають фінансові штрафи, репутаційні втрати та можливе зменшення клієнтської бази.

Захист інформації в банківських установах є критичним завданням для забезпечення стабільності фінансової системи та збереження конфіденційності даних клієнтів. Статистика атак на українські банки за останні 5 років демонструє значне зростання як кількості інцидентів, так і фінансових збитків. Особливу загрозу становлять віруси-шифрувальники типу Petya/NotPetya, що здатні паралізувати роботу банківської інфраструктури. Вразливими місцями часто виступають застаріле програмне забезпечення, людський фактор та недостатня фізична безпека, що підкреслює необхідність комплексного підходу до захисту інформації.

У сучасних умовах системи захисту інформації в банках повинні базуватися на поєднанні різних методів. Основні підходи включають фізичний захист (контроль доступу, захист периметру), технічний захист (мережева безпека, антивірусне програмне забезпечення, шифрування даних, безпека веб-додатків) та адміністративний захист (політики безпеки, навчання персоналу, управління ризиками) [1]. Однак ефективність захисту залежить від правильної інтеграції цих компонентів в єдину систему.

Запропонована модель базується на багаторівневому підході до захисту з акцентом на проактивність, безперервний моніторинг та адаптивність [2]. Технічні компоненти моделі включають Next-Generation Firewall (NGFW), Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), Threat Intelligence та Data Loss Prevention (DLP). Адміністративні заходи передбачають розробку детальних політик безпеки, навчання персоналу, впровадження системи управління ризиками, проведення регулярних аудитів безпеки та співпрацю з правоохоронними органами.

Впровадження розробленої моделі потребує економічного обґрунтування, що включає аналіз витрат на обладнання, програмне забезпечення та навчання персоналу, а також оцінку потенційних збитків від інцидентів. Розрахунок Return on Investment (ROI) демонструє економічну доцільність впровадження запропонованих заходів захисту з точки зору співвідношення витрат та вигод.

Реалізація моделі передбачає п’ять етапів: проведення аудиту безпеки та оцінки ризиків; розробку та затвердження політик безпеки; впровадження технічних рішень; навчання персоналу; тестування та моніторинг системи; Такий поетапний підхід забезпечує систематичне підвищення рівня захисту інформації в банківській установі.

Висновки. Запропонована модель забезпечує комплексний та ефективний захист інформації в банківській установі. Впровадження моделі сприятиме зниженню ризиків кіберзагроз та підвищенню фінансової стабільності банку. Перспективи подальших досліджень включають автоматизацію процесів захисту, використання штучного інтелекту для виявлення аномалій, розробку адаптивних систем захисту, що самонавчаються, та дослідження нових видів кіберзагроз та методів протидії.

Список використаних джерел:

1. Усік П. С.,Буравченко К.О. Безпека банківських систем : навч. посіб. Кропивницький, 2022. 194 с.

2. Мартинчук О.О. Мельник П.О., Дубовик Н.А. Проактивні методи захисту банківських систем від кіберзагроз // Матеріали четвертої Міжнародної науково-практичної конференції «Інформаційна безпека та захист даних». Харків, ХНУРЕ, 2023, с. 112-118.