

Чернадчук Тамара Олександрівна к.ю.н., доцент
Сумський національний аграрний університет, Україна

ПРОБЛЕМНІ ПИТАННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПЛАТІЖНИХ СИСТЕМ

В сучасних умовах особливу актуальність набувають питання організації грошових розрахунків, що обумовлено значною роллю грошового обігу в забезпеченні розвитку економіки держави. Провідна роль в процесі здійснення суб'єктами переказу коштів і розрахунків відводиться платіжним системам та системам розрахунків, так як саме надійні й ефективні платіжні системи забезпечують розрахунки за зобов'язаннями і є запорукою стабільного функціонування фінансової системи та економіки країни загалом.

Враховуючи те, що електронні документи на переказ, розрахункові документи та документи за операціями із застосуванням електронних платіжних засобів можуть містити інформацію, що є банківською таємницею або є інформацією з обмеженим доступом, яка в свою чергу, під час їх передавання засобами телекомунікаційного зв'язку потребує відповідного захисту від несанкціонованого доступу (доступу до інформації осіб, які не мають на це прав або повноважень); несанкціонованих змін інформації (внесення змін або часткового чи повного знищення інформації особами, які не мають на це права або повноважень); несанкціонованих операцій з компонентами платіжних систем (використання або внесення змін до компонентів платіжної системи протягом її функціонування особами, які не мають на це права або повноважень), актуального значення набувають питання захисту інформації при проведенні переказу. Система такого захисту повинна забезпечувати безперервний захист інформації щодо переказу коштів на усіх етапах її формування, обробки, передачі та зберігання.

На нашу думку, основними напрямками діяльності банківських підрозділів щодо захисту інформації (інформаційної безпеки) є розробка основних

напрямів використання технічних та програмних засобів та способів захисту електронної банківської інформації; аналіз та організація діяльності щодо виявлення можливих каналів витoku банківської інформації за допомогою технічних засобів захисту. Заходи щодо забезпечення інформаційної безпеки банку мають бути систематичними і здійснюватися у комплексі із іншими заходами. Важливого значення для забезпечення інформаційної безпеки банківської діяльності має законодавчий рівень такого забезпечення. При розробці системи забезпечення інформаційної безпеки банку особливу увагу потрібно приділяти оцінці відповідності управлінських рішень, технологій, підходів та конкретних програмно-апаратних засобів вимогам чинного законодавства.

Адміністративний рівень інформаційної безпеки реалізується у формі прийнятої політики безпеки, що містить основні принципи та правила, дотримання яких забезпечить цілісність та конфіденційність банківської інформації. Такі принципи та правила політики безпеки містяться у спеціальному документі та відповідних організаційно-розпорядчих документах, які стосуються усіх сфер банківської діяльності і є комплексом управлінських рішень та інструкцій щодо регламентації дій як в звичайному режимі банківської діяльності, так і в екстремальних випадках.

Отже, з метою запобігання порушенням інформаційної безпеки інформаційних банківських ресурсів потрібно виявляти та аналізувати вразливі місця інформаційної системи банку та ресурси, які потребують захисту, а також ймовірні атаки, які можуть відбутися в конкретному оточенні. Після цього потрібно визначити інформаційні ризики для визначеного інформаційного ресурсу та обрати контрзаходи, згідно обраної політики банківської безпеки та забезпечити за допомогою механізмів і сервісів безпеки. В свою чергу, політика інформаційної безпеки платіжних систем має визначати взаємопов'язану сукупність механізмів і сервісів безпеки, адекватну ресурсам, що захищаються, і оточенню, в якому їх використовують.