V. ФІНАНСИ, БАНКІВСЬКА СПРАВА ТА СТРАХУВАННЯ

УДК 33.68. 004.056

ОРГАНІЗАЦІЯ ЗБЕРІГАННЯ ЕЛЕКТРОННИХ АРХІВІВ БАНКУ ЯК ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРАТАКАМ

М. Ю. БОГОСЛАВСЬКИЙ,
(Національна академія управління, м. Київ)

***Анотація**. **Мета** статті полягає в дослідженні організації зберігання електронних архівів банку як забезпечення протидії кібератакам. **Методика дослідження.** Вирішення поставлених у статті завдань здійснено за допомогою таких методів дослідження: аналіз і синтез, систематизація та узагальнення, діалектичний підхід. **Результати.** У рамках статті розглянуто особливості сучасного стану та нормативно-правові акти, які регламентують зберігання архівів програмно-технічного комплексу банку відповідно до вимог НБУ. Обґрунтовано важливість інформаційної безпеки банку як складової ризик-орієнтованого підходу банку у випадках витоку клієнтської інформації, іміджевих втрат, несанкціонованого розкриття інформації та похідних видів ризику в рамках банківської діяльності. Доопрацьовано функціонал архівного підрозділу банку та доповнено його визначення в контексті засад формування електронних архівів та їх здатності протидіяти сучасним кіберзагрозам. **Практична значущість результатів дослідження.** Важливість дотримання стабільного функціонування банку в межах платіжної системи. яка його обслуговує, залежить від безпеки проходження транзакцій, оперативної фільтрації загроз та резервування клієнтської інформації для збереження цілісності фінансової активності установи.*

***Ключові слова:** архів програмно-технічного комплексу, інформаційна безпека банку, протидія кібератакам, архівний підрозділ банку, резервна копія, платіжна система.*

Постановка проблеми в загальному вигляді та зв'язок із найважливішими науковими чи практичними завданнями. Інформаційна безпека комерційного банку має пряме відношення до протидії кіберзлочинності, основним об'єктом якої є несанкціоноване заволодіння базами даних банку. З огляду на сучасний стан банківської системи та внутрішньополітичну ситуацію у країні постає необхідність доопрацювання внутрішньобанківських правил формування, обліку, ведення, передавання, зберігання та знищення електронних архівів програмно-технічних комплексів автоматизації банківської діяльності та платіжних систем, які об'єднуються навколо процедури ведення електронного архіву даних банку.

Аналіз останніх досліджень і публікацій. Серед розробок значної кількості методичних підходів з організації формування та управління електронними банківськими архівами більшість напрацювань належать самим банкам та НБУ, оскільки ця тематика є життєво необхідною для забезпечення фінансової

безпеки (ФБ), швидкості відновлення дієздатності банку після кібератаки, збереження банківської таємниці та супроводу транзакцій платіжними системами. Однак слід відмітити дослідження О. В. Мельниченко, С. Т. Іванишина, В. Ю. Дубницького, В. В. Домарєва, Д. В. Домарєва, А. М. Кобиліна, Т. М. Болгар, С. І. Юрія, орієнтовані на покращення загального рівня інформаційної безпеки банку та технологічних властивостей цього процесу.

Формування цілей статті (постановка завдання). Мета статті полягає в дослідженні організації зберігання електронних архівів банку як забезпечення протидії кібератакам.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Архівний підрозділ комерційного банку в адаптованому значенні до сучасних викликів, завданих кіберзагрозами, постає в особі структурного підрозділу або відповідального працівника банку, призначені для виконання функцій формування, зберігання, контролю цілісності та достовірності електронних архівів банку та передачі їх до архівних установ відповідно до вимог законодавства з метою швидкого відновлення після кібератаки або несанкціонованого втручання [2, с. 65].

Набір затверджених з урахуванням вимог законодавства України, нормативно-правових актів НБУ та комерційних банків з питань архівної справи та внутрішніх нормативних документів для протидії загрозам подано в таблиці 1 [6, с. 108].

Таблиця 1

Перелік законодавчого підґрунтя щодо архівації даних банків

Документ	Назва	Дата
Закон України	«Про Національний архівний фонд та архівні заклади»	24.12.1993 № 3814-XII
Закон України	«Про електронні документи та електронний документообіг»	22.05.2003, №851-IV
Закон України	«Про захист інформації в інформаційно-телекомунікаційних системах»	05.07.1994 №80/94-ВР
Закон України	«Про електронний цифровий підпис»	22.05.2003 № 852-IV
Закон України	«Про банки і банківську діяльність»	07.12.2000 № 2121-III
Постанова Правління НБУ	Положення про порядок формування, зберігання та знищення електронних архівів у НБУ і банках України	12.09.2006
Наказ Міністерства юстиції України	Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання	11.11.2014 № 1886/5
Постанова Правління НБУ	Перелік документів, що утворюються в діяльності НБУ та банків України із зазначенням строків зберігання	08.12.2004 № 601
Зведена номенклатура справ комерційного банку	Внутрішні інструкції про порядок архівації документів розроблені під його актуальну роботу	За регламентом роботи банку

Необхідність усебічного вдосконалення програмного забезпечення банку для використання його структурними підрозділами є важливим фактором у разі протидії та нівелізації загроз, а також збереження інформації, що має банківську таємницю в рамках критичних бізнес-процесів на всіх рівнях. Організаційно-розпорядча діяльність банку потребує відповідних програмно-технічних комплексів, що забезпечать ефективне функціонування банку та нівелізує ризики інформаційної безпеки та наслідків кібератак.

Сукупність організаційних, програмно-апаратних засобів для збереження електронних документів та інших даних в електронному вигляді, сформованих в установлені терміни, передбачають автоматизацію банківської діяльності. У процесі діяльності банку на двох рівнях проведення транзакцій генеруються два типи електронних архівів: електронний архів платіжної системи на зовнішньому рівні та електронний архів внутрішньобанківських документів на зовнішньому рівні. Під електронним архівом, що утворюється у процесі ді-

яльності банку (архів внутрішньобанківських документів), розуміють електронні документи, що створюються в ході діяльності керівних органів банку, структурних підрозділів, комітетів та інших колегіальних органів, та належать до компетенції ФБ банку через можливість витоків банківської таємниці чи збоїв у розрахункових операціях [4, с. 218].

Під ефективним електронним архівом, здатним протидіяти загрозам ФБ банку через блокування транзакцій у платіжній системі розуміють автоматизовану підбірку масиву документів та інформації, що створюються платіжною системою та робочими інстанціями під час оброблення електронних документів і повідомлень у структурованому за правилами цієї платіжної системи в електронному вигляді та можуть бути переглянуті й роздруковані засобами в режимі он-лайн, формується з резервних копій програмно-технічного комплексу платіжної системи [1, с. 30].

З технічної точки зору програмний комплекс банківської діяльності базується на взаємодії апаратних та програмних засобів, що забезпечують: автоматизацію та підтримку діяльності підрозділів банку; надання сервісів та продуктів клієнтам, їх обслуговування, у тому числі сервери, бази даних, описи інформації та процедур обробки, форматів документів тощо в робочій документації, журнали роботи системи та підсистем, довідники, штучні пастки для програмних продуктів та іншу необхідну для загрозливого комплексів інформацію. – Технологічність програмних комплексів банківської діяльності у сучасній інтерпретації загрозливого середовища для ФБ банків потребує врахування оперативного та системного резервування, що передбачає створення резервних копій даних через буфер обміну даних на носіях, яка призначена для відновлення даних на новоствореному сервері їх розміщення у випадку їх пошкодження або несанкціонованого використання. Серед методик резервування використовують «повне резервне копіювання» (Full backup), або альтернативні методики супроводу безперервності функціонування програмного комплексу. до яких зараховують «інкрементальне резервне копіювання» або «диференціальне резервне копіювання», що є ефективними в окремих випадках забезпечення ФБ банку за рахунок формування окремих типів архівів [5, с. 44].

Зазвичай архіви електронних документів створюються структурними підрозділами переважно в головному офісі банку, якщо інше не передбачене технологічними або супутніми аспектами забезпечення ФБ банку, що має бути визначено та затверджено внутрішніми розпорядчими документами комерційного банку. Період зберігання електронних архівів та резервних копій визначається нормативною документацією, яку регламентує НБУ та внутрішні методологічні підрозділи банків залежно від специфіки банку на ринку та ступеня потенційного проникнення загрози до нього.

Регламентований період зберігання приймається рішенням правління та відображається в затвердженій номенклатурі справ комерційного банку на базі Постанови правління НБУ від 08.12.2004 № 601. Електронні архіви програмно-технічних комплексів з автоматизації банківської діяльності та платіжної системи тимчасового (до 10 років) строку зберігання перебувають на оперативному зберіганні у структурному підрозділі, де вони перебували на виконанні або були створені і з часу їх створення до закінчення їх зберігання в цьому структурному підрозділі [8, с. 116].

На мікрорівні конкретної фінансової установи формування електронних архівів за результатами роботи програмно-технічних комплексів з автоматизації банківської діяльності здійснюється відповідно до технології роботи цих комплексів у такому бажаному порядку:

1) структура та зміст електронних архівів за результатами роботи програмно-технічних комплексів з автоматизації банківської діяльності визначаються технологією роботи цих комплексів і внутрішніми нормативними документами банку й нормативно-правовими актами НБУ;

2) методичне керівництво з питань формування електронних архівів за результатами роботи програмно-технічних комплексів з автоматизації банківської діяльності здійснюють розробники або спеціалісти, які супроводжують роботу цих комплексів;

3) технічні та технологічні умови зберігання та користування електронними архівами за результатами роботи програмно-технічних комплексів з автоматизації банківської діяльності забезпечує підрозділ банку, який здійснює експлуатацію або супроводження цього комплексу (зокрема управління інформацій-

них технологій), або інший підрозділ, призначений згідно з розпорядженням керівництва банку [3, с. 140].

На макроекономічному рівні порядок формування електронних архівів платіжних систем здвійснюється відповідно до регламенту платежів у платіжних системах, які задіяні в технологічному процесі забезпечення ФБ банку та сприяють захисту фінансової установи та її швидке відновлення після кібератак, куди включено структура та зміст електронних архівів за результатами роботи платіжних систем, визначаються документами платіжної системи та нормативно-правовими актами НБУ; а також технічні та технологічні умови зберігання й користування електронними архівами за результатами роботи платіжних систем, що забезпечуються структурними підрозділами банку – учасниками платіжної системи, які здійснюють експлуатацію відповідного програмного забезпечення платіжної системи, або інший підрозділ, призначений для моніторингу кіберзагроз та оперативного відновлення банку після них [7, с. 344].

Актуальною проблемою є те, що з метою мінімізації ризику втрати інформації під час оперативного зберігання територіально відокремленими структурними підрозділами (якщо це передбачено технологічними або іншими причинами) виготовляються резервні копії електронних архівів програмно-технічних комплексів з автоматизації банківської діяльності тимчасового зберігання (що мають силу оригіналу) на зовнішніх носіях, які передаються на зберігання до архівного підрозділу банку. Після закінчення строку зберігання електронних архівів тимчасового типу вони знищуються структурним підрозділом, хоча на цьому етапі є ризик втрати чи несанкціонованого дублювання інформації, що може мати катастрофічні наслідки не тільки для забезпечення ФБ банку, а також для його репутації та платоспроможності. Особливістю складання електронних архівів програмно-технічного комплексу за автоматизації банку є генерація відповідних електронних документів та інформації щодо транзакцій, що створюються програмно-технічним комплексом під час обробки електронних документів і повідомлень у структурованому за правилами операційної програми банку в електронному вигляді та можуть бути переглянуті й роздруковані засобами цього комплексу. Вони формуються з резервних копій програмно-технічного комплексу в рамках забезпечення ФБ банку[8, с. 12].

Хоча резервні копії не надаються територіально відокремленим підрозділам для використання в повсякденній роботі, а слугують тільки на випадок централізованого поновлення даних у разі їх втрати, пов’язаної з непередбачуваними та незалежними від користувачів обставинами.

Зберігання електронних архівів може мати додаткові ризики з позиції проникнення до них у довгостроковому періоді, тому строк зберігання електронних архівів визначається періодом функціональної необхідності та потенційної користі відповідних електронних даних, які продубльовано документами на паперових носіях. Електронні архіви тимчасового строку зберігання (звичайний строк зберігання становить 3 роки, але може бути подовжений до 10 років включно) перебувають на оперативному зберіганні у структурному підрозділі банку, де вони були реалізовані з часу їх створення протягом двох років, після чого передаються на зовнішніх носіях до архівного підрозділу [6, с. 108].

Якщо електронні архіви утворюються за результатами роботи програмно-технічних комплексів, відповідальність за їх зберігання несе підрозділ, у якому вони перебували на оперативному зберіганні. Після закінчення строку їх зберігання вони знищуються структурним підрозділом банку, у якому вони перебували на оперативному зберіганні, в установленому порядку.

Висновки із зазначених проблем і перспективи подальших досліджень у поданому напрямі. Забезпечення оперативного зберігання електронних архівів у рамках забезпечення ФБ банку здійснюється за допомогою створених резервних копій електронних архівів на електронних носіях. Збереженість електронних архівів, що перебувають на оперативному зберіганні, забезпечується тим структурним підрозділом банку, у якому вони перебувають на оперативному зберіганні.

Резервні копії в загальноприйнятому вжитку формуються управлінням інформаційних технологій, проте такий процес має дублюватися підрозділом ФБ банку відповідно до встановлених регламентів створення резервних копій та встановлених функціональних зв’язків у бізнес-середовищі банку.

Резервні копії архівів для оперативного відновлення роботи таких комплексів створюються щоденно, а застаріла (не більше ніж 3 дні) резервна копія послідовно замінюється на нову після створення поточної нової резервної копії.

Автоматизація формування електронних архівів та користування ними, у тому числі ведення справ, реєстрів, формування ідентифікаційних написів, накладання та перевірки електронних цифрових підписів, передбачається на базі адаптованих сервісів, які реалізовані спільно із платіжною системою та внутрішнім забезпеченням електронного документообігу з функцією автоматизації створення та ведення електронних архівів. Зокрема для збільшення їх ефективності необхідно застосовувати підготовку до передавання електронних архівів через підрозділи інформаційної безпеки банку в такому порядку: перевірка всіх електронних підписів; експертиза цінності електронних документів; оформлення електронних справ; складання описів електронних справ; підготовка комплекту супровідної документації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дубницький В. Ю. Порівняльний аналіз результатів планування нормативів банківської безпеки засобами класичної та нестандартної інтервальної арифметики / В. Ю. Дубницький, А. М. Кобилін // Радіоелектронні і комп'ютерні системи. − 2014. − № 5. − С. 29−33.

2. Домарєв Д. В. Методика управління інформаційною безпекою в банківських установах за допомогою СУІБ «Матриця» / Д. В. Домарєв, В. В. Домарєв // Безпека інформації. − 2013. − Т. 19. − № 1. − С. 60−70.

3. Домарєв В. В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) / В. В. Домарєв, Д. В. Домарєв. – Донецьк : «Велстар», 2012. – 146 с.

4. Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности / В. А. Курбатов, В. Ю. Скиба. – Санкт-Петербург : Питер, 2008. – 320 с.

5. Іванишин С. Т. Менеджмент безпеки ІТ комплексної автоматизації у територіально рознесених відділеннях банку / С. Т. Іванишин // Інформаційна безпека. − 2013. − № 2. − С. 42−47.

6. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) : ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – Київ : Національний банк України, 2010. – 163 с.

7. Мельниченко О. В. Аудит інформаційної безпеки банку при роботі з електронними грошима / О. В. Мельниченко // Проблеми економіки. − 2013. − № 4. − С. 341−347.

8. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України : лист департаменту інформатизації Національного банку України банкам України від 03 березня 2011 р. № 24-112/365. – Київ : Національний банк України, 2011.

REFERENCES

1. Dubnytskyi, V. Iu. & Kobylin, A. M. (2014). Porivnialnyi analiz rezultativ planuvannia normatyviv bankivskoi bezpeky zasobamy klasychnoi ta nestandartnoi intervalnoi aryfmetyky [Comparative analysis of the results of banking safety standards planning by means of classical and non-standard interval arithmetic]. *Radioelektronni i komp'iuterni systemy − Radioelectronic and computer systems*, 5, 29−33 [in Ukrainian].

2. Domariev, D. V. & Domariev, V. V. (2013). Metodyka upravlinnia informatsiinoiu bezpekoiu v bankivskykh ustanovakh za dopomohoiu SUIB «Matrytsia» [Methodology of Information Security Management in Banking Institutions with the help of ISIB "Matrix"]. *Bezpeka informatsii − Information Security*, 1 (19), 60−70 [in Ukrainian].

3. Domariev, V. V. & Domariev, D. V. (2012). *Upravlinnia informatsiinoiu bezpekoiu v*

bankivskykh ustanovakh (Teoriia i praktyka vprovadzhennia standartiv serii ISO 27k) [Management of Information Security in Banking Institutions (Theory and Practice of the Implementation of ISO 27k Standards)]. Donetsk: "Velstar" [in Ukrainian].

4. Kurbatov, V. A. & Skyba, V. Iu. (2008). *Rukovodstvo po zashchyte ot vnutrennykh uhroz ynformatsyonnoi bezopasnosty [Guidance on protection from internal threats to information security]*. Sankt-Peterburg: Pyter [in Russian].

5. Ivanyshyn, S. T. (2013). *Menedzhment bezpeky it kompleksnoi avtomatyzatsii u teritorialno roznesenykh viddilenniakh banku [Safety Management and Integrated Automation in Territorially Distributed Bank Offices]*. *Informatsiina bezpeka − Information Security*, 2, 42−47. [in Ukrainian].

6. *Informatsiini tekhnolohii. Metody zakhystu. Zvid pravyl dlia upravlinnia informatsiinoiu bezpekoiu (ISO/IEC 27002:2005, MOD): HSTU SUIB 2.0/ISO/IEC 27002:2010 [Information Technology. Methods of protection. Code of Conduct for Information Security Management (ISO / IEC 27002: 2005, MOD): GATS SOIB 2.0 / ISO / IEC 27002: 2010]*. (2010). Kyiv : Natsionalnyi bank Ukrainy [in Ukrainian].

7. Melnychenko, O. V. (2013). Audyt informatsiinoi bezpeky banku pry roboti z elektronnymy hroshyma [Audit of information security of the bank when working with electronic money]. *Problemy ekonomiky − Economy problems*, 4, 341−347 [in Ukrainian].

8. *Metodychni rekomendatsii shchodo vprovadzhennia systemy upravlinnia informatsiinoiu bezpekoiu ta metodyky otsinky ryzykiv vidpovidno do standartiv Natsionalnoho banku Ukrainy: lyst departamentu informatyzatsii Natsionalnoho banku Ukrainy bankam Ukrainy vid 03 bereznia 2011 r. № 24-112/365 [Methodical recommendations on the implementation of the information security management system and risk assessment methodology in accordance with the standards of the National Bank of Ukraine: the letter of the Department of Informatization of the National Bank of Ukraine to the banks of Ukraine from March 03, 2011, No. 24-112 / 365]*. Kyiv : Natsionalnyi bank Ukrainy [in Ukrainian].

Н. Ю. Богославский *(Национальная академия управления, Киев).* ***Организация хранения электронных архивов банка как обеспечение противодействия кибератакам.***

Аннотация. Цель *статьи заключается в исследовании организации хранения электронных архивов банка в качестве обеспечения противодействия кибератакам.* ***Методика исследования.*** *Решение задач, поставленных в статье, осуществлено с помощью таких методов исследования: анализ и синтез, систематизация и обобщение, диалектический подход.* ***Результаты.*** *В рамках статьи рассмотрены особенности современного состояния и нормативно-правовые акты, регламентирующие хранение архивов программно-технического комплекса банка в соответствии с требованиями НБУ. Обоснована важность информационной безопасности банка как составляющей риск-ориентированного подхода банка в случаях утечки клиентской информации, имиджевых потерь, несанкционированного раскрытия информации и производных видов риска в рамках банковской деятельности. Доработан функционал архивного подразделения банка и дополнено его определение в контексте принципов формирования электронных архивов и их способности противодействовать современным киберугрозам.* ***Практическое значение результатов исследований.*** *Важность соблюдения стабильного функционирования банка в пределах платежной системы, которая его обслуживает, зависит от безопасности прохождения транзакций, оперативной фильтрации угроз и резервирование клиентской информации для сохранения целостности финансовой активности учреждения.*

Ключевые слова: *архив программно-технического комплекса, информационная безопасность банка, противодействие кибератакам, архивное подразделение банка, резервная копия, платежная система.*

N. Bogoslavskij *(National Academy of Management, Kyiv).* ***Organization of storage of the bank's electronic archives as measures of protection against cyberattacks.***

Annotation. The purpose *of the paper is to investigate the organization of storage of the bank's electronic archives as measures of protection against cyberattacks.* ***Methodology of research.*** *The*

objectives of the article implemented by using the following general and specific research methods: analysis and synthesis, systematization and generalization, dialectical approach. ***Findings.*** *In the article, the features of the current state and regulations of archives' storage by the program-technical complex of the bank were observed in accordance with the requirements of the National Bank of Ukraine. The importance of information security of the bank as a risk-oriented approach was substantiated according to such components as leakage of client information, image losses, and unauthorized disclosure of information and derivative types of risk within the framework of banking activity. The functionality of the bank's archival department was refined and its definition was also supplemented in the context of the foundations of electronic archives formation and their capability to stand against cyber threats.* ***Practical value.*** *The importance of maintaining a stable bank function within the payment system depends on the security of transactions, operational filtering of threats and the provision of client information to maintain the integrity of the bank's financial activity.*

Keywords: *archive of software and hardware complex, bank's information security, counteraction to cyberattacks, bank archival division, backup, payment system.*