Секція: Фінанси, гроші і кредит, страхування і біржова справа

СТЕЦЬ МАКСІМ СЕРГІЙОВИЧ

Студент ДВНЗ

«Олександрійського політехнічного коледжу»

м. Олександрія, Україна

Науковий керівник та співавтор:

Дмитрієва Ю.С.

Викладач першої категорії

юридичних дисциплін ДВНЗ

«Олександрійського політехнічного коледжу»

м. Олександрія, Україна

ПЕРСПЕКТИВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКОГО СЕКТОРУ В УКРАЇНІ

Мета дослідження. Метою мого дослідження є аналіз стану засад інформаційної безпеки банківських установ, джерел основних загроз банківського сектору. Визначення основних шляхів політики управління інформаційною безпекою в Україні з метою досягнення максимальної якості та дієвості банківської системи.

Актуальність. Питання інформаційної безпеки в Україні є органічною складовою національної, тому її поглиблений аналіз формує базові знання та уявлення про національну безпеку, однією з складових якої - є забезпечення конфіденційності інформації різного рівня, яка обробляється в системі банківських установ. Вважаю, що поглибленого аналізу заслуговують наступні чинники, які впливають на розуміння стану та перспектив інформаційної безпеки банківських установ, а саме це: потужні кроки розвитку інформаційних технологій; всеохоплююча глобалізація інформаційного середовища; значення інформації у сучасному світі, як основного атрибуту, від якого в перспективі залежить

загальна ефективність сучасної діяльності Банківської системи та життєдіяльності суспільства загалом; принциповість інформаційних технологій щодо змінення обсягів і важливості інформації, яка обертається в різноманітних технічних засобах її збереження, обробки та передачі; загальна комп'ютеризація основних сфер діяльності, що в свою чергу призводить до появи широкого спектру внутрішніх і зовнішніх загроз, різноманітних нетрадиційних каналів втрати інформації і несанкціонованого доступу до неї.

Слід зазначити, що дана тема хоч і є актуальною, але юристами – науковцями досліджується мало. Мною проаналізовані роботи вітчизняних фахівців, які досліджували окремі аспекти проблеми, доцільно виокремити праці: В.А. Ліпкан, Ю.Є. Максименко, В.М.Желіховський, О.І. Косілова, Микола Дмитренко, Я. Малик.

Основні результати дослідження. Під засадами інформаційної безпеки банківських установ потрібно розуміти нормативно-правове регулювання захисту всіх інформаційних ресурсів банківських установ, що регулюються нормами Закону України «Про банки і банківську діяльність», Законом України «Про інформацію» та Законом України «Про електронну комерцію».

Слід зазначити окремо, про стратегію розвитку інформаційного суспільства в Україні від 2013 року відповідно до якої вважаю за потрібне виділити пріоритети діяльності в галузі забезпечення інформаційної безпеки, що спрямовані на:

1) створенню захищених інформаційно-телекомунікаційних систем, запровадження сучасних захищених інформаційних технологій в інтересах державного управління;

2) створення ефективної системи виявлення та запобігання загрозам державних електронних інформаційних ресурсів, у тому числі щодо протидії розповсюдженню комп'ютерних вірусів, програмних і

апаратних закладок, а також витоку інформації технічними каналами та за рахунок несанкціонованих дій;

3) забезпечення цілісності, доступності та конфіденційності інформаційних ресурсів України, які створюють умови для розвитку особи, стійкого функціонування суспільства і держави, захисту персональних даних та інформації, що перебуває у володінні фізичних, юридичних осіб та держави, від зовнішніх і внутрішніх інформаційних загроз, зокрема шляхом протидії комп'ютерним злочинам;

4) забезпечення безпеки інформаційно-телекомунікаційних систем органів державної влади та органів місцевого самоврядування, інформаційно-телекомунікаційних систем, які функціонують в інтересах управління державою, задовольняють потреби оборони та безпеки держави, кредитно-банківських та інших сфер національної економіки, систем управління об'єктами критичної інфраструктури;

5) удосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема кібернетичної безпеки національної критичної інфраструктури;

6) впровадження захищеного механізму ідентифікації учасників електронної взаємодії;

7) формування системи моніторингу безпеки інформаційних ресурсів та систем.

8) розвитку інформаційного суспільства в Україні.[1]

Потрібно зазначити, що в питаннях інформаційної безпеки банківських установ важливе місце займають і нормативні акти НБУ з питань організації і управління інформаційною безпекою.

Так, станом на 2017 рік Національним банком України затверджений План підготовки проектів регуляторних актів, які розподілені за періодичністю виконання до кінця 2017 року. Вважаю, що запланована і виконана робота першого кварталу щодо урегулювання порядку погодження засобів криптографічного захисту інформації для

використання в НБУ та банківській системі України, суттєво і перспективно підсилило роботу банківського сектору взагалі.

Крім цього пропоную звернути увагу, що політика інформаційної безпеки банків – це внутрішній нормативний документ, який описує та регламентує систему управління інформаційною безпекою банку. Політика складається у відповідності до вимог законодавства України та рекомендацій стандартів НБУ. Тому наступним кроком у другому кварталі 2017 року Національним банком України заплановане затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» основною метою цільового прийняття якої є: урахування вимог та рекомендацій національних стандартів із питань інформаційної безпеки ДСТУ ISO/ 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)" та ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT», що вступають у дію з 01.01.2017, врегулювання порядку укладання та ведення договорів із питань забезпечення засобами захисту інформації Національного банку банківських та інших установ, які є безпосередніми учасниками системи електронних платежів та інформаційних задач Національного банку України, удосконалення порядку взаємодії цих установ із Національним банком України під час забезпечення засобами захисту інформації, впровадження нової апаратури захисту, що базується на апаратній платформі, для вдосконалення підходів до перевірок стану інформаційної безпеки організацій. [2, с.1-2].

Також перспективним вважаю заплановану регуляторну політику НБУ до кінця року, щодо: удосконалення порядку відкриття та використання рахунків клієнтів банків; удосконалення порядку електронного документообігу при здійсненні документарних операцій та

операцій з електронними грошима; удосконалення порядку ведення Реєстру аудиторських фірм, які мають право на проведення аудиторських перевірок банків, уточнення переліку документів, що подаються аудиторською фірмою для включення до Реєстру, та порядку прийняття рішень із питань ведення Реєстру; удосконалення та приведення у відповідність до вимог нормативно-правових актів, приміщень небанківських фінансових установ в Україні; приведення нормативно-правових актів НБУ у відповідність до поточних соціально-економічних умов та міжнародних зобов'язань України; Удосконалення питань, пов'язаних із порядком проведення перевірок юридичних осіб, які отримали ліцензію НБУ на надання банкам послуг з інкасації, з питань організації та здійснення інкасацій коштів та перевезення валютних цінностей. [2, с.3-4].

Кожен Банк в рамках даної політики під інформаційною безпекою передбачає забезпечення наступних характеристик інформації:

1) конфіденційність: надання доступу до інформації тільки тим, у кого є на це право;

2) цілісність: захист точності і повноти інформації і методів її обробки;

3) доступність: забезпечення доступу до інформації і пов'язаних з нею ресурсів авторизованими користувачами по мірі необхідності.

Так, як інформація є ресурсом, який, як і інші важливі бізнес-ресурси, має певну цінність для Банку, а, отже, потребує відповідного захисту. Інформаційна політика безпеки банків, якої притримується кожен Банк з метою підтримання належного захисту інформації та її забезпечення повинна відповідати принципам інформаційної безпеки. Загальноприйнятими принципами вважаються: цілісності - властивості захищеності, безпомилковості та повноти ресурсів СУІБ; конфіденційності – властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів; доступності – властивість доступності та можливості використання ресурсів СУІБ на

вимогу санкціонованого об'єкта. Аналізуючи данні питання за працями науковців, а також враховуючи стрімкі рухи розвитку інформаційних технологій вважаю, що крім загально визначених принципів Банкам потрібно особливої уваги у своїй політиці приділити принципу «Спостережності» - властивість системи (автоматизованої, контролю доступу, моніторингу тощо) фіксувати діяльність ідентифікованих користувачів і процесів. Це в свою чергу підсилить захист інформації з обмеженим доступом, до якої відносяться відомості, що становлять банківську таємницю, персональні дані та іншу конфіденційну інформацію.

Вважаю за потрібне зазначити, що у ч.3 ст.12 Обмін інформацією та конфіденційність Закону України «Про Фінансову реструктуризацію» зазначено, що Боржник та залучені кредитори, спостережна рада, секретаріат, арбітражний комітет (арбітр) та інші особи, що залучаються до проведення процедури фінансової реструктуризації, зобов'язані не розголошувати дані, інформацію, документи та звіти, що пов'язані з процедурою фінансової реструктуризації та визначаються їх володільцями як конфіденційні. [3].

Це в свою чергу підкреслює те, що захист інформації клієнтів та захист Банківської інформації потрібно підсилити.

Крім цього вважаю, що Банки повинні постійно стимулювати своїх працівників приймати участь у Міжнародних Форумах «IT-інфраструктура та кібербезпека банківської системи», що присвячується питанням банківського кібернавчання на яких фахівці та керівники служб інформаційної безпеки банків можуть попрактикуватись в реагуванні на кіберінциденти в форматі інтерактивної гри.

Отже, правильне тлумачення і розуміння норм фінансового законодавства, міжнародних стандартів, досвіду, своєчасне внесення змін до політики Банків враховуючи всі заплановані перспективи регуляторних політик НБУ, щодо СУІБ дасть можливість забезпечити належний захист

інформації, що в свою чергу підсилить стабільність банківського сектору України в умовах бурхливих змін економічного і соціального розвитку держави.

Література:

1. Стратегія розвитку інформаційного суспільства в Україні Схвалено Розпорядженням КМУ від 15 травня 2013 р. № 386-р [Електронний ресурс] / Режим доступу: http://zakon3.rada.gov.ua/laws/show/386-2013-%D1%80
2. План підготовки проектів регуляторних актів Національного банку України на 2017 рік [Електронний ресурс] / Режим доступу: https://bank.gov.ua/control/uk/publish/category?cat_id=37193
3. Закон України «Про фінансову реструктуризацію» Верховна Рада України; Закон від 14.06.2016 № 1414-VIII [Електронний ресурс] / Режим доступу: http://zakon2.rada.gov.ua/laws/show/1414-19