

ПУБЛІЧНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «КОМЕРЦІЙНИЙ БАНК «АКОРДБАНК»

ЗАТВЕРДЖЕНО

**рішенням Наглядової ради
протокол №20230116001
від «16» січня 2023 р.**

ОЗНАЙОМЛЕНИЙ

«11» січня 2023 р.

Голова Правління

ПОЛОЖЕННЯ

про підрозділ внутрішнього аудиту (Управління внутрішнього аудиту)

ПУБЛІЧНОГО АКЦІОНЕРНОГО ТОВАРИСТВА «КОМЕРЦІЙНИЙ БАНК «АКОРДБАНК»

м. Київ - 2023

1. ЗАГАЛЬНА ЧАСТИНА

1.1. ТЕРМІНИ ТА СКОРОЧЕННЯ за текстом цього Положення:

НБУ - Національний банк України;

ЗОВНІШНІ ОРГАНІЗАЦІЇ - зовнішній аудитор, органи державної влади й управління, у тому числі НБУ, які в межах своєї компетенції здійснюють нагляд за діяльністю Банку;

Банк - ПУБЛІЧНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «КОМЕРЦІЙНИЙ БАНК «АКОРДБАНК»»;

Рада - Наглядова Рада Банку;

УПРАВЛІННЯ - Управління внутрішнього аудиту Банку;

структурні підрозділи - структурні підрозділи Банку, у тому числі відокремлені, що забезпечують надання банківських та інших фінансових послуг;

НПА - нормативно-правові акти Національного банку України;

ЗАКОНОДАВСТВО - чинне законодавство України, у тому числі НПА НБУ;

НПА №311 - " Положення про організацію внутрішнього аудиту в банках України ", затверджене постановою Правління НБУ (за текстом - ПП НБУ) від 10.05.2016 №311 (або інший документ йому на зміну);

НПА №88 - «Положення про організацію системи внутрішнього контролю в банках України та банківських групах», затверджене ПП НБУ від 02.07.2019 №88 (або інший документ йому на зміну);

НПА №149 - «Положення про ліцензування банків», затверджене ПП НБУ від 22.12.2018 №149, п.43.

МСВА, НОРМИ ЕТИКИ АУДИТОРІВ (міжнародні стандарти професійної практики внутрішнього аудиту, загальні етичні норми) - документи (вимоги), прийняті Радою з Міжнародних Стандартів внутрішнього аудиту (International Internal Audit Standards Board - IIASB) та схвалені Наглядовою Радою Професійної Практики (International Professional Practices framework oversight council - IPPFOS), які визначають *загальні принципи (процедури), принципи етики та правила поведінки*, яких у своїй діяльності мають дотримуватися підрозділи внутрішнього аудиту банків під час виконання своїх функцій;

Інші терміни, що вживаються в цьому Положенні, застосовуються в значеннях, визначених законодавчими та нормативно-правовими актами України.

1.2. Це Положення розроблено відповідно до вимог Закону України “Про банки і банківську діяльність”, НПА №311 та Статуту Банку, при цьому враховані норми МСВА та ЕТИКИ АУДИТОРІВ.

1.3. Це Положення визначає організаційну структуру, підпорядкування та підзвітність, задачі, функції *підрозділу внутрішнього аудиту Банку*, в якості якого Банком створено Управління внутрішнього аудиту.

1.4. Правове положення, завдання, обов’язки, права, кваліфікаційні вимоги, вимоги до об’єму та рівня професійних знань, відповідальність за виконання покладених функцій начальника УПРАВЛІННЯ визначаються, в тому числі, у цьому Положенні, яке одночасно **виконує функцію Посадової інструкції начальника УПРАВЛІННЯ**.

1.5. УПРАВЛІННЯ діє на підставі цього Положення.

При здійсненні своєї діяльності працівники УПРАВЛІННЯ керуються:

- вимогами ЗАКОНОДАВСТВА, в тому числі керуються вимогами НПА НБУ, *який визначає вимоги щодо здійснення аудиторської перевірки (аудиту) дотримання банком вимог законодавства у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення;*

- нормами МСВА, ЕТИКИ АУДИТОРІВ, а також Кодексом етики Банку;

- Статутом і рішеннями Загальних зборів акціонерів Банку, Ради, Правління та Голови Правління Банку, а також іншими внутрішніми нормативними та організаційно-розпорядчими документами Банку.

Стосовно всього, що не передбачено цим Положенням, УПРАВЛІННЯ керується вищезазначеними (п.1.2, п.1.5) НПА та іншими документами, які регулюють діяльність внутрішнього аудиту в банках.

1.6. УПРАВЛІННЯ здійснює свою діяльність з дотриманням принципів безперервності, незалежності, об’єктивності і неупередженості, професійної компетентності, належної професійної ретельності та етики.

1.7. За організацію ефективної роботи УПРАВЛІННЯ несуть відповідальність Голова Банку та начальник УПРАВЛІННЯ.

Рада Банку забезпечує ефективне функціонування УПРАВЛІННЯ. Рада та Правління Банку мають забезпечити УПРАВЛІННЯ усіма необхідними фінансовими та іншими ресурсами для виконання поставлених перед УПРАВЛІННЯМ завдань, в т.ч. достатніми ресурсами для виконання річного плану проведення аудиторських перевірок (аудиту).

1.8. Це Положення є обов'язковим до виконання не тільки працівниками УПРАВЛІННЯ (внутрішніх аудиторів), але і всіма працівниками Банку.

2. ОРГАНІЗАЦІЙНА СТРУКТУРА, СТАТУС, ПІДПОРЯДКУВАННЯ УПРАВЛІННЯ ТА ЗАБЕЗПЕЧЕННЯ ЙОГО НЕЗАЛЕЖНОСТІ І ОБ'ЄКТИВНОСТІ

2.1. УПРАВЛІННЯ є самостійним структурним підрозділом Банку, який підпорядковується та є підзвітним Раді Банку.

2.2. УПРАВЛІННЯ в своїй діяльності є незалежним від інших підрозділів та від Правління Банку.

2.3. Організаційний статус УПРАВЛІННЯ забезпечує його незалежність, можливість вільного та об'єктивного виконання покладених на нього обов'язків, надання справедливих та неупереджених висновків щодо результатів перевірок, їх адекватний розгляд та прийняття відповідних рішень.

2.4. Організаційна структура УПРАВЛІННЯ затверджується Радою Банку ^{ПРИМ. 2.4}. До складу УПРАВЛІННЯ входять:

- Відділ виїзного аудиту,
- Відділ безвиїзного аудиту.

Очолює і організовує роботу УПРАВЛІННЯ начальник УПРАВЛІННЯ.

2.5. Штатний розклад УПРАВЛІННЯ затверджується ^{ПРИМ. 2.4} в порядку, передбаченому діючим ЗАКОНОДАВСТВОМ, Статутом та відповідними внутрішніми документами Банку, за умови дотримання вимог п.2.7 цього Положення.

Скорочення чисельності штату УПРАВЛІННЯ має бути оформлено відповідним рішенням Ради Банку.

2.6. Рішення щодо прийому до штату УПРАВЛІННЯ кандидата на вакантну посаду приймає начальник УПРАВЛІННЯ - у разі професійної відповідності кандидата вакантній посаді та за умови позитивних висновків Підрозділу безпеки Банку і Підрозділу контролю за дотриманням норм (компласнс).

Оцінку професійної відповідності кандидата вакантній посаді, а працівників УПРАВЛІННЯ - посадам, які вони займають, може проводити тільки начальник УПРАВЛІННЯ.

2.7. Умови оплати праці начальника та працівників УПРАВЛІННЯ, не зазначені в цьому Положенні, затверджуються окремими рішеннями Ради Банку.

Умови оплати праці працівників УПРАВЛІННЯ мають формуватися таким чином, щоб не створювати конфлікту інтересів, не ставити під загрозу незалежність та об'єктивність діяльності УПРАВЛІННЯ, а також сприяти комплектуванню УПРАВЛІННЯ професійно придатними та кваліфікованими працівниками.

У разі прийняття Правлінням Банку рішення щодо покращання соціальних гарантій та пільг працівників всіх підрозділів Банку на рівних умовах, вказане рішення не потребує додаткового затвердження Радою Банку, в частині розповсюдження вказаних гарантій та пільг на працівників УПРАВЛІННЯ.

2.8. Працівники УПРАВЛІННЯ працюють відповідно до цього Положення, інших документів УПРАВЛІННЯ, які регламентують порядок проведення внутрішнього аудиту в Банку, а також відповідно до їх посадових інструкцій.

Для начальника УПРАВЛІННЯ роль посадової інструкції виконує це Положення, посадові інструкції інших працівників УПРАВЛІННЯ розробляються на підставі норм чинного ЗАКОНОДАВСТВА з урахуванням норм цього Положення та затверджуються начальником УПРАВЛІННЯ.

2.9. Начальник УПРАВЛІННЯ оцінює повноту та якість виконання посадових обов'язків працівниками УПРАВЛІННЯ.

2.10. Дисциплінарні стягнення до працівників УПРАВЛІННЯ застосовуються на підставі відповідного наказу/розпорядження Голови Правління Банку за узгодженням з начальником УПРАВЛІННЯ.

У разі наявності з боку начальника УПРАВЛІННЯ заперечень проти наміру застосувати дисциплінарне стягнення до працівників УПРАВЛІННЯ, це питання надається на розгляд Ради Банку.

Рішення щодо застосування дисциплінарного стягнення до начальника УПРАВЛІННЯ приймається виключно Радою Банку.

2.11. УПРАВЛІННЯ самостійно розробляє внутрішні методичні та організаційні документи стосовно методології, технології здійснення перевірок та інших контрольних заходів внутрішнього аудиту для їх

^{ПРИМ. 2.4} За поданням начальника УПРАВЛІННЯ, з огляду на розмір Банку (обсяг активів, кількість структурних підрозділів Банку, рівень програмного забезпечення, яке підтримує діяльність Банку, у тому числі операційний день Банку, тощо), види його діяльності, рівень ризиків, на які може наражатися Банк у процесі своєї діяльності.

наступного затвердження начальником УПРАВЛІННЯ і не має їх узгоджувати з іншими підрозділами Банку.

2.12. Працівники УПРАВЛІННЯ не повинні входити (функціонально) до складу інших структурних підрозділів Банку. Начальнику УПРАВЛІННЯ забороняється займати посади в інших банках.

2.13. Працівники УПРАВЛІННЯ, які раніше займали посади в інших структурних підрозділах Банку, не можуть здійснювати аудит в тій області, за яку відповідали протягом періоду, що підлягає перевірці, та протягом 12 місяців після завершення такої діяльності.

Працівник УПРАВЛІННЯ не може здійснювати аудит також у випадку, якщо стало відомо щодо його наміру (прийнято рішення) найближчим часом зайняти вакантну посаду у підрозділі, діяльність якого підлягає перевірці.

2.14. УПРАВЛІННЯ не може бути задіяне у процесі надання банківських та інших фінансових послуг, здійсненні іншої діяльності Банку, які підлягають внутрішньому аудиту, або у визначенні чи реалізації заходів із створення в Банку адекватної системи внутрішнього контролю.

2.15. Працівники УПРАВЛІННЯ не можуть брати участі в створенні та організації, у тому числі разом із структурними підрозділами Банку, будь-яких заходів та процесів, що забезпечують діяльність Банку або сприймаються як такі, що впливають на неупередженість та об'єктивність внутрішніх аудиторів, розробленні внутрішніх документів Банку (крім випадків надання внутрішніми аудитором консультативних послуг, які передбачені функцією внутрішнього аудиту), візувати такі документи.

2.16. Об'єктивність висновків внутрішніх аудиторів УПРАВЛІННЯ досягається, крім іншого, і за рахунок періодичної **ротації внутрішніх аудиторів**, яка може здійснюватися за наступними напрямками (правило ротації):

- внутрішній аудитор може керувати групою, яка проводить внутрішній аудит, або проводити перевірку самостійно одного й того самого об'єкту аудиту не частіше 2х разів поспіль;

- один й той самий склад групи може проводити внутрішній аудит одного й того самого об'єкту аудиту за умови зміни керівника групи перевірки або за умови виконання членами групи перевірки інших питань програми аудиту, ніж ті, що вони виконували попереднього разу.

У будь-якому випадку начальник УПРАВЛІННЯ має право скасувати правило ротації, якщо застосування ротації може загрожувати якості проведення внутрішнього аудиту.

2.17. ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВНУТРІШНЬОГО АУДИТУ, ВИМОГИ ДО ПРОГРАМИ ЗАБЕЗПЕЧЕННЯ ТА ПІДВИЩЕННЯ ЯКОСТІ ВНУТРІШНЬОГО АУДИТУ БАНКУ, ОЦІНКА ЕФЕКТИВНОСТІ ТА ЯКОСТІ РОБОТИ УПРАВЛІННЯ.

2.17.1. Якість діяльності УПРАВЛІННЯ підлягає постійному моніторингу з боку начальника УПРАВЛІННЯ.

2.17.2. Начальник УПРАВЛІННЯ розробляє і щороку актуалізує *Програму гарантії та підвищення якості діяльності УПРАВЛІННЯ*, яка охоплює всю діяльність УПРАВЛІННЯ, визначену цим Положенням.

2.17.3. *Програма гарантії та підвищення якості діяльності УПРАВЛІННЯ* визначає інструменти постійного моніторингу якості діяльності УПРАВЛІННЯ і включає *внутрішні* і *зовнішні* оцінки діяльності УПРАВЛІННЯ, а також визначає напрямки розвитку компетенцій та навичок працівників УПРАВЛІННЯ у звітному році.

2.17.4. Реалізація *Програми гарантії та підвищення якості діяльності УПРАВЛІННЯ* здійснюється під безпосереднім контролем начальника УПРАВЛІННЯ.

2.17.5. За підсумком звітнього року начальник УПРАВЛІННЯ надає Правлінню та Раді Банку звіт щодо результатів реалізації у році, що минув, розробленої УПРАВЛІННЯМ на звітний рік *Програми гарантії та підвищення якості діяльності УПРАВЛІННЯ*. Структура та формат такого звіту визначаються начальником УПРАВЛІННЯ та мають забезпечити достатню ступінь інформативності та об'єктивності.

2.17.6. Оцінка ефективності та якості роботи УПРАВЛІННЯ забезпечується шляхом проведення *внутрішньої* та *зовнішньої* оцінок.

Внутрішня оцінка проводиться шляхом:

- поточного моніторингу начальником УПРАВЛІННЯ якості функції внутрішнього аудиту;
- щорічного розгляду та затвердження Радою Банку Звіту про роботу УПРАВЛІННЯ за звітний рік;

- щорічного проведення самооцінки діяльності УПРАВЛІННЯ у звітному році та періодичного (не рідше 1 разу на 3 роки) проведення самооцінки діяльності УПРАВЛІННЯ на відповідність МСВА;

- оцінки з боку Ради Банку матеріалів самооцінки УПРАВЛІННЯ шляхом їх розгляду та, у разі необхідності, - затвердження відповідного плану заходів за результатами самооцінки.

2.17.7. Відповідно до МСВА, діяльність УПРАВЛІННЯ також підлягає **зовнішній оцінці**. Періодичність оцінки визначена ЗАКОНОДАВСТВОМ ¹ раз в ⁵ років. Формат проведення зовнішньої оцінки обговорюється начальником УПРАВЛІННЯ, Головою Правління, Радою і затверджується рішенням Ради. Результати оцінки надаються Раді і Голові Правління Банку.

3. ЗВІТНІСТЬ УПРАВЛІННЯ ТА ЙОГО ПРАЦІВНИКІВ, ПОРЯДОК ДОВЕДЕННЯ РЕЗУЛЬТАТІВ АУДИТУ ДО РАДИ ТА ПРАВЛІННЯ БАНКУ

3.1. Звітність УПРАВЛІННЯ.

періодичність	адресати звітності			зміст звітності
	РАДА	ПРАВЛІННЯ	НБУ	
Не рідше ніж 1 раз на 6 місяців	ТАК	Голові Правління Банку		Інформація (звіт) про стан реалізації, у тому числі невжиття Правлінням та керівниками підрозділів Банку рекомендацій (пропозицій) із усунення порушень і недоліків у діяльності Банку, виявлених за результатами аудиту.
Щопівроку			ТАК	Звіт про роботу УПРАВЛІННЯ та інші документи щодо внутрішнього аудиту Банку відповідно до вимог НПА №311.
Не рідше ніж 1 раз на рік, не пізніше останнього дня першого місяця року, наступного за звітним	ТАК	Голові Правління Банку		Звіт за відповідний період, що вміщує наступну інформацію: <ul style="list-style-type: none"> • щодо виконання річного плану проведення аудиторських перевірок (аудиту); • щодо суттєвих проблем, ризиків та недоліків у діяльності Банку; • щодо суттєвих обмежень, що заважають УПРАВЛІННЮ ефективно виконувати поставлені завдання; • підтвердження організаційної незалежності. Крім цього, УПРАВЛІННЯ підсумовує результати оцінки стану контролю розглянутих протягом звітного періоду процесів, враховує поточний стан впровадження планів заходів, затверджених за результатами аудиту, аналізує повноту переліку ВНД та управлінських звітів Банку з питань ризиків і контролю та зазначає у річному звіті оцінку системи внутрішнього контролю Банку, з точки зору її відповідності вимогам НПА №88.
	ТАК	Голові Правління Банку на обговорення		Проект річного плану проведення аудиторських перевірок (аудиту) на наступний звітний період.
Після розробки плану	ТАК (до відома, інформаційно)			За рішенням начальника УПРАВЛІННЯ, в умовах стабільного зовнішнього та внутрішнього середовища може складатися довгостроковий план робіт УПРАВЛІННЯ (3-5 років).
Не рідше ніж 1 раз на рік	ТАК	ТАК		Звіт щодо результатів самооцінки діяльності УПРАВЛІННЯ у звітному році ^{ФОРМАТ} та про виконання програми забезпечення та підвищення якості внутрішнього аудиту Банку у звітному році. Програма забезпечення та підвищення якості внутрішнього аудиту Банку на новий звітний рік доводиться до Правління та Ради інформаційно.
Не рідше 1 разу на 3 роки	ТАК			Звіт щодо результатів проведення самооцінки діяльності УПРАВЛІННЯ на відповідність МСВА ^{ФОРМАТ} ² .

3.2. Результати перевірки документуються і можуть бути оформленими:

- у вигляді звіту ^{ПРИМ. 3.2}, який, як правило, складається з 2-х частин: *детального* звіту з докладним описом виконаної роботи та *підсумкового резюме* із висновками, яке може бути оформлене у вигляді презентації;

¹ раз в 5 років На поточний момент - не рідше 1 разу на п'ять років.

^{ФОРМАТ} Результати самооцінки оформлюються за діючою редакцією типової форми, затвердженої відповідним рішенням Ради Банку («типова форма Звіту про самооцінку роботи УПРАВЛІННЯ у звітному році»).

^{ФОРМАТ 2} Результати самооцінки відповідності діяльності УПРАВЛІННЯ вимогам МСВА оформлюються звітом, структура якого складається, враховуючи перелік норм МСВА, у форматі на професійний розсуд начальника УПРАВЛІННЯ.

- у вигляді складеного працівниками УПРАВЛІННЯ акту ревізії каси / АТМ;
- у вигляді службової записки/інформаційного листа щодо виявлених недоліків. Зазначені документи складаються до закінчення аудиту ^[проміжне інформування], у разі встановлення недоліків, які є суттєвими та вимагають термінового усунення / прийняття управлінського рішення. Або можуть складатися у доповнення до аудиторського звіту, у разі виявлення недоліків / ризиків процесу, який не є об'єктом аудитом ^[суміжні проблеми].

Звіт про хід виконання та результати консультаційного завдання може відрізнятися за формою та змістом, залежно від характеру завдання та потреб замовника.

3.3. Результати перевірок обговорюються з суб'єктами аудиту, а також з відповідальними працівниками ^{ПРИМ. 3.3}, в компетенції яких усунення встановлених аудитом недоліків та вжиття заходів щодо посилення систем внутрішнього контролю, управління ризиками та корпоративного управління.

3.4. Після завершення всіх обговорень та підписання документів стосовно результатів аудиту, матеріали надаються на розгляд Ради. До адресатів також обов'язково ^{!!!} додаються Голова Правління та керівники Департаменту ризик-менеджменту і Управління контролю дотримання норм (комплаєнс).

У разі необхідності, за ініціативою начальника УПРАВЛІННЯ / членів Правління результати аудиту, перед їх передаванням на розгляд Ради, можуть обговорюватися на засіданні Правління Банку ^{!!!}.

Акт ревізії або службова записка / інформаційний лист за результатами аудиту можуть надаватися тільки на адресу відповідальних осіб та/або окремих членів Правління / Комітету Ради з питань аудиту / Ради Банку - залежно від критичності встановлених недоліків та/або необхідного рівня компетенції. У цьому випадку УПРАВЛІННЯ може на розгляд Ради Банку надавати підсумкову узагальнену довідку за результатами аналізу результатів декількох ревізій / тематичних моніторингов, які були проведені у звітному періоді.

У будь-якому випадку, у разі ідентифікації потенційних та/або реалізованих ^{суттєвих} ризиків начальник УПРАВЛІННЯ терміново інформує стосовно них Голову Правління ^{!!!}, Раду Банку.

4. ЦІЛІ, НАПРЯМИ ДІЯЛЬНОСТІ ТА ФУНКЦІЇ УПРАВЛІННЯ

4.1. Мета діяльності УПРАВЛІННЯ - сприяти органам управління та керівництву Банку у досягненні цілей і завдань Банку та у підвищенні ефективності систем корпоративного управління, управління ризиками та внутрішнього контролю.

4.2. Напрямки діяльності УПРАВЛІННЯ:

- забезпечення незалежної, об'єктивної *оцінки* комплексності, адекватності та ефективності систем внутрішнього контролю, управління ризиками, корпоративного управління, *оцінки* дотримання банком вимог ЗАКОНОДАВСТВА та внутрішніх нормативних документів, *оцінки* ефективності інших систем, створених з метою дотримання правових вимог та професійних кодексів поведінки (із врахуванням вимог НПА №88 або іншого документа йому на зміну);
- організація процесів планування, розвитку та надання звітності щодо стану внутрішнього аудиту.

4.3. УПРАВЛІННЯ для досягнення покладених на нього завдань виконує наступні функції:

4.3.1. перевіряє та оцінює процеси, які забезпечують діяльність Банку (*фінансово-господарську діяльність Банку*), у тому числі ті, що несуть потенційний ризик та виконання яких забезпечується шляхом залучення юридичних та фізичних осіб на договірній основі (*аутсорсинг*);

4.3.2. оцінює ефективність та адекватність організації *корпоративного управління* в Банку, *системи внутрішнього контролю*, у тому числі системи управління ризиками, *процесів управління Банком*

ПРИМ. 3.2. Обов'язкові вимоги щодо формату аудиторського звіту встановлюються «Регламентом роботи підрозділу внутрішнього аудиту (Управління внутрішнього аудиту) Банку» [або іншим документом, прийнятим на зміну регламенту].

ПРИМ. 3.3. Результати аудиту обговорюються на всіх організаційних рівнях, як з безпосередніми виконавцями/ керівниками підрозділів, які забезпечують функціонування розглянутого процесу, так і з членами Правління, відповідальними за цей процес. Відповідальним особам, які не є суб'єктами аудиту, на розсуд начальника УПРАВЛІННЯ, може направлятися як повний аудиторський звіт, так і тільки окремий його розділ, що стосується недоліку їх зони відповідальності.

^{!!!} За умови відсутності конфлікту інтересів.

^{суттєвих} Наприклад, випадки шахрайства, втрати активів, значні випадки порушення діючого ЗАКОНОДАВСТВА, збоїв системи внутрішнього контролю Банку, які можуть суттєво вплинути на фінансові результати роботи Банку, та таке інше.

ПРИМ. 4.3.2, їх відповідність розміру Банку, складності, обсягам, видам, характеру здійснюваних Банком операцій, організаційній структурі та профілю ризику Банку, з урахуванням особливостей діяльності Банку як системно важливого (за наявності такого статусу) та/або діяльності банківської групи, до складу якої входить Банк (за наявності такої групи), організації внутрішньої системи протидії відмиванню коштів/фінансуванню тероризму, системи управління ризиками відмивання коштів/фінансування тероризму;

4.3.3. оцінює діяльність підрозділів з управління ризиками та комплаєнс-ризиком, комітетів, що створені Банком, та якість звітів про ризики, що надаються Раді та Правлінню Банку;

4.3.4. здійснює оцінку впроваджених керівництвом Банку систем контролю, зокрема:

- системи контролю за дотриманням керівниками та працівниками Банку, що забезпечують надання банківських та інших фінансових послуг, вимог ЗАКОНОДАВСТВА та внутрішніх положень Банку, за виконанням професійних обов'язків і правил, що встановлені Статутом та внутрішніми документами Банку, у тому числі з питань комплаєнсу та управління ризиками, а також за виявленням та аналізом фактів порушень працівниками Банку вимог чинного ЗАКОНОДАВСТВА, стандартів професійної діяльності, внутрішніх положень, що регулюють діяльність Банку;
- системи контролю своєчасності усунення недоліків, виявлених Національним банком та іншими органами державної влади та управління, які в межах компетенції здійснюють нагляд за діяльністю Банку;

4.3.5. перевіряє правильність ведення та достовірність бухгалтерського обліку, інформації, фінансової та іншої звітності, що складається Банком, їх повноту та вчасність надання, у тому числі до Національного банку, органів державної влади та управління, які в межах компетенції здійснюють нагляд за діяльністю Банку;

4.3.6. оцінює надійність, ефективність та цілісність управління інформаційними системами та процесами Банку, у тому числі релевантність, точність, повноту, доступність, конфіденційність, комплексність даних (інформаційно-технічне забезпечення управління та проведення операцій) ПРИМ. 4.3.6;

4.3.7. в рамках аудиту, перевіряє дотримання керівниками та працівниками Банку вимог ЗАКОНОДАВСТВА і внутрішніх положень Банку; перевіряє відповідність кваліфікаційним вимогам та виконання професійних обов'язків працівниками Банку; виявляє та перевіряє випадки перевищення повноважень посадовими особами Банку і виникнення конфлікту інтересів у Банку;

4.3.8. оцінює ефективність та достатність складеного Банком плану відновлення його діяльності (у разі його складання);

4.3.9. розробляє пропозиції та рекомендації щодо усунення виявлених недоліків та порушень, зниження ризиків, підвищення якості та ефективності систем корпоративного управління, управління ризиками та внутрішнього контролю, а також щодо попередження дій, результатом яких може стати порушення Банком вимог ЗАКОНОДАВСТВА;

ПРИМ. 4.3.2 У тому числі - процеси оцінки достатності капіталу, достатності ліквідності, засобів забезпечення збереження активів з урахуванням ризиків Банку, тощо.

ПРИМ. 4.3.6 У випадку відсутності у штаті УПРАВЛІННЯ кваліфікованого спеціаліста для проведення ІТ/СУІБ-аудиту, є можливим виконання цієї функції шляхом залучення юридичних/фізичних осіб з належним рівнем компетенції та практичного досвіду, на договірній основі (АУТСОРСИНГ).

Загальні підходи до проведення ІТ/СУІБ-аудиту. ІТ/СУІБ-аудит проводиться з метою впевнитися, що цілі контролю, контролі/ процеси/ процедури, які Банк застосовує в СУІБ, забезпечують:

- дотримання вимог галузевих стандартів та ЗАКОНОДАВСТВА в області СУІБ;
- мінімізацію ідентифікованих інформаційних ризиків;
- ефективне управління СУІБ в Банку та достатність ресурсу для його підтримки;
- фактичне функціонування СУІБ відповідно до вимог ВНД стосовно цього напрямку.

У звіті за результатами перевірки зазначається загальна оцінка рівня розвитку СУІБ Банку та відповідні висновки та рекомендації. При вирішенні питання стосовно доцільності додавання ІТ/СУІБ-аудиту до складу річного плану УПРАВЛІННЯ застосовує ризик орієнтовний підхід, із врахуванням результатів річної оцінки ризиків. Формат (комплексна/тематична перевірка) та тематика аудиту визначаються із врахуванням критичності процесів та тематичних напрямків, які підлягають аудиту, та із застосуванням професійного судження начальника УПРАВЛІННЯ. В тому числі враховуються: результати попередніх перевірок, в т.ч. регулятора та зовнішніх контролюючих органів; результати оцінки ризиків та інформація щодо інцидентів ІБ; питання роботи процесу внутрішнього контролю за виконанням Банком вимог МПС.

4.3.10. здійснює моніторинг усунення виявлених УПРАВЛІННЯМ порушень та недоліків, а також виконання наданих УПРАВЛІННЯМ рекомендацій та пропозицій (наступний контроль аудиту);

4.3.11. розроблює річний план аудиту та довгостроковий план аудиту - якщо прийнято рішення щодо доцільності розробки останнього;

4.3.12. розробляє програми внутрішнього аудиту;

4.3.13. готує внутрішню звітність, в тому числі щодо виконання річного плану аудиту, та звітність щодо стану внутрішнього аудиту Банку для Національного банку;

4.3.14. організовує процеси розвитку внутрішнього аудиту;

4.3.15. надає в межах Банку та за відсутності загрози незалежності консультаційні послуги ПРИМ. 4.3.15, виконує інші передбачені ЗАКОНОДАВСТВОМ функції, пов'язані зі здійсненням нагляду за діяльністю Банку;

4.4. Розподіл функцій між відділами, які входять до складу УПРАВЛІННЯ:

- Відділ безвиїзного аудиту виконує вищезазначені функції відносно об'єктів аудиту, в якості яких розглядаються структурні підрозділи / процеси Головного Банку;
- Відділ виїзного аудиту виконує вищезазначені функції відносно об'єктів аудиту, в якості яких розглядаються відділення Банку та процеси, як відбуваються на відділеннях Банку.

4.5. Працівники відділів, які входять до складу УПРАВЛІННЯ, виконують функції, передбачені для кожного відділу, при цьому працівники відділів за усним розпорядженням (розподілом) начальника УПРАВЛІННЯ також зобов'язані виконувати функції в компетенції УПРАВЛІННЯ.

5. КВАЛІФІКАЦІЙНІ ВИМОГИ ДО ПРАЦІВНИКІВ УПРАВЛІННЯ, ПОРЯДОК ПРИЗНАЧЕННЯ ТА ЗВІЛЬНЕННЯ, ПІДПОРЯДКУВАННЯ НАЧАЛЬНИКА ТА ІНШИХ ПРАЦІВНИКІВ УПРАВЛІННЯ

5.1. Обов'язкові вимоги до внутрішніх аудиторів Банку:

- повна вища освіта;
- стаж роботи в банківській системі не менше трьох років;
- знання ЗАКОНОДАВСТВА щодо банківської діяльності та щодо проведення внутрішнього аудиту в банках, володіння основами бухгалтерського обліку;
- високий рівень відповідальності за свою роботу, вимогливість до себе, ділова принциповість;
- ініціативність в роботі, навички комунікації та дисциплінованість;
- знання державної мови, правил експлуатації комп'ютерної і обчислюваної техніки;
- достатні знання, навички і досвід, необхідні для проведення аудиту всіх сфер діяльності банку, ризиків, які притаманні банку. Навички повинні включати здатність проведення аудиторських перевірок різноманітної складності, які необхідно виконувати в результаті впровадження в Банку нових продуктів та процесів, сприяючи їх удосконаленню;
- здатність збирати і розуміти інформацію, вивчати та оцінювати аудиторські докази, кваліфіковано та конструктивно спілкуватись із працівниками Банку;
- уміння під час виконання завдань внутрішнього аудиту проявляти старанність, сумлінність та застосовувати професійні навички, МСВА.

ПРИМ. 4.3.15 **КОНСУЛЬТАЦІЙНІ ПОСЛУГИ УПРАВЛІННЯ.** Прикладом консультаційної послуги може бути складання працівником УПРАВЛІННЯ оціночного висновку відносно проекту ВНД на предмет доцільності, достатності та ефективності передбачених в ньому процедур внутрішнього контролю.

Консультаційні послуги надаються працівниками УПРАВЛІННЯ у випадку наявності в УПРАВЛІННІ працівників необхідної компетенції (знання, навички та інші професійні здібності, необхідні для виконання завдання в цілому або його частини) та при наявності неутілізованого ліміту передбаченого Радою Банку резерву часу УПРАВЛІННЯ. Запит на отримання консультаційної послуги має бути документально оформленим підрозділом - замовником. Члени Правління Банку можуть замовити консультаційну послугу у робочому порядку (без документального оформлення запиту), про що зазначається у висновку аудиту за результатами виконаної роботи.

Якщо є потенційна загроза обмеження незалежності або об'єктивності при виконанні УПРАВЛІННЯМ замовлених консультаційних послуг, ця інформація обговорюється із замовником до прийняття від нього завдання на виконання.

Внутрішній аудитор, який безпосередньо надав консультаційну послугу, **протягом 6 місяців з дати оформлення оціночного висновку** не має права проводити повторну оцінку об'єкту цієї консультаційної послуги.

При наданні консультаційних послуг внутрішній аудитор має всі права та повинен дотримуватися всіх обов'язків, передбачених цим Положенням, із урахуванням особливостей цього аудиторського продукту (**КОНСУЛЬТАЦІЯ**).

Ці вимоги є мінімальними.

5.2. Додаткові вимоги до професійної придатності та ділової репутації працівників УПРАВЛІННЯ можуть встановлюватися начальником УПРАВЛІННЯ та визначатися в їх посадових інструкціях.

5.3. На посаду начальника УПРАВЛІННЯ призначається особа, яка має вищу освіту, досвід роботи у сфері аудиторської діяльності не менше п'яти років, із яких не менше ніж три роки в банку(ах), стосовно якої дотримані обмеження, визначені у статті 45 Закону України "Про банки і банківську діяльність" щодо зайняття посад в інших банках, та яка відповідає іншим кваліфікаційним вимогам до професійної придатності та ділової репутації ^{ПРИМ. 5.3}.

5.4. На виконання вимог ЗАКОНОДАВСТВА (в тому числі НПА №149), не рідше ніж один раз на рік Банк перевіряє начальника УПРАВЛІННЯ щодо його відповідності вимогам, установленим ЗАКОНОДАВСТВОМ для зазначеної посади та, після розгляду цього питання Радою Банку, письмово повідомляє Національний банк про результати такої перевірки.

5.5. Начальник УПРАВЛІННЯ призначається на посаду/звільнюється з неї - за рішенням Ради Банку, в порядку, передбаченому діючим ЗАКОНОДАВСТВОМ, Статутом та іншими внутрішніми документами Банку.

Кандидатура начальника УПРАВЛІННЯ погоджується з НБУ. Начальник УПРАВЛІННЯ вступає на посаду після погодження його кандидатури Національним банком України.

Рішення щодо звільнення з посади начальника УПРАВЛІННЯ, крім випадків звільнення за його власним бажанням, за згодою сторін або у зв'язку із закінченням строку трудового договору (контракту), - в обов'язковому порядку узгоджується з НБУ.

5.6. Працівники УПРАВЛІННЯ призначаються та звільняються з посади в порядку, передбаченому діючим ЗАКОНОДАВСТВОМ, Статутом та іншими внутрішніми документами Банку, за поданням начальника УПРАВЛІННЯ.

5.7. Начальник УПРАВЛІННЯ підпорядковується та звітує перед Радою Банку.

Всі працівники УПРАВЛІННЯ підпорядковуються начальнику УПРАВЛІННЯ, працівники відділів, що входять до складу УПРАВЛІННЯ, підпорядковуються начальнику відповідного відділу УПРАВЛІННЯ.

5.8. На час тимчасової відсутності начальника УПРАВЛІННЯ виконання його обов'язків покладається на його заступника, а в період тимчасової відсутності як начальника УПРАВЛІННЯ, так і його заступника (одночасно) - на одного з працівників УПРАВЛІННЯ за поданням начальника УПРАВЛІННЯ (або особи, яка виконує його обов'язки) на підставі відповідного розпорядчого документу, у визначеному у Банку порядку.

5.9. На час тимчасової відсутності начальників відділів, що входять до складу УПРАВЛІННЯ, їх обов'язки виконує інший працівник УПРАВЛІННЯ за поданням начальника УПРАВЛІННЯ на підставі відповідного розпорядчого документу у визначеному Банком порядку.

6. ОБОВ'ЯЗКИ НАЧАЛЬНИКА УПРАВЛІННЯ ТА ВНУТРІШНІХ АУДИТОРІВ ^{ПРИМ. Р.6}

6.1. Для виконання поставлених перед УПРАВЛІННЯМ завдань, **НАЧАЛЬНИК УПРАВЛІННЯ ЗОБОВ'ЯЗАНИЙ:**

6.1.1. мати достатній кваліфікаційний рівень знань і навичок, постійно їх удосконалювати, демонструвати менеджерські та лідерські якості;

6.1.2. забезпечувати безперервну роботу УПРАВЛІННЯ відповідно до цього Положення, НПА №311, МСВА, НОРМ ЕТИКИ АУДИТОРІВ та принципів діяльності, визначених у зазначених документах;

6.1.3. забезпечувати комплектацію УПРАВЛІННЯ висококваліфікованим персоналом з необхідними навичками роботи, що включають здатність ефективно та професійно оцінювати результати діяльності Банку, здійснювати вплив на найвищому рівні управління Банком;

^{ПРИМ. 5.3} Професійна придатність начальника УПРАВЛІННЯ (як керівника підрозділу внутрішнього аудиту Банку) визначається як сукупність знань, професійного та управлінського досвіду, необхідних для належного виконання своїх посадових обов'язків з урахуванням бізнес-плану та стратегії розвитку Банку. Інші кваліфікаційні вимоги до кандидата на посаду начальника УПРАВЛІННЯ, порядок погодження Національним банком його кандидатури та його звільнення [крім випадків звільнення такої особи за власним бажанням, за згодою сторін або у зв'язку із закінченням строку трудового договору (контракту)] установлюються нормативно-правовим актом Національного банку, що визначає порядок реєстрації та ліцензування банків.

^{ПРИМ. Р.6} У випадку залучення спеціалістів Банку для виконання окремих завдань внутрішнього аудиту, на період їх залучення на цих спеціалістів, в межах їх компетенції та дорученого завдання, розповсюджуються права, обов'язки та відповідальність, передбачені для внутрішніх аудиторів УПРАВЛІННЯ Банку.

- 6.1.4. забезпечувати безперервну професійну підготовку та навчання внутрішніх аудиторів;
- 6.1.5. складати та подавати на затвердження Раді Банку плани УПРАВЛІННЯ та забезпечувати їх виконання ^{ПРИМ. 6.1.5;};
- 6.1.6. визначати політики та аудиторські процедури, які застосовуються внутрішніми аудиторами для проведення аудиторської перевірки (аудиту), відповідно до вимог внутрішніх документів Банку з питань проведення аудиторської перевірки (аудиту) та МСВА;
- 6.1.7. забезпечувати відповідність, достатність та ефективність використання ресурсів УПРАВЛІННЯ для виконання річного плану проведення аудиторської перевірки (аудиту) Банку;
- 6.1.8. складати звіт про виконання річного плану проведення аудиторських перевірок (аудиту) та подавати його на затвердження Раді **не пізніше останнього дня першого місяця року**, наступного за звітним, із наданням підтвердження щодо організаційної незалежності УПРАВЛІННЯ;
- 6.1.9. забезпечувати подання керівникам структурних підрозділів ^[учасників процесів, які підлягали аудиторській перевірці (аудиту)], Правлінню та Раді Банку звітів за результатами проведення аудиторських перевірок (аудиту) для прийняття ними відповідних організаційних (коригувальних) заходів;
- 6.1.10. розробити та підтримувати систему моніторингу виконання керівниками Банку рекомендацій (пропозицій), наданих за результатами аудиторських перевірок (аудиту);
- 6.1.11. подавати Раді Банку **не рідше ніж один раз на півроку** інформацію (звіт) про стан реалізації, у тому числі невжиття, Правлінням та керівниками підрозділів Банку рекомендацій (пропозицій) із усунення порушень і недоліків у діяльності Банку, виявлених за результатами аудиту;
- 6.1.12. у випадку виникнення обставин, які перешкоджають ^{ПРИМ. 6.1.12} внутрішнім аудиторам Банку виконувати свої обов'язки, втручання посадових осіб Банку в діяльність УПРАВЛІННЯ, виявлення рівня ризику, що є неприйнятним для діяльності Банку, **письмово проінформувати про це Раду Банку** для прийняття нею відповідних рішень або вжиття заходів;
- 6.1.13. розробити та підтримувати програму забезпечення та підвищення якості внутрішнього аудиту Банку з урахуванням вимог МСВА, забезпечити **періодичне** звітування Раді та Правлінню Банку про її виконання;
- 6.1.14. забезпечити відсутність втрати об'єктивності внутрішніх аудиторів, у тому числі шляхом проведення періодичної ротації внутрішніх аудиторів, яка не повинна позначатися на якості проведення аудиту;
- 6.1.15. складати і подавати до Національного банку відповідно до вимог НПА №311 Звіт про роботу УПРАВЛІННЯ та інші документи за результатами внутрішнього аудиту Банку;
- 6.1.16. письмово повідомляти Національний банк про виявлені під час проведення аудиторської перевірки (аудиту) викривлення показників фінансової звітності Банку, порушення та недоліки в роботі Банку, а також будь-які події в діяльності Банку, які можуть негативно вплинути на платоспроможність, безпеку і надійність Банку / учасника банківської групи, якщо Правління Банку своєчасно не вжило заходів щодо усунення цих порушень та недоліків, а Рада Банку не розглянула звернення начальника УПРАВЛІННЯ щодо бездіяльності Правління Банку та за результатами розгляду цього звернення не вжила відповідних заходів;
- 6.1.17. забезпечити в межах своїх повноважень на постійній основі співпрацю із зовнішніми аудиторами, органами державної влади та управління, які в межах компетенції здійснюють нагляд за діяльністю Банку, у тому числі з Національним банком.

6.2. Крім вищезазначеного начальник УПРАВЛІННЯ:

- керує діяльністю начальників відділів зі складу УПРАВЛІННЯ, організовує та координує їх роботу;

ПРИМ. 6.1.5 В тому числі забезпечувати здійснення періодичних перевірок дотримання Банком вимог законодавства у сфері запобігання легалізації кримінальних доходів / фінансування тероризму (у тому числі щодо достатності вжитих Банком заходів з управління ризиками легалізації кримінальних доходів / фінансування тероризму).

ПРИМ. 6.1.12 У разі виникнення зазначених обставин начальник УПРАВЛІННЯ звертається (у разі відсутності конфлікту інтересів) до Голови Правління Банку для врегулювання ситуації. Якщо Голова Правління Банку своєчасно не вживає відповідних заходів щодо усунення порушень повноважень працівників УПРАВЛІННЯ, начальник УПРАВЛІННЯ повідомляє стосовно цього факту Раду Банку.

- розподіляє обов'язки між начальниками відділів зі складу УПРАВЛІННЯ. У разі наявності функціоналу, не розподіленого між працівниками УПРАВЛІННЯ (в тому числі це стосується і функціоналу працівників, які тимчасово відсутні (відпустка, лікарняний)), такий функціонал відноситься до зони відповідальності начальника УПРАВЛІННЯ;

- контролює дотримання працівниками УПРАВЛІННЯ трудової дисципліни;

- в межах своїх повноважень, вирішує оперативні питання, розглядає вхідну / вихідну кореспонденцію УПРАВЛІННЯ, підписує документи з питань, які належать до діяльності УПРАВЛІННЯ;

- є особою, відповідальною за ведення діловодства в УПРАВЛІННІ та за своєчасне здавання документів УПРАВЛІННЯ до архіву Банку згідно номенклатури справ УПРАВЛІННЯ. Начальник УПРАВЛІННЯ *має право делегувати* цей обов'язок іншому(шим) працівнику(кам), за умови, що цей делегований функціонал зазначається у посадовій інструкції відповідного працівника УПРАВЛІННЯ. При цьому за начальником УПРАВЛІННЯ залишається обов'язок здійснення загального контролю за належним виконанням цієї функції. За ведення діловодства структурних підрозділів в складі УПРАВЛІННЯ відповідають їх керівники в рамках кожного окремого підрозділу;

- забезпечує взаємодію з іншими структурними підрозділами Банку для вирішення завдань УПРАВЛІННЯ;

- в межах компетенції УПРАВЛІННЯ представляє УПРАВЛІННЯ та взаємодіє зі зовнішніми організаціями, в тому числі Національним банком, зовнішніми аудиторами;

- проводить системний аналіз стану справ щодо питань, які входять до компетенції УПРАВЛІННЯ, та на його підставі готує пропозиції Голові Правління Банку та/або Раді Банку стосовно вдосконалення наявних та впровадження нових форм, методів роботи УПРАВЛІННЯ.

6.3. Для виконання поставлених перед УПРАВЛІННЯМ завдань, НАЧАЛЬНИК та ІНШІ ПРАЦІВНИКИ УПРАВЛІННЯ ЗОБОВ'ЯЗАНІ:

6.3.1. належним чином виконувати свої функції (посадові обов'язки);

6.3.2. дотримуватись вимог ЗАКОНОДАВСТВА, у тому числі НПА №311, цього Положення, МСВА, НОРМ ЕТИКИ АУДИТОРІВ, Кодексу етики Банку, принципів діяльності, визначених у зазначених документах, дотримуватись вимог нормативно-правових актів з охорони праці;

6.3.3. виявляти за результатами аудиту сфери потенційних збитків для Банку, сприятливі умови для шахрайства, зловживань і незаконного присвоєння коштів Банку та повідомляти про це в установленому порядку Раді та Правлінню Банку;

6.3.4. здійснювати незалежну оцінку створеної керівництвом Банку системи внутрішнього контролю за дотриманням працівниками Банку нормативно-правових актів НБУ, внутрішніх положень Банку щодо порядку надання банківських та інших фінансових послуг, внутрішніх документів Банку з питань фінансового моніторингу, ефективності дій менеджменту, видів діяльності Банку, у тому числі тих, виконання яких забезпечується ним шляхом залучення юридичних і фізичних осіб на договірній основі (аутсорсинг), а також здійснення іншої діяльності, передбаченої Статутом Банку. Внутрішній аудитор повинен бути особливо уважним щодо оцінки ефективності процесів управління значними ризиками, які можуть вплинути на діяльність Банку;

6.3.5. ініціювати подання Раді, Правлінню Банку, керівникам структурних підрозділів, що перевіряються, звітів за результатами проведення аудиторських перевірок (аудиту), у тому числі щодо забезпечення виконання Банком вимог законодавства України у сфері запобігання легалізації кримінальних доходів / фінансуванню тероризму;

6.3.6. ініціювати надання рекомендацій керівникам структурних підрозділів щодо вжиття заходів для уникнення та недопущення дій, результатом яких може стати порушення Банком вимог ЗАКОНОДАВСТВА, та здійснювати моніторинг повноти та своєчасності впровадження рекомендацій, що були надані за результатами попередніх аудиторських перевірок (аудиту);

6.3.7. надавати пропозиції щодо підвищення ефективності роботи системи управління ризиками, у тому числі її відповідності видам і обсягам здійснюваних Банком операцій, та системи внутрішнього контролю;

6.3.8. перевіряти ефективність застосованих Банком заходів щодо виправлення виявлених УПРАВЛІННЯМ порушень та недоліків;

6.3.9. забезпечувати схоронність і своєчасність повернення одержаних від керівників або структурних підрозділів Банку документів на всіх носіях;

6.3.10. не розголошувати та не використовувати конфіденційну інформацію, яка стала їм відома під час виконання своїх функцій, на свою користь чи на користь третіх осіб, **уникати конфлікту інтересів**;

6.3.11. удосконалювати свої знання, навички та інші вміння шляхом постійного професійного розвитку, демонструвати професійну компетентність та належну ретельність;

6.3.12. своєчасно інформувати начальника УПРАВЛІННЯ щодо встановлених проблем, реалізованих або потенційних ризиків, порушень та недоліків, загроз інтересам Банку, а також **негайно повідомити** начальника УПРАВЛІННЯ у разі виникнення фактичного / потенційного конфлікту інтересів та/ або фактичної / потенціальної загрози втрати об'єктивності / незалежності працівника УПРАВЛІННЯ, в їх визначенні МСВА та/або ВНД УВА/Банку ^{загроза}, або у разі відмови підрозділами Банку в отриманні інформації/ документу/ необмеженого доступу, необхідних для виконання посадових обов'язків;

6.3.13. проявляти ретельність та застосовувати вміння, що очікуються від розсудливого та компетентного внутрішнього аудитора; бути особливо уважними щодо значних ризиків, які можуть вплинути на цілі, операційну діяльність або ресурси Банку; але при цьому належна професійна ретельність аудитора не означає, що він не має права на помилку, а самі аудиторські процедури, навіть виконані з належною професійною ретельністю, не гарантують виявлення аудитом всіх значних ризиків;

6.3.14. з метою попередження конфлікту інтересів, утриматися від участі в перевірці у випадках, коли працівник УПРАВЛІННЯ збирається найближчим часом перевестися до іншого підрозділу Банку, якій має бути суб'єктом аудиту в перевірці, в якій цей працівник планував приймати участь;

6.3.15. виконувати **інші обов'язки**, передбачені для внутрішніх аудиторів Банків ЗАКОНОДАВСТВОМ, в тому числі НПА №311, а також визначені Статутом, рішеннями Загальних зборів акціонерів, Ради Банку та цим Положенням, в тому числі в інших розділах.

6.3.16. Всі працівники УПРАВЛІННЯ при вступі на посаду підписують зобов'язання щодо збереження банківської таємниці, а також зобов'язання про нерозголошення та невикористання з вигодою для себе чи третіх осіб комерційної таємниці та конфіденційної інформації, яка стане їм відомою при виконанні посадових обов'язків.

6.4. ОBOB'ЯЗКИ ВСІХ ПРАЦІВНИКІВ УПРАВЛІННЯ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

6.4.1. Зобов'язання працівників УПРАВЛІННЯ:

6.4.1.1. Особисто сповіщати відповідальних осіб служби безпеки Банку про розголошення чи будь-які спроби розголошення, несанкціонованого отримання та використання третіми особами інформації, що складає ІзОД ¹, компрометації аутентифікаційних даних, секретних ключів, підозри на такі спроби, факти виявлення вірусів, підозр на їхнє проникнення або про будь-які інші інциденти безпеки;

6.4.1.2. Зберігати відомі їм паролі в таємниці. В разі складнощів з запам'ятанням паролів доступу, зберігати паролі в запечатаному конверті в сейфі начальника УПРАВЛІННЯ або в сертифікованому програмному забезпеченні менеджера паролів (наприклад, - KeePass);

^{загроза} У разі виявлення зазначених обставин аудитор повідомляє про це начальника Управління засобами корпоративної пошти.

¹ Інформація з обмеженим доступом. До ІзОД належать такі види інформації:

- банківська таємниця, комерційна таємниця;
- конфіденційна інформація -
 - про фізичну особу (персональні дані працівників та членів Ради Банку, тощо),
 - про Банк,
 - конфіденційна інформація, доступ до якої обмежено контрагентом Банку;
- інформація, що міститься в системі депозитарного обліку;
- службова інформація суб'єктів владних повноважень, що міститься у документах із грифом "Для службового користування", що надійшли від суб'єктів владних повноважень.

- 6.4.1.3. Проводити обов'язкову ідентифікацію «співробітника Банку» у разі телефонної розмови **зі стаціонарних чи мобільних пристроїв**, якщо метою розмови буде розголошення конфіденційної інформації або ідентифікаційних даних (облікові записи) співробітників;
- 6.4.1.4. Матеріальні носії конфіденційної інформації повинні замикатися в сейфі чи металевій шафі, по завершенню роботи з ними;
- 6.4.1.5. Комп'ютери та термінали повинні бути залишені в стані виконаного виходу з системи, коли вони знаходяться без нагляду;
- 6.4.1.6. Факсимільна апаратура, багатофункціональні пристрої, телефони, що знаходиться без нагляду, повинна бути захищена від доступу сторонніх осіб;
- 6.4.1.7. Документи, що містять конфіденційну інформацію, повинні бути забрані з принтерів негайно;
- 6.4.1.8. Для утилізації конфіденційних документів, повинні використовуватися знищувачі паперу;
- 6.4.1.9. Після закінчення робочого дня і в разі тривалої відсутності на робочому місці співробітник повинен привести в порядок письмовий стіл і прибрати всі конфіденційні документи в шафу, що замикається, або сейф. Всі технічні засоби (персональні комп'ютери, сканери, принтери та інше), які не беруть участь у цілодобовому технологічному процесі, повинні бути відключені від електромережі.

6.4.2. Працівникам УПРАВЛІННЯ забороняється:

- 6.4.2.1. Забороняється вести запис паролів (наприклад, на папері, в файлах на персональному комп'ютері або в кишеньковому пристрої);
- 6.4.2.2. Забороняється переходити за посиланнями в листах електронної пошти, які мають ознаки Спаму, та вводити свої ідентифікаційні дані (логін, пароль), поки не переконаєтеся в легітимності листа та **коректності запиту**;
- 6.4.2.3. Забороняється в листуванні з зовнішніми респондентами передавати вкладення, використовуючи зашифровані чи запаролені архіви, архіви, розділені на томи;
- 6.4.2.4. Забороняється вести запис/фотографування екранів комп'ютерів мультимедійною апаратурою чи мобільними гаджетами;
- 6.4.2.5. Забороняється здійснювати доступ з робочої станції до ненадійних (незнайомих) інтернет-ресурсів, користуватися для передачі інформації поштовими інтернет-сервісами третіх сторін (*mail.ru, rambler.ru, gmail.com, ukr.net* тощо);
- 6.4.2.6. Забороняється використовувати при листуванні з зовнішніми респондентами шифровані, архівовані вкладення, які неможливо перевірити на malware;
- 6.4.2.7. Забороняється використовувати при листуванні з зовнішніми респондентами архіватори з відкритим кодом, наприклад, - 7Z (7-zip), тобто - free software with open source (**GNU LGPL license**);
- 6.4.2.8. Забороняється використовувати корпоративний email щодо реєстрації на конференціях, виставках тощо, тобто ресурсах Інтернет, що не мають відношення до банківських послуг;
- 6.4.2.9. Забороняється здійснювати доступ до інтернет-ресурсів в особистий цілях (інтернет-серфінг, скачування даних);
- 6.4.2.10. Залишати увімкненою без нагляду свою робочу станцію/комп'ютер, не активізувавши засоби захисту від несанкціонованого доступу (тимчасове блокування екрану і клавіатури);
- 6.4.2.11. Залишати без особистого нагляду на робочому місці або де інше свій персональний ключ доступу;
- 6.4.2.12. Самостійно, без наявності на те дозволу співробітників Департаменту ІТ, встановлювати або видаляти програмне забезпечення або підключати - відключати будь-які технічні засоби до комп'ютерного устаткування;
- 6.4.2.13. Змінювати налаштування технічних засобів/комп'ютерів і встановленого програмного забезпечення, розкривати комп'ютерне устаткування;
- 6.4.2.14. Приносити, а також використовувати технічні засоби, що належать третім особам;

- 6.4.2.15. Вносити/передавати з Банку засоби копіювання й передачі інформації/даних, програмне забезпечення, якщо інше не входить у службові обов'язки співробітника;
- 6.4.2.16. Вносити з Банку обчислювальну й іншу техніку/устаткування, крім випадків вибуття у відрядження з ноутбуком, тощо;
- 6.4.2.17. Вносити та передавати засобами електронної пошти з Банку внутрішньобанківські нормативні документи, документи, що містять ІзОД;
- 6.4.2.18. Псувати/завдавати навмисної шкоди й використовувати технічні засоби, що належать Банку, в особистих цілях, записувати й програвати на робочій станції відео -, аудіо -, фото - та інші файли, що не мають відношення до службової діяльності, крім осіб, в обов'язку яких входять дані функції.
- 6.4.2.19. В частині виконання вимог законодавства та/або внутрішніх документів Банку з питань ПВК/ФТ:
- вступати у будь-які контакти з клієнтами Банку, фінансові операції яких несуть для Банку потенційні ризики легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та/або фінансування розповсюдження зброї масового знищення, крім спілкування в межах, необхідних для виконання покладених на працівника функціональних обов'язків;
 - повідомляти будь-яким третім особам (крім працівників Підрозділу фінансового моніторингу та Голови Правління Банку (особи, що виконує його обов'язки)) відомості про клієнтів та про операції, які підлягали фінансовому моніторингу або які можуть бути причетними до фінансування тероризму або фінансуванню розповсюдження зброї масового знищення;
 - повідомляти сторонніх осіб про зміст внутрішніх документів Банку з питань ПВК/ФТ;
 - повідомляти осіб, які здійснили операцію, що підлягає фінансовому моніторингу, та/або будь-яких третіх осіб про надання Підрозділу фінансового моніторингу повідомлення про підозрілу (сумнівну) активність клієнта або про надсилання до Спеціально уповноваженого органу повідомлення про таку операцію та/або про осіб, які її здійснили;
 - надавати консультації чи іншу допомогу фізичним особам чи суб'єктам господарювання щодо шляхів порушення або обходу законодавства та/або внутрішніх документів Банку з питань ПВК/ФТ;
 - у разі отримання від Спеціально уповноваженого органу, НБУ або правоохоронних органів запиту щодо операцій або іншої інформації з питань ПВК/ФТ, розголошувати (зокрема, особам, стосовно фінансових операцій яких проводиться перевірка, а також будь-яким третім особам) зміст запиту, інформацію, що подається на запит (у т.ч. про факт подання такої інформації або отримання запиту).

7. ПРАВА, ПОВНОВАЖЕННЯ ТА ВІДПОВІДАЛЬНІСТЬ НАЧАЛЬНИКА УПРАВЛІННЯ ТА ВНУТРІШНІХ АУДИТОРІВ ^{ПРИМІТКА}

7.1. Для виконання поставлених перед УПРАВЛІННЯМ завдань, **НАЧАЛЬНИК УПРАВЛІННЯ МАЄ ПРАВО:**

- 7.1.1. надавати на розгляд та затвердження Радою Банку розрахунок потреби в ресурсах УПРАВЛІННЯ, повідомляти про наявні обмеження;
- 7.1.2. ініціювати для проведення внутрішнього аудиту залучення працівників інших структурних підрозділів Банку ^{ПРИМ. 7.1.2;}

^{ПРИМІТКА} У разі залучення спеціалістів Банку для виконання окремих завдань внутрішнього аудиту, на період їх залучення на цих спеціалістів, в межах їх компетенції та дорученого завдання, розповсюджуються права, обов'язки та відповідальність, передбачені для внутрішніх аудиторів УПРАВЛІННЯ Банку.

^{ПРИМ. 7.1.2} **УМОВИ ЗАЛУЧЕННЯ УПРАВЛІННЯ СПЕЦІАЛІСТІВ БАНКУ ДЛЯ ВИКОНАННЯ ОКРЕМИХ ЗАВДАНЬ ВНУТРІШНЬОГО АУДИТУ.** У разі потреби скористатися зазначеним правом, начальник УПРАВЛІННЯ обговорює це питання з начальником структурного підрозділу, в якому знаходиться необхідна УПРАВЛІННЮ компетенція (СП - ВИКОНАВЕЦЬ). У випадку, коли начальник СП - ВИКОНАВЕЦЯ відмовляє у наданні УПРАВЛІННЮ працівника для виконання окремого аудиторського завдання, це питання, для вирішення, начальник УПРАВЛІННЯ може надати на розгляд Головою Правління Банку та, надалі, на розгляд Ради Банку, якщо на рівні Голови Правління питання не буде узгоджено.

Перед залученням працівника СП - ВИКОНАВЕЦЯ для виконання окремого аудиторського завдання начальник УПРАВЛІННЯ повинен впевнитися у **відсутності конфлікту інтересів**. А саме, залучений виконавець не може перевіряти/давати оцінку процесів, які знаходяться в зоні компетенції його основних (постійних) обов'язків та якщо у періоді, що підлягає перевірці, виконавець за цей напрямок відповідав або не минуло 12 місяців після завершення такої діяльності.

- 7.1.3. ініціювати залучення зовнішніх постачальників послуг (сторонніх фахівців та консультантів) для проведення внутрішнього аудиту ^{ПРИМ. 7.1.3};
- 7.1.4. надавати пропозиції Раді Банку щодо проведення планової аудиторської перевірки (аудиту);
- 7.1.5. ініціювати (за потреби) проведення позапланової аудиторської перевірки (аудиту) ^{ПРИМ. 7.1.5};
- 7.1.6. на пряму та необмежену можливість звернення до Ради, Правління Банку, брати участь ^{ПРИМ. 7.1.6} без права голосу в засіданнях Ради та/або Правління, створених в Банку профільних комітетів або комісій;
- 7.1.7. висловлювати свою думку, у тому числі на запит Правління Банку, з питань, пов'язаних з ризиковою діяльністю та засобами внутрішнього контролю Банку;
- 7.1.8. вимагати позачергового скликання засідання Ради Банку (Комітету Ради з питань аудиту);
- 7.1.9. надсилати до інших організацій та установ або третіх осіб запити щодо отримання потрібних відомостей та документів, пов'язаних з аудиторською перевіркою (аудитом);
- 7.1.10. на власний розсуд готувати пропозиції стосовно розміру преміювання працівників УПРАВЛІННЯ, враховуючи при цьому особисті результати кожного працівника, рівень їх компетенції та професіоналізму, наявність професійних ініціатив.

7.2. Для виконання поставлених перед УПРАВЛІННЯМ завдань, НАЧАЛЬНИК та ІНШІ ПРАЦІВНИКИ УПРАВЛІННЯ МАЮТЬ ПРАВО:

- 7.2.1. під час виконання своїх функцій, ініціювати спілкування з керівниками та з будь-якими працівниками Банку, структурними підрозділами Банку, незалежно від країни їх місцезнаходження;
- 7.2.2. на ознайомлення ^{ПРИМ. 7.2.2-1} з інформацією та документами, у тому числі тими, що зберігаються на електронних носіях, будь-якого підрозділу Банку, письмовими поясненнями з питань діяльності Банку, включаючи всі підрозділи Банку незалежно від країни їх місцезнаходження, та афілійованих осіб Банку - *мати доступ до будь-яких документів, інформації* Банку, його афілійованих осіб, архівів, даних, у тому числі електронних баз даних у режимі перегляду ^{ПРИМ. 7.2.2-2}, а також *мати доступ до об'єктів* Банку ^{ПРИМ. 7.2.2-3}, у тому числі до управлінської інформації, документів з прийняття рішень органами управління Банку;

^{ПРИМ. 7.1.3} У цьому разі з залученими фахівцями укладається відповідний договір, який передбачає відповідальність залучених фахівців за розголошення комерційної та банківської таємниці. Крім цього, Програма гарантії якості внутрішнього аудиту Банку, на дотримання вимог МСВА №2070, передбачає, що у випадках залучення Банком зовнішнього постачальника послуг до виконання окремих функцій внутрішнього аудиту (аутсорсинг проведення перевірок певного напрямку) відповідальність за якість, ефективність внутрішнього аудиту залишається за Банком. У таких випадках діє Програма гарантії та підвищення якості діяльності УПРАВЛІННЯ, із урахуванням особливостей, властивих процесу аутсорсингу. Зазначена норма враховується при укладенні договору на аутсорсинг аудиту певного напрямку - у частині "*Замовник (БАНК) несе відповідальність за належне застосування Програми гарантії та підвищення якості внутрішнього аудиту Банку в межах реалізації цього Договору*".

^{ПРИМ. 7.1.5} У разі, коли позапланова перевірка здійснюється в межах затвердженого Радою Банку резерву часу, зазначене рішення приймається начальником УПРАВЛІННЯ без оформлення відповідного протоколу Ради. Проведення позапланових перевірок за рахунок передбаченого резерву часу має відбуватися без загрози не виконання річного плану аудиту, в іншому випадку - питання щодо необхідності внесення змін до річного плану аудиту надається УПРАВЛІННЯМ на розгляд Радою Банку

^{ПРИМ. 7.1.6} З метою забезпечення належних умов реалізації даного права, секретарі колегіальних органів додають начальника УПРАВЛІННЯ до складу відповідної групи у корпоративній пошті/системі електронного документообігу, на адресу якої надсилаються порядок денний та документи до розгляду колегіальним органом.

^{ПРИМ. 7.2.2-1} В тому числі знімати копії з наданих для перевірки паперових документів, робити копії файлів будь-якої інформації, що зберігається на електронних носіях та є необхідною для проведення аудиторської перевірки (аудиту).

^{ПРИМ. 7.2.2-2} В тому числі (але не обмежуючись) - *доступ* до системи автоматизації банківських операцій; а також *право використовувати* бази даних та іншу інформацію з первинних документів Банку; програмне забезпечення, яке застосовується для автоматизації процесів у діяльності Банку, **у тому числі з питань фінансового моніторингу**; *право використовувати* фінансову, статистичну, управлінську та інші види звітності; інвентаризаційні матеріали Банку та документи створених в Банку профільних комітетів/ комісій; документи органів управління Банку, у тому числі з питань запровадження та функціонування систем управління ризиками та внутрішнього контролю; інші документи Банку, які необхідні для проведення аудиторських перевірок (аудиту).

^{ПРИМ. 7.2.2-3} В тому числі мати доступ до всіх приміщень Банку, у тому числі тих, що використовуються Банком для зберігання документів, готівки та інших цінностей.

7.2.3. отримувати письмові пояснення від керівників і працівників Банку з питань, що виникають під час проведення аудиторської перевірки (аудиту) та за її (його) результатами;

7.2.4. перевіряти вміст незгораємих сховищ, сейфів (в тому числі сейфів на робочих місцях працівників Банку, які надані їм для виконання посадових обов'язків) та робочих місць працівників Банку [крім індивідуальних сейфів, переданих в оренду клієнтам Банка на підставі відповідних договорів];

7.2.5. перевіряти відповідність кваліфікаційним вимогам та виконання професійних обов'язків працівниками Банку; перевіряти дотримання керівниками та працівниками Банку вимог ЗАКОНОДАВСТВА і внутрішніх положень Банку; перевіряти випадки перевищення повноважень посадовими особами Банку і виникнення конфлікту інтересів у Банку; оцінювати діяльність структурних підрозділів Банку (в тому числі підрозділів з управління ризиками та комплаєнс-ризик), створених Банком профільних комітетів/комісій;

7.2.6. обговорювати результати перевірок та висновки з Радою, Правлінням^{ПРИМ. 7.2.6}, керівниками структурних підрозділів Банку;

7.2.7. надавати керівництву Банку пропозиції стосовно заходів впливу на працівників, які дозволили виникнення порушень та недоліків;

7.2.8. бути обраним до складу ревізійних комісій дочірніх залежних товариств Банку (ДЗТ);

7.2.9. на робочі місця, обладнані відповідно до правил охорони праці, техніки безпеки та виробничої санітарії, на відвідування за рахунок Банку семінарів, конференцій, курсів та тренінгів з підвищення кваліфікації, придбання за рахунок Банку наукової, довідкової та іншої літератури та періодичних видань за напрямком роботи УПРАВЛІННЯ;

7.2.10. здійснювати інші права, передбачені для внутрішніх аудиторів Банків: ЗАКОНОДАВСТВОМ; НПА №311; Статутом і рішеннями Загальних зборів акціонерів Банку; Ради, Правління та Голови Правління Банку; цим Положенням, а також іншими внутрішніми нормативними та організаційно-розпорядчими документами Банку.

7.3. Працівники УПРАВЛІННЯ несуть відповідальність за:	начальник УПРАВЛІННЯ	внутрішні аудитори
7.3.1. організацію роботи та виконання поставлених перед УПРАВЛІННЯМ завдань;	ТАК	ПРИМ. 7.3
7.3.2. наявність у внутрішніх аудиторів достатньої кваліфікації та навичок;	ТАК	
7.3.3. здійснення контролю належного виконання підлеглими їх посадових обов'язків;	ТАК	ПРИМ. 7.3
7.3.4. належне, своєчасне виконання доручень начальника УПРАВЛІННЯ в межах своєї компетенції;		ТАК
7.3.5. професійний рівень та якість робіт, які виконуються працівником для вирішення завдань УПРАВЛІННЯ, неупередженість та об'єктивність оцінок;	ТАК	ТАК
7.3.6. якість та ефективність пропозицій ^{ПРИМ. 7.3.6} щодо вдосконалення систем корпоративного управління, управління ризиками та внутрішнього контролю, тощо;	ТАК	ТАК
7.3.7. несвоєчасне, неповне та неякісне виконання (в тому числі бездіяльність) посадових обов'язків, відповідно до чинного ЗАКОНОДАВСТВА, цього Положення та посадових інструкцій працівників;	ТАК	ТАК
7.3.8. схоронність документів Банку, наданих для перевірки;	ТАК	ТАК
7.3.9. не повідомлення/несвоєчасне повідомлення Підрозділу контролю за дотриманням норм (комплаєнс) Банку щодо наявності конфлікту інтересів при здійсненні свої функціональних обов'язків;	ТАК	ТАК

ПРИМ. 7.2.6 **Комунікації на рівні Правління та Ради Банку - компетенція начальника УПРАВЛІННЯ.**

ПРИМ. 7.3 начальники відділів зі складу УПРАВЛІННЯ несуть персональну відповідальність за організацію роботи цих відділів, належне і своєчасне виконання покладених на ці підрозділи завдань, функцій, за контроль належного виконання підлеглими їх посадових обов'язків.

ПРИМ. 7.3.6 Працівники УПРАВЛІННЯ несуть відповідальність за якісне опрацювання рекомендацій за результатами аудиту, **відповідальність за прийняте рішення стосовно підсумкового варіанту плану заходів до впровадження (та можливі наслідки) - несуть особи, які затвердили цей план заходів.**

7.3.10. порушення обов'язку щодо збереження комерційної та банківської таємниці, за незабезпечення режиму конфіденційності та інформації, що містить банківську, комерційну таємницю і іншу конфіденційну інформацію, розголошення персональних даних клієнтів, які стали відомі в ході проведення працівниками своєї діяльності на займаній посаді;	ТАК	ТАК
7.3.11. збереження майна та іншої власності Банку, що знаходиться у його безпосередньому користуванні;	ТАК	ТАК
7.3.12. недотримання вимог внутрішнього розпорядку роботи в Банку, правил з охорони праці, техніки безпеки та протипожежної безпеки.	ТАК	ТАК

7.4. Порушення трудової дисципліни, зокрема: невиконання або неналежне виконання з вини працівника покладених на нього посадових обов'язків, тягне за собою застосування заходів дисциплінарного впливу, а також застосування інших заходів, передбачених чинним ЗАКОНОДАВСТВОМ та внутрішньобанківськими нормативними документами Банку.

Порядок застосування дисциплінарних стягнень, а також підстави для цього визначаються чинним ЗАКОНОДАВСТВОМ.

Обов'язки і міра відповідальності начальника та працівників УПРАВЛІННЯ встановлюються у відповідності до діючого ЗАКОНОДАВСТВА, Статуту Банку, рішень Загальних зборів акціонерів, Ради та Правління Банку, даного Положення (в тому числі п.2.10, тощо) та посадових інструкцій працівників УПРАВЛІННЯ.

Начальник та працівники УПРАВЛІННЯ при підписанні цього Положення підтверджують, що їх проінформували про дисциплінарні стягнення, які застосовуватимуться до них у разі неприйнятної поведінки/ порушень у діяльності.

7.5. Персональна відповідальність працівників УПРАВЛІННЯ щодо ІНФОРМАЦІЙНОЇ БЕЗПЕКИ:

7.5.1. Співробітник несе всі ризики, пов'язані з тим, що надана Банком інформація може стати доступною третім особам;

7.5.2. За недотримання обов'язків щодо інформаційної безпеки співробітник може бути притягнутий до адміністративної чи кримінальної відповідальності, згідно чинного законодавства України ^{прим.ІБ};

7.5.3. Працівники УПРАВЛІННЯ особисто ознайомлені з *Політикою інформаційної безпеки Банку* та презентаціями щодо тематик інформаційної безпеки (<https://portal.accord.local/infobez/>);

7.5.4. Працівники УПРАВЛІННЯ, виконуючи роботу ^(або при проходженні практики або стажування в УПРАВЛІННІ) у Банку, **ЗОБОВ'ЯЗУЮТЬСЯ:**

- *Не розголошувати* відомостей, що складають банківську, комерційну таємницю та конфіденційну інформацію, які будуть довірені або стануть відомі їм при виконанні роботи;
- *Чітко і ретельно виконувати вимоги* наказів, інструкцій і положень щодо захисту банківської, комерційної таємниці та конфіденційної інформації, з якими ознайомлені по роботі;
- *Не повідомляти* в будь-якій формі будь-яким особам відомостей, що складаються банківську, комерційну таємницю та конфіденційну інформацію;
- У випадку припинення роботи *не розголошувати і не використовувати* для себе або для інших фізичних, юридичних осіб відомостей, що складають банківську, комерційну таємницю та конфіденційну інформацію.

7.5.5. Працівники УПРАВЛІННЯ попереджені, що у випадку порушення даного зобов'язання вони будуть зобов'язані відшкодувати Банку спричинений їх діями майновий та/або моральний збиток і завдану

^{прим.ІБ} Ст.363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електров'язку або порядку чи правил захисту інформації, яка в них оброблюється. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електров'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

За неодноразове або грубе порушення встановленого в Банку порядку захисту інформації з обмеженим доступом до працівника можуть бути застосовані дисциплінарні стягнення. Підставою для їх застосування є ст.147 КЗпП, Правила внутрішнього трудового розпорядку, Положення про комерційну таємницю. Відповідно до статті 147 КЗпП до порушника трудової дисципліни можуть застосовуватися такі заходи: • догана; • звільнення.

шкоду та будуть притягнені до кримінальної, а також до матеріальної відповідальності у відповідності до чинного законодавства України. Зі змістом статті ²³² КК України **працівники УПРАВЛІННЯ ознайомлені (про що працівники підтверджують своїм підписом при ознайомленні з цим Положенням).**

8. ВЗАЄМОДІЯ ТА ОБМІН ІНФОРМАЦІЄЮ МІЖ УПРАВЛІННЯМ ТА ЗОВНІШНІМИ ОРГАНІЗАЦІЯМИ, СТРУКТУРНИМИ ПІДРОЗДІЛАМИ ТА ОРГАНАМИ УПРАВЛІННЯ І КОНТРОЛЮ БАНКУ

8.1. Начальник УПРАВЛІННЯ має забезпечити в межах своїх повноважень на постійній основі співпрацю із ЗОВНІШНІМИ ОРГАНІЗАЦІЯМИ ^{ПРИМ. 8.1}.

8.2. Рада Банку має забезпечити надання УПРАВЛІННЮ плану та програми перевірки річної фінансової звітності, консолідованої фінансової звітності та іншої інформації щодо фінансово-господарської діяльності Банку, що здійснюється зовнішнім аудитором Банку.

8.3. Начальник УПРАВЛІННЯ має забезпечити можливість обміну між УПРАВЛІННЯМ та зовнішнім аудитором Банку - інформацією з питань проведення внутрішнього аудиту, у тому числі порядку застосування відповідних процедур аудиту. На вимогу зовнішнього аудитора Банку йому надаються на ознайомлення звіти внутрішнього аудиту Банку. Ознайомлення відбувається у присутності представника УПРАВЛІННЯ, який контролює повноту пакету документів (матеріали перевірок внутрішнього аудиту) після завершення контрольних процедур зовнішнього аудитора.

8.4. Взаємовідносини та обмін інформацією між УПРАВЛІННЯМ та ЗОВНІШНІМИ ОРГАНІЗАЦІЯМИ мають відбуватися з дотриманням вимог ЗАКОНОДАВСТВА та внутрішніх документів Банку щодо зберігання, захисту, використання та розкриття інформації, що становить банківську та комерційну таємницю. У разі надання ЗОВНІШНІМ ОРГАНІЗАЦІЯМ оригіналів документів УПРАВЛІННЯ на ознайомлення, факт передавання оформлюється відповідним Актом прийому - передавання зі здійсненням УПРАВЛІННЯМ контролю за наступним поверненням документів.

8.5. УПРАВЛІННЯ здійснює свою діяльність у постійній співпраці ^{ПРИМ. 8.5.1} зі структурними підрозділами та органами управління і контролю Банку з питань, які входять до компетенції УПРАВЛІННЯ. Взаємодія відбувається ^{ПРИМ. 8.5.2} по корпоративній електронній пошті *або* шляхом персонального інформування/ обговорення/ опитування ^{ПРИМ. 8.5.3} *або* із використанням системи електронного документообігу ^(з моменту її впровадження). Порядок взаємодії крім цього Положення регулюється «Регламентом роботи підрозділу внутрішнього аудиту (Управління внутрішнього аудиту) Банку» ^[або іншим документом, прийнятим на зміну регламенту], а також відповідними нормативними та іншими організаційно-розпорядчими документами Банку.

Обговорення Радою питань порядку денного засідання Ради відбувається після їх попереднього розгляду Комітетом Ради з питань аудиту. Порядок проведення засідань Комітету Ради з питань аудиту визначений у Положенні про цей Комітет.

Крім цього, у *поточному режимі* ^{ПРИМ. 8.5.4} можливі робочі комунікації між УПРАВЛІННЯМ та членами Комітету Ради з питань аудиту щодо питань, стосовно яких законодавство України не містить вимоги обов'язкового їх розгляду на засіданні Ради ^(із відповідним оформленням протоколу).

Стаття 232. Розголошення комерційної, банківської таємниці *або* професійної таємниці на ринках капіталу та організованих товарних ринках.

Умисне розголошення комерційної, банківської таємниці *або* професійної таємниці на ринках капіталу та організованих товарних ринках без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

^{ПРИМ. 8.1} Разом з тим, УПРАВЛІННЯ **не супроводжує** процеси проходження Банком зовнішнього аудиту і взаємодіє з зовнішнім аудитором лише з питань, які віднесені до компетенції УПРАВЛІННЯ.

^{ПРИМ. 8.5.1} Взаємодія, обмін інформацією та звітування, тощо.

^{ПРИМ. 8.5.2} Канали комунікації обираються на професійний розсуд начальника УПРАВЛІННЯ.

^{ПРИМ. 8.5.3} Із одночасним отриманням підтверджувального підпису проінформованих осіб.

^{ПРИМ. 8.5.4} Без подальшого документування.

Комітет Ради з питань аудиту в межах своїх наглядових обов'язків здійснює контроль за своєчасним інформуванням УПРАВЛІННЯ Правлінням та керівниками структурних підрозділів Банку про значні зміни у стратегії, методах та процедурах управління ризиками Банку, запровадження нових продуктів і змін в операційній діяльності Банку на ранньому етапі їх застосування, про ініціювання службових розслідувань та їх результати, щодо результатів перевірок органів контролю Банку.

9. ЗАГАЛЬНІ ВИМОГИ ДО РИЗИК-ОРІЄНТОВНОГО ПЛАНУВАННЯ АУДИТОРСЬКИХ ПЕРЕВІРОК ТА РІЧНОГО ПЛАНУ ПРОВЕДЕННЯ АУДИТОРСЬКИХ ПЕРЕВІРОК

9.1. УПРАВЛІННЯ здійснює аудиторські перевірки (аудит) відповідно до річного плану проведення аудиторських перевірок (аудиту) Банку на звітний рік, який може бути частиною довгострокового плану аудиту.

9.2. Річний план (зміни до плану) проведення аудиторських перевірок (аудиту) Банку складається начальником УПРАВЛІННЯ із застосуванням ризик-орієнтованого підходу та з урахуванням пропозицій і завдань, отриманих від Ради або Правління Банку, і, за потреби, може переглядатися (принаймні один раз на рік або частіше) для забезпечення оцінки тих сфер діяльності Банку, де містяться значні ризики.

9.3. Складання річного плану здійснюється в декілька етапів. Початок процедури та хід всіх етапів планування має бути організований таким чином, щоб забезпечити дотримання вимоги НПА №311 стосовно надання Банком до Національного банку плану проведення аудиторських перевірок (аудиту) на наступний звітний рік **не пізніше останнього робочого дня першого місяця** цього звітного року.

9.3.1. **Перший етап** - повідомлення про початок процесу планування та збір інформації.

9.3.1.1. Начальник УПРАВЛІННЯ інформує Раду та Правління Банку про початок процесу планування для надання пропозицій для включення до річного плану, проводить з ними ^{ПРИМ.9.3.1.1} ряд зустрічей, обговорює їх бачення ризиків, що властиві Банку, їх побажання та очікування від внутрішнього аудиту у плановому році.

9.3.1.2. УПРАВЛІННЯ запитує у підрозділів Банку інформацію: щодо нових видів впроваджених (або тих, що планується впровадити у звітному році) послуг / продуктів; перелік підрозділів, у яких відбулися (або заплановані) організаційні зміни; перелік підрозділів із рівнем плинності кадрів, що перевищує середній рівень по Банку, в тому числі зі змінами у керівному складі; інформацію стосовно впроваджених до експлуатації нових автоматизованих систем; перелік напрямків діяльності, за якими посилилась увага регулятора, присутні значні зміни у ЗАКОНОДАВСТВІ, тощо. Також розглядаються скарги, інциденти операційного ризику, матеріали службових розслідувань, результати внутрішнього аудиту, перевірок Банку органами нагляду та таке інше. Зазначений перелік інформації для розгляду є орієнтовним та може буде змінений за рішенням начальника УПРАВЛІННЯ.

9.3.2. **Другий етап** - аналіз та визначення об'єктів аудиту, оцінка ризиків.

9.3.2.1. Внутрішньому аудиту можуть підлягати (бути об'єктом аудиту) всі напрямки діяльності Банку ^{ПРИМ. 9.3.2.1}, будь-який процес, діяльність будь-якого підрозділу та працівника Банку.

9.3.2.2. УПРАВЛІННЯ концентрує свою увагу на тих напрямках, яким властивий більший рівень ризику та/або на яких рівень ризику збільшується у зв'язку з неадекватністю систем внутрішнього контролю. Оцінка ризиків здійснюється шляхом визначення переліку параметрів, варіантів їх кількісної оцінки та питомої ваги впливу значення кількісної оцінки кожного параметру на загальну оцінку ризику потенційного об'єкту аудиту.

9.3.2.3. Щодо кожного потенційного об'єкту аудиту обчислюється загальний бал оцінки ризику, як сума оцінок кожного із параметрів даного об'єкту аудиту, зважених на питому вагу їх впливу на загальну оцінку ризику об'єкту.

ПРИМ. 9.3.1.1 На розсуд начальника УПРАВЛІННЯ, таке обговорення також може бути проведено із керівниками самостійних структурних підрозділів Банку.

ПРИМ. 9.3.2.1 В тому числі види діяльності Банку, виконання яких забезпечується шляхом залучення юридичних і фізичних осіб на договірній основі (аутсорсинг).

9.3.3. **Третій етап** - оцінка ресурсів УПРАВЛІННЯ, визначення пріоритетів та складання проекту річного плану.

9.3.3.1. Начальник УПРАВЛІННЯ оцінює ресурси УПРАВЛІННЯ. Розраховується потенційний фонд робочого часу працівників УПРАВЛІННЯ на звітний рік, прогноз його (фонду) утилізації, враховуючи передбачені вимогами чинного ЗАКОНОДАВСТВА, цим Положенням обов'язкові *інші функції* (навчання, звітність, розробка/доопрацювання методології внутрішнього аудиту, тощо).

9.3.3.2. Також у розрахунок прогнозованої утилізації потенційного річного фонду робочого часу працівників УПРАВЛІННЯ додається ^{РЕЗЕРВ} часу на позапланові процедури. Резерв може бути використаний внутрішніми аудиторами за наступними напрямками (але не обмежуючись):

- надання консультативних послуг;
- проведення позапланових раптових ревізій кас відділень Банку;
- проведення перевірок, ініційованих членами Ради, Правління Банку, начальником УПРАВЛІННЯ тощо.

9.3.3.3. Для формування проекту річного плану, начальник УПРАВЛІННЯ враховує:

- прогнозний розмір не утилізованого ² потенційного річного фонду робочого часу УПРАВЛІННЯ;
- перелік перевірок, які обов'язкові для проведення у звітному році відповідно до вимог чинного законодавства та нормативно-правових актів Національного банку;
- перелік перевірок, рекомендованих контролюючими органами та органами нагляду;
- пропозиції Ради та Правління Банку;
- результати оцінки ризиків потенційних об'єктів аудиту.

9.3.3.4. За кожним із потенційних об'єктів аудиту обчислюються орієнтовні затрати часу, необхідні для перевірки. Також приймається до уваги фактична кваліфікація працівників УПРАВЛІННЯ, ступінь їх досвіду, можливі обмеження щодо ротації аудиторів.

9.3.3.5. Для прийняття кінцевого рішення стосовно складу переліку перевірок у проекті річного плану внутрішнього аудиту начальник УПРАВЛІННЯ застосовує професійне судження аудитора.

9.3.3.6. Результати проведеного аналізу документуються у довільні формі на розсуд начальника УПРАВЛІННЯ.

9.4. Розроблений проект річного плану начальник УПРАВЛІННЯ обговорює із Головою Правління Банку та надає план на розгляд та затвердження Радою Банку. Проект річного плану надається на розгляд Ради незалежно від наявності або відсутності його узгодження Головою Правління Банку, але у разі не згоди Голови Правління Банку це питання та аргументи, як Голови Правління, так і начальника УПРАВЛІННЯ, зазначаються та обговорюються на засіданні Ради Банку при розгляді проекту річного плану.

9.5. У затверджений річний план аудиту протягом року можуть бути внесені зміни, які узгоджуються та розглядаються, затверджуються у порядку, аналогічному порядку затвердження річного плану аудиту.

10. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

10.1. Це Положення складається та переглядається ^{ПРИМ. 10.1.1} начальником УПРАВЛІННЯ, затверджується Радою Банку ^{ПРИМ. 10.1.2}, набуває чинності з моменту його затвердження та діє безстроково до моменту його відміни або прийняття нового внутрішнього нормативного документу, зі вступом в силу якого це Положення втрачає свою чинність.

^{РЕЗЕРВ} Розмір резерву робочого часу, передбаченого у розрахунку прогнозованої утилізації потенційного річного фонду робочого часу УПРАВЛІННЯ, вказується в матеріалах на затвердження річного плану.

² Після врахування резерву часу на позапланові процедури та обов'язкові *інші функції*.

^{ПРИМ. 10.1.1} Начальник УПРАВЛІННЯ щороку аналізує необхідність оновлення цього Положення (внесення змін / викладення у новій редакції), в тому числі досліджує зміни у МСВА, НОРМАХ ЕТИКИ АУДИТОРІВ, ЗАКОНОДАВСТВІ, що відбулися з дати останньої редакції Положення. За результатами опрацювання начальник УПРАВЛІННЯ надає на розгляд Радою проект оновленого Положення або інформацію щодо відсутності необхідності оновлювати Положення.

^{ПРИМ. 10.1.2} Всі зміни та доповнення до цього Положення затверджуються у порядку, аналогічному процедурі затвердження цього Положення.

10.2. У випадку, коли окремі норми цього Положення будуть суперечити діючому законодавству України / МСВА/ НОРМАМ ЕТИКИ АУДИТОРІВ або рішенням, які пізніше дати затвердження цього Положення прийняті Радою або Загальними зборами акціонерів Банку, такі норми не мають сили та не застосовуються.

10.3. Положення доводиться до відома всіх керівників і працівників Банку, а також розміщується на загальнодоступному мережевому диску / порталі або у системі електронного документообігу Банку, тощо, для можливості ознайомлення з ним усіх зацікавлених осіб Банку.

10.4. Після затвердження один примірник цього Положення зберігається у начальника УПРАВЛІННЯ. Другий примірник Положення зберігається в Управлінні по роботі з персоналом Банку. Начальник та інші працівники УПРАВЛІННЯ мають бути ознайомлені з цим Положенням під особистий підпис (в тому числі, до початку роботи особи на посаді та/або у разі внесення змін до Положення). Відповідальність за ознайомлення з Положенням (в діючій (затвердженій) редакції) начальника та інших працівників УПРАВЛІННЯ (в тому числі, до початку роботи особи на посаді та/або у разі внесення змін до Положення) під особистий підпис покладається на Управління по роботі з персоналом Банку.

Начальник Управління внутрішнього аудиту

К.В. Шляхтіна