ПРАВЛІННЯ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ

ПОСТАНОВА

28.09.2017 № 95

Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України

Відповідно до статей 7, 15, 56 Закону України "Про Національний банк України", з метою удосконалення вимог до захисту інформації в інформаційних системах банків з урахуванням актуальних кіберзагроз, установлення вимог щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту банків, Правління Національного банку України **ПОСТАНОВЛЯЄ:**

1. Затвердити Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України (далі - Положення), що додається.

2. Департаменту безпеки (Скомаровський О.А.) протягом чотирьох місяців з дати офіційного опублікування цієї постанови розробити Методичні рекомендації для перевірки системи управління інформаційною безпекою та виконання заходів з безпеки інформації під час проведення інспекційних перевірок банків України.

3. Департаменту безпеки (Скомаровський О.А.) після офіційного опублікування довести до відома банків України інформацію про прийняття цієї постанови для використання в роботі.

4. Контроль за виконанням цієї постанови покласти на першого заступника Голови Національного банку України Смолія Я.В.

5. Постанова набирає чинності з 01 березня 2018 року, крім розділу V Положення, який набере чинності з 01 вересня 2019 року.

В.о. Голови **Я.В. Смолій**

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
28.09.2017 № 95

ПОЛОЖЕННЯ
про організацію заходів із забезпечення інформаційної безпеки в банківській системі України

І. Загальні положення

1. Це Положення розроблено відповідно до Законів України "Про Національний банк України", "Про банки і банківську діяльність", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про основи національної безпеки України", указів Президента України від 13 лютого 2017 року № 32/2017 "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" та від 15 березня 2016 року № 96/2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", національних стандартів України з питань інформаційної безпеки ДСТУ ISO/IEC 27000:2015 "Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник" (далі - ДСТУ ISO/IEC 27000:2015), ДСТУ ISO/IEC 27001:2015 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги" (далі - ДСТУ ISO/IEC 27001:2015), ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки" (далі - ДСТУ ISO/IEC 27002:2015), які прийняті наказом Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 18 грудня 2015 року № 193, та з урахуванням міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту з метою підвищення рівня інформаційної безпеки в банківській системі України.

2. Це Положення встановлює:

1) обов'язкові мінімальні вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту;

2) принципи управління інформаційною безпекою;

3) вимоги до інформаційних систем банку, що взаємодіють з інформаційними системами Національного банку України (далі - Національний банк), з урахуванням напрямів розвитку криптографічного захисту інформації в інформаційних системах Національного банку.

3. У цьому Положенні терміни та поняття вживаються в таких значеннях:

1) багатофакторна автентифікація - автентифікація, яка здійснюється за допомогою захищених механізмів двох або більше типів [наприклад, застосування для автентифікації пароля разом із апаратним засобом захисту інформації (токеном) або біометричної автентифікації разом із паролем];

2) зловмисний код - комп'ютерна програма/комплекс комп'ютерних програм або частина програмного коду інформаційної системи, що впроваджується за участю користувача або виконується автоматично, створює загрозу або умови для реалізації загрози порушення штатної роботи обладнання банку та/або порушення конфіденційності, цілісності, доступності інформації, яка обробляється в інформаційних системах банку;

3) критичні бізнес-процеси банку - бізнес-процеси діяльності банку, визначені банком критичними щодо інформаційної безпеки за результатом їх оцінювання банком за такими критеріями: конфіденційність, цілісність, доступність;

4) мережа банку - комплекс технічних засобів телекомунікацій, призначених для маршрутизації, комутації, передавання та/або приймання інформації дротовим та/або бездротовим зв'язком між кінцевим обладнанням (комп'ютерне обладнання, інші компоненти інформаційних систем банку) усередині периметра банку;

5) мінімальний рівень повноважень - повноваження та права доступу, мінімально необхідні для якісного виконання персоналом банку службових обов'язків;

6) пристрої уніфікованого управління загрозами (Unified threat management, UTM) - пристрої, які можуть виконувати кілька функцій безпеки з одного пристрою: міжмережевий екран, запобігання несанкціонованого доступу до мережі, антивірусний шлюз, антиспамовий шлюз, віртуальна приватна мережа (Virtual private network, VPN), фільтрація вмісту, балансування навантаження, запобігання витоку даних;

7) ризик-орієнтований підхід до забезпечення інформаційної безпеки - прийняття управлінських рішень на підставі аналізу порівняння поточних ризиків інформаційної безпеки з прийнятними.

Інші терміни, що вживаються в цьому Положенні, використовуються в значеннях, визначених законами України, нормативно-правовими актами Національного банку та ДСТУ ISO/IEC 27000:2015.

4. Це Положення не встановлює вимог щодо:

1) фізичної безпеки приміщень банків, технічного захисту інформації для приміщень банків, використання криптографічних засобів захисту інформації Національного банку в інформаційних системах Національного банку, вимоги до яких визначені відповідними нормативно-правовими актами Національного банку;

2) використання хмарних технологій/сервісів (Cloud technologies) у сфері автоматизації, технічної й технологічної підтримки діяльності банків, вимоги до яких визначаються окремим документом.

5. Вимоги цього Положення поширюються на банки. Вимоги розділу III цього Положення також поширюються на небанківські установи - учасників інформаційних систем Національного банку.

6. Принципи забезпечення інформаційної безпеки:

1) підхід до забезпечення інформаційної безпеки має бути системним (комплексним);

2) процес удосконалення та розвитку інформаційної безпеки має бути безперервним і здійснюватися шляхом обґрунтування та реалізації раціональних засобів, методів, заходів із застосуванням найкращого міжнародного досвіду;

3) заходи захисту від реальних та потенційних загроз інформаційній безпеці банку мають бути своєчасні й адекватні;

4) забезпечення належного рівня інформаційної безпеки банку неможливе без підтримки та контролю з боку керівників банку;

5) сталий розвиток систем інформаційної безпеки можливий лише в разі забезпечення достатності ресурсів, у тому числі фінансових.

7. Принципи криптографічного захисту інформаційних систем Національного банку:

1) криптографічний захист інформації в інформаційних системах Національного банку на ділянці зв'язку між учасником інформаційних систем Національного банку та Національним банком забезпечується застосуванням багаторівневого (ешелонованого) підходу, за яким окремо за допомогою незалежних систем криптографічного захисту інформації захищається сеансовий рівень базової еталонної моделі взаємодії відкритих систем (Open systems interconnection basic reference model, OSI/ISO) та прикладний рівень моделі взаємодії відкритих систем інформаційних систем Національного банку;

2) для захисту сеансового рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовується криптографічний протокол захисту на транспортному рівні (Transport layer security, TLS), забезпечуються контроль цілісності та конфіденційність інформації. Для прикладного рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовуються такі механізми захисту: ідентифікація/автентифікація підписувача, контроль цілісності та конфіденційність на всіх етапах оброблення інформації;

3) залежно від категорії інформації щодо критерію конфіденційності, для забезпечення ідентифікації та автентифікації, використовується односпрямований (криптографічний ключ лише на стороні сервера, сувора криптографічна автентифікація сервера) або двоспрямований достовірний канал захисту на транспортному рівні (криптографічний ключ на стороні клієнта і на стороні сервера, сувора криптографічна автентифікація обох сторін з'єднання);

4) інформаційні системи Національного банку підтримують роботу криптографічного протоколу захисту на транспортному рівні останньої версії, але не нижче версії 1.2;

5) інформаційні системи Національного банку використовують криптографічні набори захисту на транспортному рівні лише з шифруванням та застосовують симетричні криптографічні алгоритми з довжиною ключа не менше ніж 128 біт;

6) Департамент безпеки Національного банку надає криптобібліотеки для криптографічних засобів захисту інформації, рекомендації щодо їх використання та програмне забезпечення генерації ключів.

8. Банк зобов'язаний упровадити систему управління інформаційною безпекою (далі - СУІБ) згідно з ДСТУ ISO/IEC 27001:2015 для визначеної сфери застосування з урахуванням обов'язкових вимог щодо впровадження СУІБ, викладених у розділі II цього Положення.

9. Передумовами впровадження СУІБ у банку є:

1) упровадження процесного підходу до діяльності банку;

2) упровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки банку.

10. Банк зобов'язаний запровадити процес управління ризиками інформаційної безпеки в рамках системи управління ризиками банку. Банк має право самостійно визначати підходи (методики) оцінювання та оброблення ризиків інформаційної безпеки.

11. Банк зобов'язаний запровадити, використовуючи ризик-орієнтований підхід, заходи безпеки, визначені додатком А до ДСТУ ISO/IEC 27001:2015, згідно з ДСТУ ISO/IEC 27002:2015 та з урахуванням обов'язкових вимог щодо організації заходів безпеки інформації, викладених у розділах IV і V цього Положення.

12. Банк зобов'язаний визначити мінімальною сферою застосування СУІБ усі критичні бізнес-процеси банку. Банк має право розширити сферу застосування СУІБ банку відповідно до особливостей його діяльності, характеру та обсягу банківських, фінансових послуг та інших видів діяльності.

13. Національний банк має право здійснювати перевірку стану впровадження СУІБ банку та повноту виконання заходів безпеки інформації, що встановлені цим Положенням.

II. Вимоги щодо впровадження СУІБ

14. Банк зобов'язаний сформувати колективний керівний орган з питань впровадження та функціонування СУІБ (далі - керівний орган СУІБ) або наділити цими повноваженнями існуючий колективний керівний орган банку та розробити положення про керівний орган СУІБ банку з чітким визначенням його завдань, функцій та відповідальності.

15. Банк зобов'язаний включити до складу керівного органу СУІБ голову правління банку та/або його заступника, що відповідає за інформаційну безпеку банку, керівників підрозділів банку - власників критичних бізнес-процесів банку та керівника підрозділу банку з управління ризиками. Банк має право ввести до складу керівного органу СУІБ інших працівників банку відповідно до потреб, що обумовлені особливостями діяльності банку.

16. Банк зобов'язаний покласти на керівний орган СУІБ обов'язок виконання таких завдань:

1) погодження та перегляд політики інформаційної безпеки, положення щодо застосовності та стратегії розвитку інформаційної безпеки банку;

2) узгодження впровадження нових проектів, напрямів, стратегічних завдань з питань інформаційної безпеки банку та заходів інформаційної безпеки;

3) розгляд, затвердження та контроль за виконанням проектів щодо розроблення, упровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення СУІБ банку;

4) визначення необхідних оптимальних ресурсів для впровадження заходів інформаційної безпеки;

5) організація практичних заходів щодо підвищення обізнаності/навчання персоналу банку з питань інформаційної безпеки;

6) забезпечення своєчасного моніторингу стану впровадження та ефективності функціонування СУІБ банку з подальшою оцінкою можливостей вдосконалення та потреби проведення коригувальних дій.

17. Банк зобов'язаний розробити та впровадити політику інформаційної безпеки, яка має містити:

1) цілі інформаційної безпеки;

2) сферу застосування політики інформаційної безпеки;

3) принципи, правила та вимоги інформаційної безпеки в банку;

4) визначення функцій (ролей) і відповідальності за забезпечення інформаційної безпеки.

18. Банк зобов'язаний забезпечити підтримку політики інформаційної безпеки в актуальному стані та її перегляд не рідше ніж один раз на рік. Якщо за результатами перегляду зміни до політики інформаційної безпеки не вносяться, то повторне її затвердження не потрібно.

19. Банк зобов'язаний затвердити політику інформаційної безпеки і довести її зміст до відома всього персоналу банку та, за необхідності, представникам третіх сторін.

20. Банк зобов'язаний розробити та затвердити стратегію розвитку інформаційної безпеки. Банк має право затвердити стратегію розвитку інформаційної безпеки банку в документі, яким затверджено загальну стратегію розвитку банку, у вигляді окремого розділу. Зміст стратегії має узгоджуватися з політикою інформаційної безпеки банку, основними стратегічними цілями банку, що пов'язані із впровадженням нових бізнес-процесів/банківських продуктів з використанням технологій, які потребують захисту інформації, а також враховувати планування розвитку інфраструктури банку та заходів інформаційної безпеки для мінімізації ризиків інформаційної безпеки.

21. Банк зобов'язаний розробити та затвердити план забезпечення безперервності діяльності банку, у якому враховано безперервність функціонування заходів інформаційної безпеки в рамках процесу управління безперервністю діяльності банку.

22. Банк має право розробляти документи СУІБ у формі окремих документів або об'єднаних за типом (тематикою) в загальні документи, із зазначенням у них розділів, що відповідають визначеним напрямам (питанням) інформаційної безпеки.

ІІІ. Криптографічний захист інформації в інформаційних системах Національного банку

23. Учасники інформаційних систем Національного банку зобов'язані налаштувати системи криптографічного захисту інформації в інформаційних системах Національного

банку згідно з вимогами, які визначені у відповідній експлуатаційній документації кожної інформаційної системи Національного банку.

24. Банк зобов'язаний забезпечити захист інформаційних систем банку від несанкціонованого доступу та дій, направлених на відмову в обслуговуванні відповідно до вимог розділу IV цього Положення.

IV. Заходи безпеки інформації

25. Банк зобов'язаний призначити відповідальну особу за інформаційну безпеку банку (Chief information security officer, CISO), яка має повноваження, достатні для прийняття управлінських рішень (посада не нижче заступника голови правління банку), та забезпечує:

1) стратегічне керівництво з питань інформаційної безпеки банку;

2) визначення напрямів розвитку інформаційної безпеки банку, їх відповідність стратегії розвитку банку;

3) відповідність заходів безпеки інформації потребам бізнес-процесів/банківських продуктів;

4) контроль за впровадженням заходів безпеки інформації в банку.

26. Банк зобов'язаний сформувати підрозділ з інформаційної безпеки не менше як із двох працівників зі складу штатних працівників банку. Підрозділ з інформаційної безпеки банку має безпосередньо підпорядковуватися відповідальній особі за інформаційну безпеку банку.

27. Підрозділ з інформаційної безпеки банку має здійснювати:

1) розроблення вимог щодо налаштувань безпеки інформаційних систем банку;

2) розроблення або участь у розробленні документів банку щодо інформаційної безпеки;

3) контроль за виконанням заходів щодо забезпечення безпеки інформації на всіх стадіях життєвого циклу інформаційних систем банку;

4) розслідування інцидентів безпеки інформації;

5) спільно з підрозділами інформаційних технологій (інформатизації, автоматизації) банку відновлення функціонування інформаційних систем банку після збоїв у роботі внаслідок інцидентів безпеки інформації.

28. Працівникам підрозділу інформаційної безпеки/відповідальній особі за інформаційну безпеку банку забороняється мати повноваження з розроблення, упровадження, супроводження (адміністрування) та експлуатації інформаційних систем банку, крім тих, що використовуються для забезпечення безпеки інформації.

29. Підрозділу інформаційних технологій (інформатизації, автоматизації) банку забороняється бути власником інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності.

30. Банк зобов'язаний ознайомити працівників під час прийому на роботу з політикою інформаційної безпеки банку. Працівник банку зобов'язаний ознайомитися з політикою інформаційної безпеки банку під підпис та надати зобов'язання про дотримання конфіденційності.

31. Банк зобов'язаний включити до трудового контракту/договору працівника та/або посадової інструкції працівника обов'язки працівника банку щодо виконання вимог із забезпечення безпеки інформації.

32. Банк зобов'язаний ознайомити працівників банку з внутрішніми документами банку, які встановлюють вимоги щодо безпеки інформації. Документи розробляються банком з урахуванням вимог цього Положення. Перелік документів для ознайомлення визначається банком самостійно, з урахуванням принципу мінімального рівня повноважень. Працівник банку зобов'язаний ознайомитися з такими документами під підпис.

33. Банк зобов'язаний упровадити програму підвищення обізнаності/навчання працівників банку з питань безпеки інформації з урахуванням досвіду, отриманого за результатами вирішення інцидентів безпеки інформації.

34. Банк зобов'язаний розробити та затвердити внутрішні документи, які встановлюють вимоги щодо безпеки інформації під час використання змінних носіїв інформації і мають містити положення щодо:

1) контролю за використанням змінних носіїв інформації, уключаючи процедури їх обліку та виведення з експлуатації;

2) категорії інформації, яка може оброблятися на змінних носіях інформації;

3) ідентифікації змінних носіїв інформації, які використовуються в банку;

4) обмежень використання змінних носіїв інформації (у тому числі поза межами банку);

5) знищення інформації на змінних носіях інформації перед їх передаванням у користування іншому працівникові банку, третім сторонам або виведенням з експлуатації;

6) обов'язковості перевірки змінних носіїв інформації на наявність зловмисного коду перед використанням у банку.

35. Банк зобов'язаний здійснити ідентифікацію змінних носіїв інформації за допомогою унікального ідентифікатора, який дозволить визначити тип носія та користувача змінного носія.

36. Банк зобов'язаний розробити та затвердити внутрішні документи, які встановлюють вимоги щодо використання, надання, скасування та контролю доступу до інформаційних систем банку і мають містити:

1) вимоги до ідентифікації, автентифікації, авторизації користувачів;

2) послідовність дій під час управління доступом, у тому числі в разі віддаленого доступу (реєстрація, надання повноважень, перегляд та скасування доступу);

3) перелік типових функцій та прав доступу до інформаційних систем банку;

4) вимоги щодо здійснення заходів контролю доступу, уключаючи контроль за діями привілейованих користувачів;

5) періодичність контролю наданих прав доступу;

6) вимоги до протоколювання дій під час управління доступом.

37. Банк зобов'язаний забезпечити дотримання принципу надання мінімального рівня повноважень під час надання доступу до інформаційних систем банку (уключаючи доступ привілейованих користувачів).

38. В інформаційних системах банку, які безпосередньо забезпечують автоматизацію банківської діяльності, забороняється суміщення в межах однієї функції (ролі) таких повноважень: розроблення та супроводження (адміністрування), розроблення та експлуатація, супроводження (адміністрування) та експлуатація, виконання операцій в таких системах та подальшого контролю за їх виконанням.

39. Банк зобов'язаний запровадити такі заходи контролю доступу до інформаційних систем банку:

1) перевірку наявності у користувача дозволу керівництва та власника інформаційної системи на такий доступ;

2) заборону одноосібного ініціювання заявки, підтвердження та надання доступу;

3) перевірку відповідності рівня наданого доступу принципу мінімально необхідного рівня повноважень;

4) періодичну перевірку відповідності наданих прав доступу користувачеві тим, що діють на момент перевірки.

40. Банк зобов'язаний використовувати механізми багатофакторної автентифікації під час надання доступу для виконання функцій адміністрування або супроводження САБ.

41. Банк зобов'язаний забезпечити блокування облікових записів користувачів в інформаційних системах банку в таких випадках:

1) п'яти невдалих спроб автентифікації поспіль (автоматичне блокування);

2) відсутності реєстрації користувача в інформаційних системах банку протягом 90 календарних днів;

3) звільнення користувача.

42. Банк зобов'язаний здійснювати протоколювання всіх дій щодо надання, скасування чи зміни доступу до інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності, у захищених від несанкціонованої модифікації електронних журналах із забезпеченням їх збереження не менше ніж протягом трьох років.

43. Банк зобов'язаний забезпечити протоколювання, збереження та захист від модифікації інформації про події доступу до інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності, та зберігання її не менше ніж протягом одного року.

44. Банк зобов'язаний розробити та впровадити політику використання криптографічних засобів для захисту інформації, яка має містити:

1) цілі безпеки, для яких використовуються криптографічні заходи безпеки (конфіденційність, цілісність, доступність);

2) положення щодо необхідності та застосування необхідного рівня захисту інформації за допомогою криптографічних засобів залежно від її класифікації за критерієм конфіденційності.

45. Банк зобов'язаний розробити та затвердити документи, що описують процес управління ключами, які мають містити положення щодо:

1) процедури генерації ключів для різних криптографічних систем;

2) розподілу ключів серед відповідальних осіб;

3) зберігання ключів;

4) заміни або оновлення ключів;

5) поводження із скомпрометованими ключами;

6) відкликання ключів;

7) відновлення ключів, які зруйновано;

8) процедури резервного копіювання або архівування ключів;

9) знищення ключів;

10) реєстрації та аудиту діяльності, пов'язаної з управлінням ключами.

46. Банк у разі застосування криптографічного захисту зобов'язаний використовувати криптографічні алгоритми з такого переліку:

1) асиметричні алгоритми:

алгоритм Діффі - Геллмана (далі - алгоритм DH) для узгодження сеансових ключів шифрування;

алгоритм цифрового підпису (далі - алгоритм DSA) для цифрових підписів;

алгоритм Діффі - Геллмана на еліптичних кривих (далі - алгоритм ECDH) для узгодження сеансових ключів шифрування;

алгоритм цифрового підпису на еліптичних кривих (далі - алгоритм ECDSA) для цифрових підписів;

алгоритм Ривест - Шаміра - Адлемана (далі - алгоритм RSA) для цифрових підписів і узгодження сеансових ключів шифрування або аналогічних ключів;

алгоритм цифрового підпису [ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння", затверджений наказом Державного комітету України

з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі - ДСТУ 4145-2002)] для цифрових підписів;

2) алгоритми безпеки гешування SHA-224, SHA-256, SHA-384, SHA-512, "Купина" (ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування", прийнятий наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1431) або більш криптостійкі;

3) алгоритми симетричного шифрування:

алгоритм "Advanced encryption standard" (AES) із використанням довжини ключа 128, 192 і 256 біт або більше;

алгоритм криптографічного перетворення (ДСТУ ГОСТ 28147:2009 "Система оброблення інформації. Захист криптографічний. Алгоритм криптографічного перетворення", прийнятий наказом Державного комітету України з питань технічного регулювання та споживчої політики від 22 грудня 2008 року № 495);

алгоритм "Калина" (ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення", прийнятий наказом Міністерства економічного розвитку і торгівлі України від 29 грудня 2014 року № 1484).

47. Банк, який застосовує алгоритм DH для узгодження сеансових ключів шифрування, зобов'язаний використовувати розмір модуля не менше ніж 2048 біт.

48. Банк, який застосовує алгоритм DSA для цифрових підписів, зобов'язаний використовувати розмір модуля не менше ніж 2048 біт.

49. Банк, який застосовує алгоритм на еліптичних кривих, зобов'язаний використовувати еліптичні криві з ДСТУ 4145-2002 або з Федерального стандарту оброблення інформації (США) (Federal information processing standards, FIPS186-4).

50. Банк, який застосовує алгоритм ECDH для узгодження сеансових ключів шифрування, зобов'язаний використовувати розмір поля/ключа не менший, ніж 160 біт.

51. Банк, який застосовує алгоритми ECDSA, ДСТУ 4145-2002 для цифрових підписів, зобов'язаний використовувати розмір поля/ключа не менший, ніж 160 біт.

52. Банк, який застосовує алгоритм RSA для цифрових підписів і ключів шифрування сеансу або аналогічних ключів, зобов'язаний використовувати розмір модуля не менше ніж 2048 біт.

53. Банк, який застосовує алгоритм RSA для цифрових підписів і ключів шифрування сеансу або аналогічних ключів, зобов'язаний використовувати різні ключові пари для передавання ключів шифрування сеансу (або аналогічних ключів) та для цифрових підписів.

54. Банк зобов'язаний використовувати останню версію протоколу захисту на транспортному рівні та реалізацію цього протоколу, що підтримує безпечне повторне погодження з'єднання для захисту з'єднань, які управляються протоколом Transmission control protocol (TCP). Якщо безпечне повторне погодження з'єднання не підтримується, то ця процедура має бути відключена.

55. Банку забороняється використання анонімного (без автентифікації) алгоритму DH.

56. Банк, який застосовує стандарти для шифрування "Secure multipurpose internet mail extension" (далі - S/MIME), зобов'язаний використовувати цей стандарт не нижче версії 3.0.

57. Банк зобов'язаний використовувати набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу Інтернету (набір протоколів Internet protocol security, IPsec) у режимі ESP (Encapsulating security payload) (якщо банк не використовує криптографічний протокол захисту на транспортному рівні).

58. Банк зобов'язаний використовувати кабелі типу "вита пара" не нижче категорії 5E та/або оптично-волоконні кабелі для організації структурованої кабельної системи (далі - СКС).

59. Банк зобов'язаний забезпечити наявність та актуальність такої документації до СКС:

1) схеми (креслення) розміщення обладнання СКС та кабельних каналів;

2) схеми підключення обладнання СКС;

3) таблиці маркування кабелів СКС та кабельних з'єднань (кабельний журнал).

60. Банк зобов'язаний забезпечити персоналізований та контрольований доступ до комутаційних вузлів СКС.

61. Банк зобов'язаний розробити та затвердити внутрішній документ, який установлює вимоги до забезпечення захисту від зловмисного коду та описує організацію захисту від зловмисного коду в банку, який має містити положення щодо:

1) вимог до безперервного забезпечення захисту від зловмисного коду;

2) вимог до застосування засобів захисту від зловмисного коду, контролю за їх належним функціонуванням та періодичністю оновлення, з обов'язковим визначенням відповідальних осіб;

3) застосування оновлень для засобів захисту від зловмисного коду та баз даних засобів захисту від зловмисного коду на робочих станціях та серверах, що не підключені до мережі банку;

4) опису процедури централізованого розгортання та управління засобами захисту від зловмисного коду;

5) вимог до проведення профілактичних заходів з виявлення зловмисного коду в інформаційних системах банку та їх періодичності.

62. Банк зобов'язаний використовувати виключно актуальні версії ліцензійних засобів захисту від зловмисного коду, для яких не припинено підтримку виробника.

63. Банк зобов'язаний здійснювати централізоване управління захистом від зловмисного коду та забезпечувати можливість:

1) віддаленого встановлення, видалення, оновлення та конфігурації засобів захисту від зловмисного коду;

2) реєстрації всіх подій засобів захисту від зловмисного коду та централізованого зберігання такої інформації (електронних журналів);

3) контролю за наявністю та коректністю роботи агентів засобів захисту від зловмисного коду на робочих станціях та серверах банку.

64. Банк зобов'язаний забезпечити перевірку програмними та/або програмно-апаратними засобами захисту від зловмисного коду:

1) усіх вхідних та вихідних повідомлень корпоративної електронної пошти, уключаючи вкладення до них;

2) усього вхідного Інтернет-трафіку;

3) усіх змінних носіїв інформації, що підключаються до робочих станцій або іншого обладнання інформаційних систем банку.

65. Банк зобов'язаний запровадити заходи, що забезпечують захист від несанкціонованого видалення, відключення та скасування оновлень засобів захисту від зловмисного коду, а також від зміни їх налаштувань та конфігурації.

66. Банк зобов'язаний обробляти факти ураження інформаційних систем банку зловмисним кодом в рамках процесу управління інцидентами безпеки інформації. Банк самостійно визначає критерії віднесення фактів вірусного ураження до інцидентів безпеки інформації.

67. Банк зобов'язаний здійснювати перевірку всіх переносних та/або стаціонарних носіїв інформації засобами захисту від зловмисного коду, які окремо або в складі пристрою були повернуті після їх використання третіми сторонами.

68. Банк зобов'язаний зберігати електронні журнали роботи засобів захисту від зловмисного коду не менше ніж три місяці.

69. Банк зобов'язаний використовувати операційні системи, для яких не припинено підтримку виробника та які забезпечують можливість:

1) ідентифікації та автентифікації всіх користувачів операційної системи;

2) розмежування доступу користувачів операційної системи;

3) реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою.

70. Банк зобов'язаний використовувати офіційні стабільні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника.

71. Банк зобов'язаний визначити стандартне еталонне джерело часу та забезпечити синхронізацію з ним операційних систем.

72. Банк зобов'язаний забезпечити блокування або перейменування облікових записів користувачів операційних систем, що встановлюються за замовчуванням, та відключення гостьових облікових записів. Банк зобов'язаний заблокувати вбудовані облікові записи локального адміністратора операційних систем або (якщо немає технічної можливості на

рівні фунціоналу операційної системи) перейменувати такі вбудовані облікові записи та змінювати їх пароль не рідше ніж один раз на 30 діб.

73. Банк зобов'язаний забезпечити автоматичне блокування робочого стола операційної системи на робочій станції або сервері, якщо немає активності користувача протягом 15 хвилин, з наступною повторною автентифікацією користувача під час розблокування (за винятком робочих станцій або серверів, на яких блокування неможливе або потребує більшого інтервалу часу відсутності активності за технологією використання).

74. Банк зобов'язаний забезпечити централізоване розповсюдження налаштувань параметрів безпеки та інших параметрів конфігурації операційних систем (наприклад, за допомогою використання групових політик контролера домену "Active Directory").

75. Банк зобов'язаний створити та підтримувати в актуальному стані перелік програмного забезпечення, що використовується в банку (в електронному або паперовому вигляді).

76. Банк зобов'язаний забезпечити блокування можливості здійснення працівниками банку, яким не надано адміністративних прав у операційних системах, таких дій (налаштувань):

1) самостійного встановлення програмного забезпечення, яке не внесено до переліку програмного забезпечення, що використовується в банку;

2) автоматичного запуску програм із зовнішніх пристроїв та носіїв інформації;

3) самостійного видалення встановленого програмного забезпечення, оновлень безпеки.

77. Банк зобов'язаний розробити та затвердити внутрішні документи, які містять опис процесу управління оновленнями (описи дій щодо отримання, тестування, розповсюдження та застосування оновлень операційних систем, прикладного програмного забезпечення та драйверів). Процес управління оновленнями має містити такі стадії:

1) підготовка тестового середовища (тестових клієнтів);

2) підготовка переліку оновлень;

3) застосування оновлень в тестовому середовищі;

4) застосування оновлень на пілотній групі користувачів;

5) застосування протестованих оновлень.

78. Банк зобов'язаний здійснювати налаштування програмного забезпечення систем управління базами даних (далі - СУБД) для роботи під окремим обліковим записом з дотриманням принципу надання мінімального рівня повноважень (необхідних для виконання функцій СУБД).

79. Банк зобов'язаний забезпечити блокування облікових записів адміністраторів СУБД, установлених за замовчуванням (або зміну їх паролів) та використання облікових записів адміністраторів СУБД виключно для вирішення адміністративних завдань.

80. Банк зобов'язаний забезпечити видалення/блокування неперсоналізованих і гостьових облікових записів користувачів СУБД та персоналізацію технологічних облікових записів СУБД.

81. Банк зобов'язаний забезпечити фізичне або віртуальне функціональне розділення серверів СУБД та серверів застосувань інформаційних систем банку.

82. Банк зобов'язаний розміщувати сервери баз даних в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана.

83. Банк зобов'язаний визначити привілейовані облікові записи для інформаційних систем банку, мережевого обладнання та серверів. Привілейовані облікові записи надаються користувачам згідно з внутрішніми документами банку, що встановлюють вимоги до використання, надання, скасування та контролю доступу до інформаційних систем банку.

84. Банк зобов'язаний забезпечити розташування робочих станцій, з яких виконуються дії щодо адміністрування та супроводження інформаційних систем банку, мережевого обладнання та серверів банку, використовуючи привілейовані облікові записи, в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана.

85. Банк зобов'язаний забезпечити надання доступу до портів адміністрування та супроводження інформаційних систем, мережевого обладнання та серверів банку виключно з IP-адрес (робочих станцій), які визначені банком для адміністрування та супроводження таких систем або обладнання.

86. Банк зобов'язаний забезпечити використання адміністраторами інформаційних систем банку, мережевого обладнання та серверів банку облікових записів без привілейованих повноважень для автентифікації на робочих станціях, які визначені банком для адміністрування та супроводження таких систем чи обладнання.

87. Банк зобов'язаний забезпечити використання виключно персоналізованих облікових записів для виконання адміністрування чи супроводження інформаційних систем банку, мережевого обладнання та серверів.

88. Банк зобов'язаний визначити та запровадити посилені вимоги щодо парольної політики для привілейованих облікових записів (довжина та складність паролів, частота зміни) або застосовувати багатофакторну автентифікацію для таких облікових записів.

89. Банк зобов'язаний забезпечити централізоване управління мережею банку (єдине місце управління). Банк має право здійснювати локальне управління мережею банку на різних вузлах за умови централізованого управління такими функціями:

1) вибір і монтаж кабельної системи мережі;

2) підбір комутаційного обладнання мережі;

3) підбір обладнання, що підключається до мережі банку, операційних систем, програмного забезпечення інформаційних систем банку, прикладного програмного забезпечення;

4) управління мережевими адресами та ідентифікаторами обладнання і користувачів;

5) розподіл мережі на сегменти.

90. Банк зобов'язаний забезпечити підтримання в актуальному стані документації мережі банку (в електронному та/або паперовому вигляді), документування всіх змін у конфігурації мережі банку та зберігання попередніх версій документації мережі строком не менше ніж один рік. Документація мережі банку має бути погоджена відповідальною особою за інформаційну безпеку банку та містити:

1) фізичну схему мережі, уключаючи бездротові мережі, що відображає всі з'єднання в мережі;

2) логічну схему мережі, уключаючи бездротові мережі, що відображає всі мережеві пристрої, критично важливі сервери та сервіси;

3) конфігурацію мережевого обладнання, уключаючи бездротові мережі.

91. Банк зобов'язаний задокументувати порядок контролю змін у конфігурації мережі, у якому мають зазначатися вимоги щодо перегляду конфігурації мережі не рідше ніж один раз на рік з документуванням результатів перегляду.

92. Банк зобов'язаний здійснити розподіл мережі банку на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів.

93. Банк зобов'язаний забезпечити ідентифікацію обладнання (наприклад, за ідентифікатором управління доступом до обладнання, MAC-адреса), що підключається до мережі банку, та вжиття заходів, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації.

94. Банк зобов'язаний забезпечити програмне відключення портів на активних мережевих пристроях мережі банку, які не використовуються.

95. Банку забороняється використовувати облікові записи та паролі за замовчуванням на активних мережевих пристроях, які підключені до мережі банку.

96. Банку забороняється використовувати протокол Інтернету версії 6 (IPv6) у мережі банку.

97. Банку забороняється використовувати версії 1 або 2 простого протоколу керування мережею (Simple network management protocol, SNMP) для управління пристроями в мережі.

98. Банк зобов'язаний забезпечити синхронізацію всіх активних мережевих пристроїв з еталонним джерелом часу банку.

99. Банк зобов'язаний розробити та впровадити заходи безпеки інформації у разі використання бездротових мереж передавання даних (далі - бездротові мережі).

100. Банк зобов'язаний розмістити бездротові мережі банку в окремій зоні безпеки мережі банку (сегмент або набір сегментів мережі зі спільним рівнем безпеки) та розмежувати доступ із зони безпеки бездротових мереж до мережі банку з використанням міжмережевих екранів.

101. Банк зобов'язаний встановити ідентифікатори бездротових мереж (SSID), відмінні від встановлених виробником або інсталятором обладнання за замовчуванням. Банк зобов'язаний відключити трансляцію ідентифікаторів бездротових мереж (окрім бездротової мережі, призначеної для гостьових підключень).

102. Банк зобов'язаний забезпечити використання в бездротових мережах банку режиму безпеки WPA2-Enterprise (корпоративний режим у наборі алгоритмів і протоколів Wireless protected access версії 2) та використання режиму безпеки WPA2-Personal (персональний режим у наборі алгоритмів і протоколів Wireless protected access версії 2) для реалізації гостьових підключень.

103. Банк зобов'язаний застосовувати такі заходи безпеки інформації для організації віддаленого доступу до інформаційних систем банку:

1) розміщення сервера (серверів) віддаленого доступу до інформаційних систем банку в демілітаризованій зоні (DMZ) мережі банку, з обмеженням доступу до нього з публічної мережі за допомогою міжмережевого екрана або пристрою уніфікованого управління загрозами;

2) шифрування каналів зв'язку для доступу до сервера віддаленого доступу до інформаційних систем банку;

3) багатофакторна автентифікація користувачів.

104. Банк зобов'язаний забезпечити розмежування доступу між мережею банку і публічною мережею з використанням міжмережевих екранів та/або пристроїв уніфікованого управління загрозами.

105. Банк зобов'язаний обробляти виявлені атаки або вторгнення до мережі банку в рамках процесу управління інцидентами безпеки інформації. Банк самостійно визначає критерії віднесення таких атак або вторгнень до інцидентів безпеки інформації.

106. Банк зобов'язаний забезпечити доступ з публічної мережі до мережі банку виключно із застосуванням захищених з'єднань.

107. Банк зобов'язаний забезпечити розміщення в демілітаризованій зоні мережі банку серверів та обладнання, що забезпечує функціонування сервісів або банківських продуктів, які відкриті для доступу клієнтів з публічної мережі. З'єднання серверів та обладнання, що розміщено в демілітаризованій зоні, з серверами та обладнанням мережі банку захищаються міжмережевим екраном.

108. Банк зобов'язаний виконувати перевірку ефективності заходів щодо захисту периметра мережі банку шляхом виконання періодичних тестів на проникнення.

109. Національний банк визначає інформаційні задачі, у яких для забезпечення застосування електронного цифрового підпису обов'язковим є використання послуг електронного цифрового підпису від акредитованих центрів сертифікації ключів (далі - акредитовані ЦСК).

110. У випадках отримання послуг електронного цифрового підпису від зареєстрованих центрів сертифікації ключів (далі - зареєстровані ЦСК) взаємне визнання електронного цифрового підпису між учасниками електронної взаємодії визначається договірними

засадами. Крім того, у договорі обов'язково мають обумовлюватися права, обов'язки та відповідальність сторін, розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам, порядок вирішення спорів у разі їх виникнення.

111. Акредитовані ЦСК та зареєстровані ЦСК зобов'язані здійснювати свою діяльність відповідно до регламенту роботи, що визначає організаційно-методологічні та технологічні умови його діяльності в процесі надання послуг електронного цифрового підпису підписувачам. Регламент роботи ЦСК має бути розроблений та погоджений відповідно до вимог чинного законодавства.

112. Банк зобов'язаний розробити та затвердити внутрішні документи, які встановлюють вимоги щодо безпеки інформації, технічного обслуговування, експлуатації факсимільних апаратів, багатофункціональних пристроїв, телефонів та/або телефонних систем та мають містити такі положення щодо:

1) функцій та обов'язків персоналу банку стосовно підключення, технічного обслуговування та експлуатації систем та пристроїв зв'язку;

2) категорій інформації за критерієм конфіденційності, що може передаватися пристроями зв'язку;

3) обов'язковості очищення оперативної та постійної пам'яті факсимільних апаратів і багатофункціональних пристроїв перед передаванням їх третім сторонам або перед виведенням з експлуатації.

113. Банк зобов'язаний створити та підтримувати в актуальному стані перелік факсимільних апаратів і багатофункціональних пристроїв (в електронному або паперовому вигляді), який містить унікальні ідентифікатори обладнання та місце його розташування.

114. Банк зобов'язаний ознайомити своїх працівників із документами, які встановлюють вимоги щодо безпеки інформації, технічного обслуговування та експлуатації факсимільних апаратів, багатофункціональних пристроїв для друку, телефонів та/або телефонних систем.

115. Банк зобов'язаний розміщувати обладнання телефонної мережі (сервери, комутаційне та абонентське обладнання) в окремому сегменті мережі банку, захищеному за допомогою міжмережевого екрана.

116. Банк зобов'язаний запровадити такі заходи безпеки в разі використання телефонного зв'язку на основі протоколу Інтернет (IP-телефонії):

1) активувати вбудовані алгоритми шифрування трафіку між шлюзами, які забезпечують роботу телефонної системи банку, або між шлюзом та кінцевим абонентським обладнанням (телефоном);

2) здійснювати розподіл унікальних ідентифікаторів мережевого рівня (IP-адрес) у телефонній мережі банку відповідно до стандарту RFC 1918 "Розподіл адрес у приватних IP-мережах".

117. Банк зобов'язаний розробити та затвердити документ щодо використання електронної пошти, який має містити положення щодо:

1) обмежень під час пересилання інформації банку;

2) категорії інформації, яка може надсилатись засобами електронної пошти;

3) обмежень використання сторонніх сервісів електронної пошти, які не пов'язані з виконанням функціональних обов'язків персоналом банку.

118. Банк зобов'язаний розробити та впровадити заходи безпеки інформації для сервера електронної пошти, які включають:

1) додаткові заходи безпеки операційної системи, на якій встановлено сервер застосувань електронної пошти;

2) заходи безпеки сервера застосувань електронної пошти;

3) налаштування правил доступу до сервера електронної пошти.

119. Банк зобов'язаний забезпечити перевірку програмними або апаратними засобами захисту всіх повідомлень, що обробляються сервером застосувань електронної пошти, на наявність зловмисного коду.

120. Банк зобов'язаний впровадити періодичне тестування захищеності та перегляд налаштувань параметрів безпеки операційної системи сервера застосувань електронної пошти та безпосередньо сервера застосувань електронної пошти.

121. Банк зобов'язаний розміщувати сервер застосувань електронної пошти на окремому фізичному або віртуальному сервері.

122. У разі використання віддаленого доступу до сервера застосувань електронної пошти банк зобов'язаний запровадити такі заходи безпеки інформації:

1) сервер має бути розміщений в демілітаризованій зоні мережі банку з обмеженням доступу до нього з публічної мережі за допомогою міжмережевого екрана або пристрою уніфікованого управління загрозами;

2) доступ до сервера електронної пошти має надаватись лише шифрованими каналами зв'язку.

123. Банк зобов'язаний запровадити такі заходи безпеки інформації для сервера електронної пошти:

1) використовувати міжмережевий екран операційної системи сервера електронної пошти для обмеження доступу до сервера;

2) заблокувати отримання вхідних повідомлень від серверів мережі Інтернет, що розсилають спам;

3) упровадити процес постійного моніторингу вразливостей сервера застосувань електронної пошти та клієнтського програмного забезпечення доступу до сервера застосувань електронної пошти, забезпечити встановлення відповідних оновлень, що усувають виявлені вразливості.

124. Банк зобов'язаний визначити та задокументувати вимоги безпеки інформації для інформаційних систем банку під час їх розроблення, модернізації (у тому числі їх компонентів) або в разі придбання.

125. На стадії розроблення і тестування інформаційних систем банку та/або їх компонентів банк зобов'язаний використовувати тестову програмно-апаратну платформу, яка підключена до окремого (тестового) виділеного сегмента мережі банку. Як тестові дані банк має право використовувати виключно знеособлені дані.

126. Банк зобов'язаний розробити документацію для інформаційних систем банку та/або їх компонентів з обов'язковим описом реалізованих в інформаційних системах банку організаційних та технічних заходів безпеки інформації, якщо така документація не надана розробником інформаційних систем банку.

127. Банк зобов'язаний на стадії експлуатації інформаційних систем задокументувати положення щодо:

1) контролю функціонування реалізованих в інформаційних системах банку заходів безпеки інформації, уключаючи контроль реалізації організаційних заходів та контроль складу і параметрів налагодження технічних засобів безпеки інформації;

2) контролю вразливостей в обладнанні та програмному забезпеченні інформаційних систем банку;

3) контролю конфігурації програмного забезпечення інформаційних систем банку;

4) відновлення всіх реалізованих заходів щодо забезпечення безпеки інформації в інформаційних системах банку після збоїв у роботі внаслідок інцидентів безпеки інформації.

128. Банк зобов'язаний визначити функції та обов'язки, пов'язані з експлуатацією інформаційних систем і впроваджених в них заходів безпеки інформації, уключаючи внесення змін до параметрів їх налаштування.

129. Банк зобов'язаний задокументувати та впровадити порядок виведення з експлуатації обладнання інформаційних систем банку, який має містити опис процесу видалення інформації з таких систем, використовуючи алгоритми та/або методи, що забезпечать неможливість її відновлення.

130. Банк зобов'язаний упровадити процес управління інцидентами безпеки інформації та розробити і затвердити документи, які містять описи дій стосовно:

1) виявлення інцидентів;

2) інформування про інциденти, у тому числі відповідальної особи за інформаційну безпеку, підрозділу з безпеки інформації та працівників банку;

3) класифікації інцидентів та оцінки негативного впливу (збитку), нанесеного банку інцидентом;

4) реагування на інциденти;

5) аналізу причин, що призвели до інцидентів та оцінки результатів реагування на інциденти;

6) зберігання інформації щодо інцидентів, аналізу інцидентів та результатів реагування на інциденти.

131. Банк зобов'язаний визначити в посадових інструкціях працівників банку або організаційно-розпорядчих документах банку особисті функції та обов'язки з виявлення, класифікації, реагування і аналізу інцидентів безпеки інформації.

132. Банк зобов'язаний забезпечити документування інформації щодо інцидентів безпеки інформації та її зберігання не менше ніж один рік.

V. Додаткові заходи безпеки інформації

133. Банку забороняється використовувати радіотелефони та/або радіоподовжувачі телефонної лінії без активованих у них алгоритмів шифрування сигналу, який передається радіоканалом.

134. Банк зобов'язаний створити та підтримувати в актуальному стані (в електронному або паперовому вигляді) перелік змінних носіїв інформації банку.

135. Банк зобов'язаний використовувати виключно ідентифіковані змінні носії інформації в інформаційних системах банку.

136. Банк зобов'язаний автоматизувати процес контролю за використанням змінних носіїв інформації в інформаційних системах банку. Банк має право самостійно визначати методи та засоби (технології) автоматизації такого процесу.

137. Банк зобов'язаний використовувати централізовані системи управління обліковими записами.

138. Банк зобов'язаний використовувати інструменти централізованого моніторингу та застосування оновлень безпеки для операційних систем.

139. Банк зобов'язаний автоматизувати процес управління інцидентами безпеки інформації. Банк має право самостійно визначати методи та засоби (технології) автоматизації такого процесу.

140. Банк зобов'язаний використовувати досконалу пряму секретність (Perfect forward secrecy, PFS) для з'єднань на основі протоколу захисту на транспортному рівні.

141. Банк зобов'язаний здійснювати маркування та документування елементів СКС відповідно до рекомендацій міжнародного стандарту ANSI/TIA/EIA-606.

142. Банк зобов'язаний застосовувати комбінацію програмних та програмно-апаратних засобів захисту від зловмисного коду (наприклад, використання програмних антивірусних засобів на робочих станціях і серверах та використання систем запобігання несанкціонованому доступу до мережі на зовнішньому периметрі мережі банку).

143. Банк зобов'язаний використовувати стандарти, документи та настанови відкритого проекту захисту веб-додатків "Open web application security project" (OWASP) для розроблення безпечних веб-додатків.

144. Банк зобов'язаний забезпечити шифрування каналів передавання даних між серверами СУБД і серверами застосувань або шифрування даних, що передаються між серверами СУБД і серверами застосувань банку.

145. Банк зобов'язаний здійснити функціональний розподіл серверів банку на мережевому рівні та забезпечити між ними мінімально необхідний зв'язок, що дозволить працювати серверам незалежно один від одного.

146. Банк зобов'язаний використовувати проміжний сервер для виконання функцій адміністрування чи супроводження інформаційних систем банку, мережевого обладнання та серверів. Підключення до такого сервера має здійснюватися з використанням непривілейованих облікових записів, а підключення з проміжного сервера до інформаційних систем банку, мережевого обладнання та серверів - із використанням привілейованих облікових записів. Банк має право застосовувати альтернативні технології щодо управління та контролю доступом, які виключають прямий доступ привілейованих користувачів (адміністраторів) до інформаційних систем банку, мережевого обладнання та серверів.

147. Банк зобов'язаний використовувати механізми багатофакторної автентифікації під час надання доступу до САБ.

148. Банк зобов'язаний упровадити системи виявлення несанкціонованого доступу до мережі (Intrusion detection system, IDS) та системи запобігання несанкціонованому доступу до мережі (Intrusion prevention system, IPS) для захисту периметра мережі банку.

149. Банк зобов'язаний застосувати заходи безпеки для захисту від атак на відмову в обслуговуванні та/або розподілених атак на відмову в обслуговуванні (DoS/DDoS-атак) на зовнішньому периметрі мережі банку. Банк самостійно визначає методи та засоби (технології) захисту від такого типу атак.

150. Банк зобов'язаний використовувати сертифікати відкритих ключів, отримані в акредитованих/зареєстрованих ЦСК для ідентифікації та автентифікації, забезпечення конфіденційності інформації під час інформаційного обміну між інформаційними системами банку та Національного банку.

Директор
Департаменту безпеки **О.А. Скомаровський**

ПОГОДЖЕНО

В.о. Голови Національного банку України Я.В. Смолій

Постійна адреса:
https://zakon.rada.gov.ua/go/v0095500-17

Публікації документа

- **Офіційне інтернет-представництво Національного банку України** від 04.10.2017
- **Офіційний вісник України** від 27.10.2017 — 2017 р., № 84, стор. 52, стаття 2575, код акта 87649/2017