

Сергій С. Вітвіцький, Олександр Н. Куракін, Павло С. Покатаєв, Олексій М. Скрябін, Дмитро Б. Санакоєв

Особливості розслідування кіберзлочинів у банківському секторі України: загальний огляд та аналіз

Стрімке зростання рівня кіберзлочинності в банківському секторі вимагає створення ефективної системи запобігання таким злочинам та забезпечення кібербезпеки держави. Постійне оновлення засобів і методів скоєння кіберзлочинів потребує визначення ефективних заходів боротьби з ними. У статті, з метою вивчення теоретичного досвіду та практичних заходів із запобігання кіберзлочинності в банківському секторі та виявлення ефективних способів боротьби зі злочинністю у віртуальному просторі України, використано метод опитування. Проаналізовано досвід провідних країн світу щодо запобігання кіберзлочинності, розглянуто заходи з підвищення рівня кібербезпеки національного та міжнародного кіберпростору. Зроблено висновок, що рівень кібербезпеки в Україні не відповідає сучасним вимогам і потребує ефективних заходів та скоординованої співпраці приватного й державного секторів з метою ефективної боротьби з кіберзлочинністю, зокрема: закріплення класифікації кіберзлочинів в нормативно-правових актах України; запровадження поняття «банківське кримінальне право» в науково-правовій сфері; створення українських кіберсил, діяльність яких буде спрямована на попередження та протидію злочинам, скоєним у кіберпросторі.

Ключові слова: кіберзлочин, розслідування, електронний банкінг, порушення, «кібервійська»

Класифікація JEL: K14, K24, E58



Стаття знаходиться у відкритому доступі і може розповсюджуватися на умовах ліцензії [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license, що дозволяє необмежене повторне використання, розповсюдження та відтворення на будь-якому носії за умови наявності відповідного посилання на оригінальну версію статті.